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

Querschnittsprüfung der Massnahmen bei Systemausfällen von Fachapplikationen

Bundesamt für Zoll und Grenzsicherheit,
Eidgenössische Steuerverwaltung,
Bundesamt für Informatik und Telekommunikation

EFK-22520/22752 | inkl. Stellungnahmen | 5. Dezember 2022 | FinDel D1/2023

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	606.22520/609.22752
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

Querschnittsprüfung der Massnahmen bei Systemausfällen von Fachapplikationen

Bundesamt für Zoll und Grenzsicherheit, Eidgenössische Steuerverwaltung, Bundesamt für Informatik und Telekommunikation

Das Wesentliche in Kürze

Ein Business Continuity Management (BCM) dient der Aufrechterhaltung des Geschäftsbetriebs einer Organisation beim Eintreten eines Schadensereignisses. Darunter fällt die Vorbereitung, die Bewältigung und die Nachbereitung eines Ereignisses. Im Frühjahr 2017 wurde ein bundesweites BCM-Regelwerk verabschiedet und von den Departementen und der Bundeskanzlei in Kraft gesetzt.

Die Eidgenössische Finanzkontrolle (EFK) prüfte beim Bundesamt für Zoll und Grenzsicherheit (BAZG) und bei der Eidgenössische Steuerverwaltung (ESTV) den Stand der Umsetzung des BCM anhand eines Frameworks zur Ermittlung des Reifegrades.

Da die Datensicherung und die Wiederherstellung nach einem Ereignis eine wichtige Komponente eines BCM darstellt, wurde in einem parallellaufenden Audit die Sicherungsanwendung «NetBackup» beim Bundesamt für Informatik und Telekommunikation (BIT) geprüft. Dabei wurde der sichere Betrieb und die Zuverlässigkeit der Sicherungs- und Wiederherstellungsprozesse untersucht.

Das BCM-System des BAZG verfügt über einen hohen Reifegrad

Die Dokumentationen und Konzepte für das BCM weisen beim BAZG einen hohen Detaillierungsgrad aus. Die kritischen Geschäftsprozesse sind identifiziert und das Vorgehen im Schadenfall ist ausführlich beschrieben. Die geplanten Massnahmen sind nachvollziehbar und für das BAZG angemessen. Die Informatikmittel, die diese Prozesse unterstützen, sind redundant und hochverfügbar aufgebaut.

Das Testen und Üben der BCM-Massnahmen wurden in den vergangenen Jahren aufgrund verschiedener Einflüsse vernachlässigt. Eine detaillierte Aufstellung der geplanten Übungen liegt vor und diese sollen sich in den kommenden Jahren über sämtliche Bereiche des BCM erstrecken.

Die ESTV hat wesentliche Fortschritte erzielt, weitere Arbeiten sind noch zu leisten

Das BCM der ESTV hat, verglichen mit der letzten Beurteilung im Jahr 2016, grosse Fortschritte erzielt. Die erforderlichen Dokumente sind vorhanden, sind jedoch teilweise zu generisch gehalten. So werden die in der Business-Impact-Analyse festgehaltenen kritischen Geschäftsprozesse in der Planung nicht konsequent weiterbehandelt.

Ein übergeordnetes Testkonzept, welches die Testarten und Anspruchsgruppen definiert, ist nicht vorhanden. Zu einzelnen Übungen wurden jedoch gesonderte Konzepte erarbeitet. Eine Evakuierungsübung konnte im letzten Jahr erfolgreich durchgeführt werden.

Schutz vor Verschlüsselungstrojanern hat höchste Priorität

Die Systeme zur Erbringung der Marktleistung «Backup und Recovery» des BIT sind redundant aufgebaut und werden hochverfügbar betrieben. Die implementierten Sicherheitsmassnahmen entsprechen den heutigen Anforderungen.

Die vertraglich vereinbarten Wiederherstellungszeiten können jedoch bei grossen Datenbanken aufgrund ihrer Volumen nicht vollumfänglich sichergestellt werden.

Eines der grössten Risiken hinsichtlich der Verfügbarkeit von Systemen und Datenbanken sind heute Verschlüsselungstrojaner, sogenannte Ransomware. Ein expliziter Schutz dagegen ist auf den Backup-Systemen noch nicht implementiert. Das BIT hat dies adressiert, ausserdem ist ein externes Assessment zum Schutz der Datensicherungen gegen Ransomware geplant. Dieser Sachverhalt gilt es zu priorisieren, allfällige Massnahmen sind zeitnah umzusetzen.

Audit transversal des mesures en cas de défaillance des systèmes d'applications métier

Office fédéral de la douane et de la sécurité des frontières, Administration fédérale des contributions, Office fédéral de l'informatique et de la télécommunication

L'essentiel en bref

La gestion de la continuité des activités (*Business Continuity Management*, BCM) sert à maintenir les activités d'une organisation en cas de défaillance. Il inclut la préparation en vue d'une défaillance, la gestion et le suivi après une défaillance. Au printemps 2017, une réglementation relative à la BCM a été adoptée au sein de l'administration fédérale et mise en œuvre dans les départements et à la Chancellerie fédérale.

Le Contrôle fédéral des finances (CDF) a vérifié auprès de l'Office fédéral de la douane et de la sécurité des frontières (OFDF) ainsi que de l'Administration fédérale des contributions (AFC) l'avancement de la mise en œuvre de la BCM en évaluant son degré de maturité.

Étant donné que la sauvegarde des données et leur restauration à la suite d'une défaillance constituent une composante importante d'une BCM, l'application de sauvegarde « NetBackup » a été examinée dans un audit parallèle à l'Office fédéral de l'informatique et de la télécommunication (OFIT). La sécurité de l'exploitation et la fiabilité des processus de sauvegarde et de restauration ont été auditées.

Le système de BCM de l'OFDF a un degré de maturité élevé

À l'OFDF, la documentation et les plans relatifs à la BCM sont très détaillés. Les processus opérationnels critiques ont été identifiés et la marche à suivre en cas de défaillance est précisément décrite. Les mesures prévues sont compréhensibles et adéquates pour l'OFDF. Les moyens informatiques qui soutiennent ces processus sont installés de manière redondante et offrent une haute disponibilité.

Pour différentes raisons, les tests et la mise en pratique des mesures de BCM ont été négligés ces dernières années. Une liste détaillée des exercices prévus est disponible, ces derniers doivent couvrir tous les domaines concernés par la BCM dans les années à venir.

L'AFC a réalisé des progrès importants, mais certains travaux sont encore nécessaires

La BCM de l'AFC a beaucoup progressé par rapport à la dernière évaluation en 2016. Les documents nécessaires existent, mais sont parfois trop génériques. Ainsi, les processus opérationnels critiques identifiés dans l'analyse d'impact sur les activités ne sont pas traités systématiquement dans la planification.

Il n'existe pas de plan de test global définissant les types de tests à effectuer et les groupes concernés. Cependant, des plans distincts ont été établis pour certains exercices. Un exercice d'évacuation a pu être mené avec succès l'année dernière.

La protection contre les chevaux de Troie verrouillant les données est prioritaire

Les systèmes pour fournir la prestation de marché « Sauvegarde et restauration » de l'OFIT sont installés de manière redondante et offrent une haute disponibilité. Les mesures de sécurité implémentées répondent aux exigences actuelles.

Les délais de restauration convenus contractuellement ne peuvent toutefois pas être entièrement garantis pour les grandes bases de données en raison de leur volume.

Les chevaux de Troie verrouillant les données, appelés rançongiciels, constituent aujourd'hui l'un des plus grands risques pour la disponibilité des systèmes et des bases de données. Une protection spécifique contre ces logiciels malveillants n'est pas encore implémentée dans les systèmes de sauvegarde. L'OFIT traite cette question. De plus, une évaluation externe pour protéger les sauvegardes de données contre les rançongiciels est prévue. Cette thématique doit être considérée comme prioritaire et les éventuelles mesures à prendre doivent être mises en œuvre rapidement.

Texte original en allemand

Verifica trasversale concernente le misure in caso di guasti al sistema delle applicazioni specialistiche

Ufficio federale della dogana e della sicurezza dei confini, Amministrazione federale delle contribuzioni, Ufficio federale dell'informatica e della telecomunicazione

L'essenziale in breve

La gestione della continuità operativa (Business Continuity Management, BCM) serve a garantire la continuità delle attività operative di un'organizzazione in caso di evento dannoso. Ciò include la preparazione, la gestione e il follow-up di un evento. Nella primavera del 2017 è stata adottata e messa in vigore dai dipartimenti e dalla Cancelleria federale una regolamentazione concernente il BCM.

Il Controllo federale delle finanze (CDF) ha verificato lo stato di attuazione del BCM presso l'Ufficio federale della dogana e della sicurezza dei confini (UDSC) e l'Amministrazione federale delle contribuzioni (AFC), utilizzando un framework per determinarne il livello di maturità.

Poiché il backup e il ripristino dei dati dopo un evento rappresentano una componente importante del BCM, l'applicazione di sicurezza «NetBackup», messa a punto dall'Ufficio federale dell'informatica e della telecomunicazione, è stata sottoposta a una verifica parallela. In questo contesto, sono stati esaminati la sicurezza dell'esercizio e l'affidabilità dei processi di backup e ripristino.

Il sistema BCM dell'UDSC dispone di un elevato livello di maturità

La documentazione e i piani inerenti al BCM dell'UDSC presentano un grado di dettaglio elevato. Sono stati individuati i processi aziendali critici e la procedura in caso di sinistro è descritta dettagliatamente. Le misure previste sono comprensibili e adeguate all'UDSC. I mezzi informatici che supportano questi processi sono mezzi informatici ridondanti ad alta disponibilità.

Il collaudo e la messa in pratica delle misure BCM sono stati trascurati negli ultimi anni a causa di vari fattori. È disponibile un elenco dettagliato delle esercitazioni previste, che dovranno coprire nei prossimi anni tutti i settori inerenti al BCM.

L'AFC ha compiuto progressi significativi, ma occorre fornire ancora ulteriori lavori

Rispetto all'ultima valutazione del 2016, il BCM dell'AFC ha compiuto importanti progressi. I documenti richiesti sono disponibili, ma alcuni sono troppo generici. Ad esempio, i processi aziendali critici individuati nell'analisi d'impatto sull'operatività (business impact analysis) non vengono seguiti in modo sistematico nella pianificazione.

Non esiste un piano di testing sovraordinato che definisca i vari tipi di test e i gruppi di destinatari. Tuttavia sono stati elaborati piani separati per le singole esercitazioni. L'anno scorso è stata effettuata con successo una prova di evacuazione.

La protezione contro i ransomware ha la massima priorità

I sistemi per la fornitura della prestazione di mercato «backup e recovery» dell'UFIT sono sistemi ridondanti ad alta disponibilità. Le misure di sicurezza implementate soddisfanno i requisiti attuali.

Tuttavia i tempi di ripristino convenuti per contratto non possono essere completamente garantiti per le grandi banche dati a causa delle loro dimensioni.

Uno dei maggiori rischi odierni connesso alla disponibilità dei sistemi e delle banche dati sono i ransomware. Nei sistemi di backup non è ancora stata implementata una protezione specifica contro questo tipo di malware. L'UFIT ha affrontato il problema ed è prevista anche una valutazione esterna per proteggere i backup contro i ransomware. Occorre prioritizzare questa problematica e attuare tempestivamente le eventuali misure.

Testo originale in tedesco

Cross-sectional audit of measures taken during system failures in specialist applications

Federal Office for Customs and Border Security, Federal Tax Administration, Federal Office of Information Technology, Systems and Telecommunication

Key facts

Business continuity management (BCM) serves to maintain an organisation's business operations during an incident. This includes preparations for, management of and follow-up after an incident. In spring 2017, a standardised set of federal BCM rules was issued and implemented by the departments and the Federal Chancellery.

Using a maturity evaluation framework, the Swiss Federal Audit Office (SFAO) assessed the status of BCM implementation at the Federal Office for Customs and Border Security (FOCBS) and the Federal Tax Administration (FTA).

As data backup and recovery after an incident are important components of BCM, a second audit was conducted in parallel on the NetBackup security application at the Federal Office of Information Technology, Systems and Telecommunication (FOITT). This evaluated the secure operation and reliability of the backup and recovery processes.

The FOCBS's BCM system has a high degree of maturity

The documentation and concepts for BCM at the FOCBS are very detailed. The critical business processes are identified and the procedure in the event of an incident is described in detail. The planned measures are comprehensible and appropriate for the FOCBS. The IT supporting these processes has redundancy and high availability.

Testing and exercises in relation to BCM measures have been put on hold over the past few years, owing to a number of factors. The planned exercises are described in detail and they should be expanded to cover all areas of the FOCBS over the next few years.

The FTA has made significant progress, but more work is needed

Compared to the previous assessment in 2016, the FTA's BCM has made significant progress. The required documents exist, although some of them are formulated too generically. For example, the critical business processes listed in the business impact analysis are not dealt with consistently during the planning phase.

There is no overarching test concept defining the types of test and stakeholders. However, specific concepts have been drawn up for individual exercises. An evacuation exercise was carried out successfully last year.

Protection against encryption Trojans has top priority

The FOITT systems providing the backup and recovery market supply have redundancy and high availability. The implemented security measures comply with current requirements.

However, the contractually agreed recovery times cannot be completely ensured for large databases, owing to their volume.

Today, encryption Trojans, known as ransomware, pose one of the greatest risks to the availability of systems and databases. Explicit protection against this has not yet been implemented on the backup systems. The FOITT has addressed this, and an external assessment on how to protect data backups against ransomware is planned. This matter should be prioritised, and any measures required should be implemented swiftly.

Original text in German

Generelle Stellungnahme der Geprüften

Generelle Stellungnahme des BAZG

Das BAZG bedankt sich für die Prüfung und die positive Rückmeldung der EFK. Das BAZG wird die Arbeiten gemäss definierter Roadmap und Mehrjahresplanung konsequent weiterführen und insbesondere auch den Aspekt der Schulungen, Tests und Übungen beachten.

Generelle Stellungnahme der ESTV

Entsprechend der im Vergleich zum BAZG bei der ESTV tiefer liegenden Kritikalität ihrer Geschäftstätigkeit und Ausfalltoleranz wird im Jahr 2023 ein BCM-Maturitätslevel von 3 bis max. 4 in allen fünf geprüften Bereichen angestrebt. Erreicht werden soll dieses Level mit einer grundlegenden Überarbeitung der BIA, einer Aktualisierung der darauf basierenden Dokumente, einer engeren Anbindung der Notfallplanung an das BCM, einer Verbesserung der Nachvollziehbarkeit von Änderungen im BCM, der Erstellung eines bedarfsgerechten BCM-Testkonzepts sowie einer mehrjährigen Übungsplanung.

Die ESTV bedankt sich ihrerseits für die angenehme Zusammenarbeit mit der EFK. Die Prüfergebnisse bestätigen einerseits den nach 2016 erreichten Fortschritt und zeigen andererseits das konkrete Potenzial für weitere Verbesserungen auf. Die beiden Empfehlungen decken sich im Wesentlichen mit eigenen Einschätzungen, welche im Rahmen des Überarbeitungszyklus 2023 zur Umsetzung anstehen. In diesem Sinne wirkt dieser Bericht als konstruktiver Beschleuniger.

Generelle Stellungnahme des BIT

Das BIT bedankt sich bei der EFK für die konstruktive Zusammenarbeit mit den Prüfexperten und für die Hinweise in den Beurteilungen. Weitere Massnahmen zu Empfehlung 3 befinden sich in Umsetzung oder werden weitergeführt.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Querschnittsprüfung der Massnahmen bei Systemausfällen von Fachapplikationen

Im Nachgang zu der strategischen Führungsübung des Bundes im Jahr 2009 wurde festgestellt, dass die Bundesverwaltung über keine Vorgaben für ein Business Continuity Management (BCM) verfügt. Die Thematik wurde ab 2009 in verschiedenen Prüfungen der Eidgenössischen Finanzkontrolle (EFK) abgedeckt.

Mit der Querschnittsprüfung «Angemessenheit des Business Continuity Managements» (PA 16564)[1] hat die EFK 2016 bei fünf Verwaltungseinheiten (VE) im Eidgenössischen Finanzdepartement (EFD) eine erste Erhebung der BCM-Massnahmen durchgeführt. Dabei wurden unter anderen auch das Bundesamt für Zoll und Grenzsicherheit (BAZG)[2] und die Eidgenössische Steuerverwaltung (ESTV) beurteilt.

In der Folge wurde im Frühjahr 2017 ein bundesweites BCM-Regelwerk verabschiedet und im darauffolgenden Sommer von den Departementen und der Bundeskanzlei in Kraft gesetzt. Um den unterschiedlichen Bedürfnissen und Situationen der einzelnen VE gerecht zu werden, wurde ein dezentraler Ansatz gewählt. Die BCM-Richtlinie garantiert eine flächendeckende Einführung eines BCM-Systems (BCMS). Des Weiteren regelt sie neben den vier bekannten Phasen (siehe Kapitel2.1) auch die Funktionen und Verantwortlichkeiten. Die Verantwortung für den Aufbau und die periodische Überprüfung des BCM obliegt den Leitungen der VE.

Der Fokus der vorliegenden Querschnittsprüfung liegt bei den Massnahmen zur Begegnung von möglichen Systemausfällen. Dabei steht die Aufrechterhaltung des Betriebs, der Kommunikation und die Verfügbarkeit wichtiger Fachapplikationen im Zentrum. Bei den beiden VE BAZG und ESTV wurden ausserdem jeweils zwei Fachanwendungen hinsichtlich der Datensicherung und Wiederherstellung näher beleuchtet (siehe Kapitel 5.2 und 5.3). Die Aspekte der Datensicherung wurden in einer gesonderten Prüfung der EFK (PA 22752) beim Bundesamt für Informatik und Telekommunikation (BIT) parallel geprüft[3]. Die Resultate sind Bestandteil dieses Berichtes.

Prüfung der Sicherheit und des Betriebs der Anwendung NetBackup (PA 22752)

Das BIT betreibt die Anwendung NetBackup[4]. Diese wird verwendet für die Sicherung und Widerherstellung aller Speichermedien mit Ausnahme der Grossrechner (sog. Mainframes) und der Cloud-Dienste. Die Anwendung hat hohe Anforderungen an den Daten- und Informationsschutz und die Verfügbarkeit. Wenn die Sicherungs- und Wiederherstellungsprozesse ungenügend funktionieren, besteht das Risiko eines Datenverlusts. Mit der Prüfung soll beurteilt werden, ob das BIT die Anwendung sicher und mit einer hohen Zuverlässigkeit betreibt. Dabei soll auch beurteilt werden, ob die Periodizität und der Umfang der Datensicherheits- oder Datensicherungsleistungen den Bedürfnissen der Kunden entsprechen. Die Ergebnisse dieser Prüfung sind im Kapitel 5 des vorliegenden Berichts festgehalten.

---

1 Der Prüfbericht wurde der Finanzdelegation vorgelegt.
2 Bis 31. Dezember 2021 Eidgenössische Zollverwaltung (EZV)
3 Der Prüfbericht wurde der Finanzdelegation vorgelegt.
4 https://www.veritas.com/de/ch/protection/NetBackup

1.2 Prüfungsziel und -fragen

Das Ziel der Querschnittsprüfung ist die Beurteilung der Massnahmen bei Systemausfällen. Daraus ergeben sich die folgenden Prüffragen:

1. Entsprechen die BCM-Vorkehrungen des BAZG/ESTV den Richtlinien des EFD?
2. Sind die kritischen Geschäftsprozesse und die dafür notwendigen Ressourcen bekannt, priorisiert und die damit verbundenen Risiken sowie deren Auswirkungen definiert?
3. Verfügt die Organisation über eine angemessene Planung zur Sicherstellung der kontinuierlichen Geschäftstätigkeit bzw. einer zeitgerechten Wiederaufnahme der kritischen Geschäftsprozesse nach einem Zwischenfall?
4. Wird das BCM regelmässig getestet und nötigenfalls angepasst?
5. Wurden die Empfehlungen 16564.001[5] und 16564.002 umgesetzt?

Die Prüfung 22752 soll beurteilen, ob das BIT die Anwendung NetBackup sicher und mit einer hohen Zuverlässigkeit betreibt. Die Prüffragen lauten:

1. Ist die Infrastruktur und Betrieb der Anwendung NetBackup so konzipiert, dass eine angemessene Sicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) und Resilienz sichergestellt sind?
2. Stellt das BIT sicher, dass eine Widerherstellung von Daten in angemessener Frist erfolgen kann?
3. Deckt das BIT die Bedürfnisse der Leistungsbezüger bezüglich Periodizität und Umfang der Backup-Leistungen ab?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Roland Gafner (Revisionsleiter), Warren Paulus und Elizabeth O'Sullivan vom 23. Mai bis 8. Juli 2022 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger.

Die Beurteilungen orientieren sich an der Richtlinie zum BCM des EFD vom 1. Juli 2017. Weiter kamen die Empfehlungen der International Organization for Standardization (ISO/IEC) Standard 22301[6] zur Anwendung. Mittels dem auf dem ISO-Standard beruhenden Framework «BCM Fitness Check» wurde der Reifegrad in den einzelnen Disziplinen ermittelt (siehe auch Anhang 6).

Die Prüfung 22752 wurde von Christian Brunner (Revisionsleiter) und Stefano Iafigliola vom 2. bis 22. Mai 2022 durchgeführt. Sie erfolgte ebenfalls unter der Federführung von Bernhard Hamberger.

Die Beurteilungen orientieren sich an den Vorgaben des Bundes und an Best-Practice-Ansätzen.

---

[5] «Prüfung der Angemessenheit des Business Continuity Managements» (PA 16564), EFD

[6] Sicherheit und Schutz des Gemeinwesens – Aufrechterhaltung der Betriebsfähigkeit – Anforderungen (ISO 22301:2012)

Die Feedbackgespräche haben am 21. Juni 2022 (BIT), 30. Juni 2022 (BAZG) und 29. August 2022 (ESTV) stattgefunden. Der vorliegende Bericht berücksichtigt nicht die Entwicklungen nach diesen Besprechungen.

1.4 Unterlagen und Auskunftserteilung

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

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 27. Oktober 2022 statt. Teilgenommen haben seitens des BAZG, der Chef Controlling und Integriertes Risikomanagement (IRM), der Dienstchef IRM sowie ein Fachspezialist IRM.

Die ESTV war vertreten durch die Vizedirektorin, den Leiter Direktionsstab, den Leiter Informatik, den Leiter Qualitätssteuerung und einen Revisionsexperten.

Vom BIT haben der Leiter Platform Services, der Leiter Business Solutions und der Product Owner Backup und Storage teilgenommen.

Von der EFK haben der Mandatsleiter, der Federführende, die Revisionsleiter und ein Teammitglied 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 Business Continuity Management

2.1 Wozu benötigt der Bund ein Business Continuity Management?

Die heutigen und künftigen Geschäftsprozesse werden durch die vermehrte Digitalisierung der Betriebsabläufe, Globalisierung, Outsourcing und stark optimierten Lieferketten zunehmend anfälliger auf Störungen aufgrund von Schadenereignissen. Solche Ereignisse können verschiedene Ursprünge haben. Dazu gehören neben Naturkatastrophen wie Überschwemmungen oder Unwetter auch Stromausfälle, Störungen und Beschädigungen der Infrastruktur. Auch lokale und globale gesundheitliche Aspekte wie Epidemien oder Pandemien sowie personelle oder materielle Verluste durch Anschläge, Cyberangriffe oder Unfälle können eine Krise auslösen und den Geschäftsbetrieb gefährden.

BCM und Risikomanagement in der Bundesverwaltung

In der Bundesverwaltung ist das BCM ein Bestandteil des integrierten Risikomanagementsystems (RM).

Das RM steuert präventiv Risiken, während die BCM-Massnahmen im Ereignisfall helfen sollen, Schadenauswirkungen zu minimieren. Das BCM fokussiert sich somit auf die Bewältigung und nicht auf die Ursachen einer Betriebsstörung.

Das Ziel des BCM ist also die Aufrechterhaltung des Geschäftsbetriebs der VE beim Eintreten eines Schadensereignisses. Dazu gehört auch die Vorbereitung, die Bewältigung und die Nachbereitung eines solchen Ereignisses. Der Betrieb eines BCM ist daher wichtig, um die Funktion einer VE bei dem Eintreten eines Schadensereignisses zu gewährleisten. Neben der Fähigkeit, bei einer auftretenden Störung oder einem Schadensereignis im Betrieb weiterzuarbeiten, ergeben sich weitere Vorteile. Zum einen führt die Entwicklung eines BCM dazu, dass sich ein besseres Verständnis für interne und externe Zusammenhänge in der VE bildet. Der Austausch und die Kommunikation zwischen verschiedenen Abteilungen werden gefördert, weil die Notwendigkeit einer abteilungsübergreifenden Zusammenarbeit beim Eintreten von Schadensereignissen sichtbar wird. Grundsätzlich sind nach gängigen Standards und den Vorgaben des Bundes beim BCM vier Phasen vorgesehen. Der BCM-Lebenszyklus stellt die Phasen der Implementierung und des Betriebs des BCM als Zyklus-Modell dar (siehe Grafik unten).

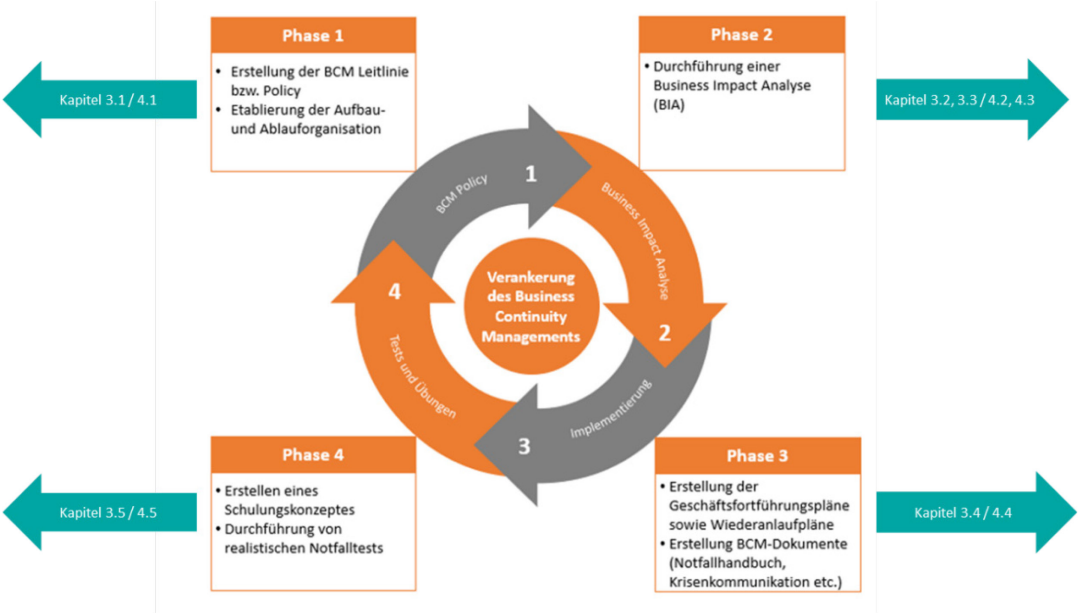

Abbildung 1: Die vier Phasen des BCM-Lebenszyklus mit Verweisen auf die Kapitel des Berichts

Die «Richtlinie zum Business Continuity Management»[7] ist für das EFD sowie sein Generalsekretariat und seine VE verbindlich. Sie schreibt vor, dass die VE für den Aufbau eines BCM zuständig sind und einen BCM-Verantwortlichen mit den erforderlichen Kompetenzen ernennen. Dieser Auftrag zusammen mit den Verantwortlichkeiten und Tätigkeiten muss in der Stellenbeschreibung des BCM-Beauftragten festgehalten sein. Die Leitungen der VE verabschieden jährlich einen Bericht zum Stand der Umsetzung des BCM zuhanden der Koordinationsstelle für BCM-Fragen. Diese rapportiert im Rahmen des jährlichen Risiko-Reportings die Umsetzungsstände an die Generalsekretärenkonferenz (GSK).

2.2 Geschäftsprozesse beeinflussen die Anforderungen

Nicht jede VE hat dieselben Ansprüche an ein BCM. Diese ergeben sich im Wesentlichen aus ihrer Geschäftstätigkeit. Dabei steht die Frage nach den gesetzlichen Aufgaben und Zielen der VE, den Erwartungen der Kunden, Geschäftspartner und der Gesellschaft im Vordergrund. Daraus leiten sich der Kern der Organisation ab, ihre Prozesse und die daraus resultierenden Produkte und/oder Dienstleistungen. Es ist daher für die Organisationen notwendig, Zusammenhänge zwischen den Prozessen zu erkennen und daraus eine Gewichtung des BCMS herzuleiten. Die Organisation sollte hierzu Kriterien festlegen. Mithilfe dieser kann sie ihre kritischen Elemente bestimmen, die im Falle einer Störung prioritär und anhand von vorbereiteten Plänen wieder funktionsfähig gemacht werden müssen. Die Business Impact Analyse (BIA) identifiziert mittels unternehmensspezifisch festgelegter Bewertungskriterien die kritischen Geschäftsprozesse. Dafür wird der Ausfall eines Geschäftsprozesses als Annahme zugrunde gelegt und ermittelt, ab wann der Schadensverlauf über die betrachteten Zeitperioden eine definierte Toleranzgrenze überschreitet. Nur die kritischen Geschäftsprozesse sollen über eine Notfallkonzeption abgesichert werden.

[7] Gestützt auf Artikel 37 des Regierungs- und Verwaltungsorganisationsgesetzes (SR 172.010), Stand Mai 2017

Die Anforderungen des BAZG hinsichtlich der Verfügbarkeit kritischer Geschäftsprozesse und Anwendungen liegt aufgrund der festgelegten Ansprüche im Bereich von Stunden. Die ESTV hingegen kann wegen ihrer Geschäftstätigkeit einen jährlichen Unterbruch von maximal 20 Tagen ohne das Einleiten sofortiger BCM-Massnahmen verkraften. Daraus lässt sich ableiten, dass die Anforderungen an das BCM beim BAZG wesentlich umfangreicher und detaillierter sein müssen. Angesichts dieser unterschiedlichen Voraussetzungen macht ein direkter Vergleich der Maturitäts-Level der beiden VE keinen Sinn.

3 Bundesamt für Zoll und Grenzsicherheit

Mit rund 4500 Mitarbeitenden im In- und Ausland trägt das BAZG zu Sicherheit und Schutz der Bevölkerung, des Staates und der Wirtschaft bei. Das BAZG ist in sechs Direktionsbereiche (DB) mit unterschiedlichen Aufgaben gegliedert.

Der Bereich des BCM ist im DB «Planung und Steuerung» angesiedelt. Es wird als eine der vier Disziplinen (RM, BCM, Business Process Management [BPM] und internes Kontrollsystem [IKS]) im integrierten Risikomanagement als Teil des Controllings bearbeitet. Dieser erarbeitet die Grundlagen zur Erfüllung der Kernaufgaben des BAZG und unterstützen die Mitarbeitenden im Einsatz bei der Aufgabenausübung.

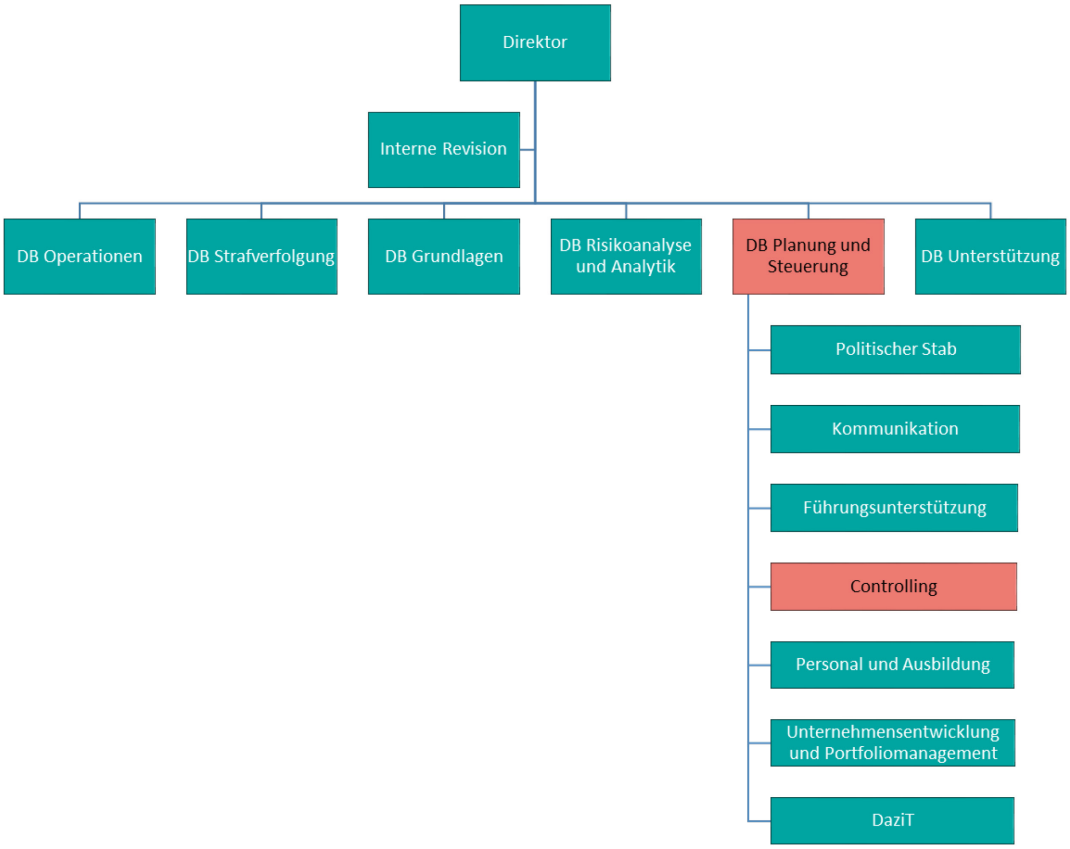

Abbildung 2: Organisatorische Angliederung des BCM im BAZG

3.1 Die Maturität des BCM ist auf einem erfreulichen Stand

Das BCM des BAZG ist strikt nach dem Standard ISO 22301 aufgebaut. Die praktische Umsetzung erfolgt nach dem Vorbild des Handbuchs «BSI 200-4»[8] des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI).

Die Dokumente sind detailliert, aktuell und von der Geschäftsleitung formell abgenommen und eine Änderungskontrolle ist in den Dokumenten ersichtlich. Die Aufgaben, Kompetenzen und Verantwortungen sind beschrieben und den entsprechenden Rollen zugewiesen.

[8] https://www.bsi.bund.de/

Die Aktualisierung erfolgt mindestens jährlich und wird durch den Business Continuity Manager in Absprache mit den Vertretern der unterschiedlichen Geschäftsfelder wahrgenommen. Das BCMS wird einem kontinuierlichen Verbesserungsprozess (KVP) unterworfen. Es werden regelmässige Schulungen, Übungen und Tests der Wiederanlaufverfahren durchgeführt, ausgewertet und die Erkenntnisse in den KVP-Prozess integriert. Im Intranet und mittels einer Wiki-Software[9] werden die aktuellen Dokumentationen und Detailinformationen (kritische Prozesse, Abhängigkeiten, Systemumgebungen, Ressourcen) stufengerecht den Mitarbeitenden zur Verfügung gestellt. Die Plattformen dienen zudem der Krisenorganisation, um im Notfall ihre Aufgaben effizient wahrnehmen zu können. Die nachfolgenden Grafiken zeigen die Maturität[10] des BCM im BAZG anlässlich der Prüfung 16564 im Jahr 2016 (Abbildung 3) und anlässlich der vorliegenden Prüfung (Abbildung 4).

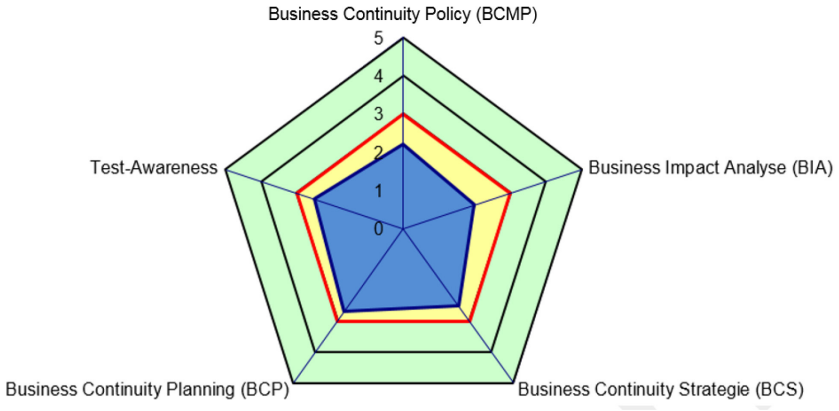

Abbildung 3: Übersicht der Maturitäts-Level in den fünf Prüfbereichen (Stand 2016)

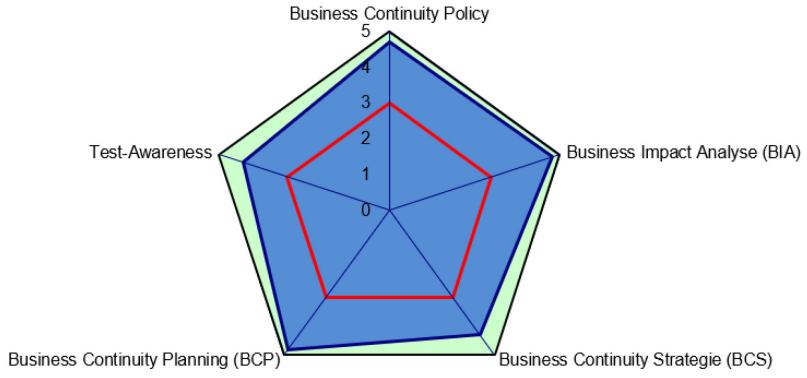

Abbildung 4: Übersicht der Maturitäts-Level in den fünf Prüfbereichen (Stand 2022)

Die geplanten Arbeiten zur Erweiterung und laufenden Verbesserung (Erhöhung der Maturität) des BCMS sind in einer Mehrjahresplanung festgehalten. Darin ist auch ersichtlich, dass das BAZG eine ISO-Zertifizierung des BCM im Jahr 2025 anstrebt. Die Direktion des BAZG informierte das Departement über den Stand der Umsetzung des BCM anhand der jährlichen Selbstdeklaration im November 2021. Der Erfüllungsgrad weist bis auf den Bereich «Test-Awareness» einen Wert zwischen 60 % und 100 % auf. Durch den Aufbau des

9 Wiki-Software: Webbasierte Software, für den internen Wissensaustausch in einer Organisation

10 Darstellung der erreichten Maturität in den Teilbereichen des BCM (rote Linie: von der EFK festgelegter Mindestwert von 3, blaue Fläche: Gesamterreichungsgrad; Beschreibung der Maturitätsstufen in Anhang 4)

BCMS in den letzten Jahren und durch die pandemiebedingten Anpassungen der Arbeitsformen und der eingeschränkten Ressourcensituation konnten im Bereich «Test-Awareness» die geforderten und geplanten Aktivitäten noch nicht umgesetzt werden.

Beurteilung

Das BAZG hat seit 2016 erhebliche Fortschritte in Bezug auf den Reifegrad des BCMS gemacht. Über alle Bereiche konnte der geforderte Minimalwert überschritten werden. Das BCMS ist weiter im Aufbau und unterliegt einem steten Verbesserungsprozess. Entscheidend ist nun, dass die Arbeiten konsequent weiterverfolgt werden, um die Funktionalität im operativen Betrieb sicherzustellen. Hierfür ist es unabdingbar, dass die Pläne anhand verschiedener Tests und Übungen erprobt werden.

Aufgrund der Entwicklung ist die EFK mit der Erledigung der Empfehlung 16504.001 einverstanden, sie kann somit geschlossen werden.

3.2 Kritische Geschäftsprozesse sind angemessen adressiert

Eine BIA ist in der Version 1.0 vorhanden und formell durch die Geschäftsleitung (GL) abgenommen. Die Vorlage hierfür wurde vom EFD entwickelt und dient als Meldeformular an das RM des Departements. Auf einer Wiki-Plattform werden die Grunddaten aus der departementalen Vorlage mit zahlreichen weiteren Informationen verknüpft. So sind den kritischen Geschäftsprozessen unter anderem die Ressourcen, Dokumentationen und Service Level Agreements (SLA) hinterlegt. Künftig sollen diese Informationen in eine Datenbank überführt werden, um die Inhalte granulärer und stufengerechter auswerten zu können.

Die Basis für die Risikoanalyse umfasst zwölf Ereignisse, deren Eintrittswahrscheinlichkeit vom Bundesamt für Bevölkerungsschutz (BABS) als sehr realistisch eingestuft wird. Diese werden in einer Matrix möglichen Szenarien gegenübergestellt. Für jedes Szenario werden Massnahmen definiert. Dabei werden die Punkte Notbetrieb, Vollbetrieb, Reputation, Finanzen und Vorgaben unter verschiedenen Gesichtspunkten bewertet. Zweimal pro Jahr werden die Risiken mit den Risiko-Eignern besprochen. Die Lage wird analysiert und allenfalls werden die Dokumente und Prozesse angepasst. Aus dem RM-Prozess findet eine Risikominderung durch die Umsetzung von präventiven Massnahmen statt.

Beurteilung

Eine fundierte BIA ist die Grundvoraussetzung für ein erfolgreiches BCM. Das BAZG hat erhebliche Aufwände in die Ausarbeitung der BIA investiert. Die Verknüpfung von Ereignissen und Szenarien erlaubt eine präzise Beurteilung der erforderlichen Massnahmen und unterstützt die Planung der Ressourcen und deren Priorisierung.

Die enge Verknüpfung mit dem unternehmensweiten RM stellt sicher, dass die kritischen Geschäftsprozesse durch angemessene präventive und reaktive Massnahmen bestmöglich geschützt werden. Durch die periodischen Neubeurteilungen ist sichergestellt, dass auf externe und interne Einflüsse angemessen reagiert werden kann.

Die EFK erachtet die getroffenen Analysen und Massnahmen als zielführend und für die Organisation als angemessen.

3.3 Viele Aspekte der Business-Continuity-Planung gehören beim BAZG zum Tagesgeschäft

Die Planung ist im BCM-Handbuch sehr detailliert beschrieben. Für die kritischen Prozesse sind die erforderlichen Massnahmen zur Reduktion von möglichen Auswirkungen beschrieben und im operativen Betrieb weitgehend umgesetzt. Die minimal benötigen personellen und materiellen Ressourcen sind definiert und die Infrastrukturen werden periodisch auf deren Funktionalität überprüft.

Notfall- und Krisenmanagement

Im Handbuch zum BCM des BAZG sind neben den präventiven Massnahmen auch die Reaktion beim Eintreten eines Ereignisses beschrieben. Mittels wöchentlich stattfindenden Lagerapporte werden in Zusammenarbeit mit dem Nachrichtendienst des Bundes (NDB) und dem Bundesamt für Polizei (fedpol) die aktuelle Lage ermittelt und allfällige proaktive Massnahmen getroffen. In einem Eskalationsmodell sind über fünf Stufen (Normalbetrieb → Katastrophe) unter anderem die Störungsart und die zuständige Organisation definiert. Der Alarmierungsprozess beschreibt in drei Schritten die Erkennung und Alarmierung, die Einstufung der Ereignismeldung und die Triage, ob es sich um eine Störungsmeldung oder Krisensituation handelt. Bei Letzterer entscheidet der diensthabende Einsatzleiter, ob der Krisenstab aktiv werden muss. Der Anhang 4 der «Geschäftsordnung der Eidgenössische Zollverwaltung (GO-EZV)» vom 6. August 2018 (in Überarbeitung) beschreibt die wesentlichen Elemente der Krisenorganisation, -kommunikation (inkl. externe Kommunikation) und der Ausbildung der Stabsmitarbeitenden. Die Ausbildung lehnt sich an die Lehrmittel des Schweizerischen Polizei-Instituts und ist allen Mitarbeitenden stufengerecht zugänglich.

Beurteilung

Durch die operative Funktion des BAZG sind Stabsarbeit und Notfallmanagement im Tagesgeschäft prominent. Im Rahmen der periodischen Lagerapporte werden Entschlüsse gefasst und allfällige Massnahmen definiert. Aufgrund der ausserordentlichen Lage im Zusammenhang mit der Pandemie leistete der Krisenstab des BAZG in den vergangenen zwei Jahren einen erheblichen Einsatz. Aus diesem wurden laufend Lehren gezogen, die wiederum in den KVP eingeflossen sind.

Grundsätzlich ist das BAZG im Bereich des Business-Continuity-Plans (BCP) sehr umfangreich dokumentiert und durch zahlreiche «Ernstfälle» auch entsprechend eingespielt.

3.4 Übungskonzepte müssen erprobt werden

Das Übungs- und Testkonzept ist ausführlich im BCM-Handbuch beschrieben. Die Übungs- bzw. die Testarten geben an, um welche Art der Prüfung es sich handelt und welches Ziel erreicht werden soll. In einer Tabelle werden die unterschiedlichen Übungsobjekte und -ziele sowie die erforderlichen Ressourcen und die Termine festgehalten. Die Planung, Abläufe und Ergebnisse der Übungen werden dokumentiert. Handlungen und Vorgänge, welche sich im Verlauf der Übung als untauglich oder fehlerhaft herausstellen, werden dokumentiert. Im Anschluss an die Übungen werden diese ausgewertet und allfällige Massnahmen zur Beseitigung der Mängel erarbeitet. Die Massnahmen werden durch den Bereich Integriertes Risikomanagement (IRM) überwacht und fliessen im Rahmen der jährlichen Überarbeitung des BCMS in die Jahresplanung ein. Die Jahresplanung 2022 für BCM-Übungen und Tests liegt vor. Diese Planung ist die Grundlage für alle BCM-Tests beim BAZG.

Die Schulung der MA des BAZG erfolgt stufengerecht. Die Mitarbeitenden des BAZG durchlaufen eine Grundausbildung, diese soll die Begrifflichkeiten und das Verhalten vermitteln. Je nach Rolle ist der Ausbildungsbedarf grösser und daher auch die obligatorischen Schulungen umfangreicher. Das Schulungskonzept definiert die Themen, Module, Inhalte und das Vorgehen, um angepasste, qualitative und termingerechte Ausbildungen aller involvierten Mitarbeitenden zu erreichen. Jeweils im dritten Quartal des Jahres wird eine Jahresplanung für die Schulungen erstellt. Diese enthält eine auf die BAZG-Aktivitäten und je Disziplin individuell erstellte Planung. Diese erfolgt in Zusammenarbeit mit dem Fachdienst und den Koordinatoren. Das Ziel ist, die Verfügbarkeit der Ressourcen sowie der Teilnehmenden und Ausbildenden aufeinander abzustimmen.

Evakuierungsübung

Mitte Mai 2022 wurde im Rahmen einer BCM-Übung die erste Evakuierung am neuen Standort in Bern durchgeführt. Diese basierte auf dem Standardmodell des Bundessicherheitsdienstes (BSD). Die primären Ziele der Übung konnten erreicht werden und die Evakuierung des Personals erfolgte ohne Zwischenfälle. Die Auswertung der Übung hat verschiedene Verbesserungsmassnahmen aufgezeigt, die mittelfristig umgesetzt werden sollen. Eine wesentliche Änderung betrifft die Rolle der Stockwerkverantwortlichen. Durch die neuen mobilen Arbeitsformen ist heute nicht mehr sichergestellt, dass die für die Evakuierung zuständigen Mitarbeitenden auch anwesend sind. Das BAZG setzt daher künftig auf Eigenverantwortung und wird die Mitarbeitenden generell in den Belangen der Evakuierung und der früheren Aufgaben der Stockwerkverantwortlichen ausbilden. Wenige Spezialisten sollen im Bedarfsfall gezielt für Aufgaben wie Sammelplatz- oder Evakuierungschef eingesetzt werden.

Beurteilung

Die besten Konzepte und Schulungen zeigen ihre Wirkung erst, wenn das Gelernte erprobt wird. Es ist daher unerlässlich, jährliche Übungen in den verschiedenen Bereichen und den Anspruchsgruppen durchzuführen. In den vergangenen Jahren wurden beim BAZG lediglich Übungen zur Evakuierung des Standortes vorgenommen. Diese wurden gut dokumentiert, es wurden auch Lehren daraus gezogen und Massnahmen festgelegt.

Die Wichtigkeit der regelmässigen Übung hat das BAZG erkannt, die Massnahmen zur Schulung und zum Training sind in einer Mehrjahressplanung verankert. Aus diesem Grund verzichtet die EFK hier auf eine Empfehlung.

3.5 Für kritische Anwendungen sind Ersatzprozesse vorgesehen

Elektronische Zolldeklaration «e-dec»

In «e-dec» (Electronic Declaration) deklarieren die Zollbeteiligten Waren für den Import und Export. Die Deklaration erfolgt entweder über den «e-dec»-Service oder über eine Webanwendung. Zu den Benutzern der Anwendung gehören Zollanmelder, Zollfachpersonen und Umsysteme. Die Benutzer befinden sich in und ausserhalb der Bundesverwaltung. Die Applikation wird beim BIT betrieben.

Das Notfallhandbuch beschreibt die Notfallplanung und Katastrophenvorsorge für das System «e-dec», um die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten. In erster Linie ist ein reibungsloser Ablauf

für die Warenein- und -ausfuhr sicherzustellen. Dabei ist die Einfuhr generell höher zu gewichten, da diese Einnahmen generiert und kein anderes System zur Verfügung steht. Bei der Ausfuhr hingegen stellt ein zweites System eine weitere Möglichkeit dar, um Exporte deklarieren zu können. Bei längeren Unterbrüchen wird das Notfallverfahren für das Weiterführen der Geschäftstätigkeiten ausgelöst.

Dabei wird auf einen manuellen Betrieb umgestellt. Dies erfordert grössere personelle Ressourcen. Nach der Behebung der Störung müssten alle in Papierform generierten Unterlagen im System nacherfasst werden. Auch dies stellt einen erheblichen Aufwand dar. Das Notfallverfahren liegt in der Hoheit des BAZG und wird nach dessen Ermessen angewendet.

Einsatzleitsystem «ELS»

Die Einsatzzentralen (EZ) des BAZG koordinieren und unterstützen die Mitarbeitenden an der Grenze bei ihrer Tätigkeit und bereiten Informationen für die Einsatz- und Führungsunterstützung auf. Das Einsatzleitsystem «ELS» unterstützt die Einsatzzentralen in der Erbringung ihrer Kernleistungen. Das «ELS» ist redundant aufgebaut, mit insgesamt vier Servern, wovon je zwei immer den Backup übernehmen.

Fallen die Systeme dennoch aus, können die primären Aufgabe nicht mehr wahrgenommen werden. Der Pikettoffizier entscheidet über die Initialisierung von BCM-Massnahmen. Es ist genau definiert, wie ohne das System gearbeitet werden soll. Bei einem Ausfall werden eingehende Meldungen in einem Journal erfasst und nach den verbleibenden Möglichkeiten behandelt. Dauert der Ausfall länger, kann (sofern verfügbar) eine andere EZ die Aufgabe temporär übernehmen. Bei einem Standortausfall besteht die Möglichkeit auf einen Ausweichstandort mit zwei Arbeitsplätzen auszuweichen. Dieser ist getestet und immer betriebsbereit. Die Kommunikation wird über Polycom[11] sichergestellt.

Beurteilung

Den hohen Anforderungen an die Verfügbarkeit der Systeme wird Rechnung getragen. Die Systemlandschaften sind mehrfach aufgebaut und gewähren so eine hohe Betriebsbereitschaft. Zudem sind für beide Prozesse alternative Vorgehensweisen vorhanden, welche den Betrieb bei einem Systemausfall regeln. Die Notfallorganisation stellt einen kurz- bis mittelfristigen Betrieb sicher, dieser ist jedoch mit einem höheren Ressourcenbedarf verbunden.

Dass die EZ für eine beschränkte Dauer die Aufgaben einer anderen Region übernehmen können und auch innerhalb der Regionen Ausweichstandorte vorhanden und erprobt sind, ist aus Sicht der EFK angemessen.

[11] Polycom ist das nationale Funksystem der Behörden und Organisationen mit Sicherheitsaufgaben.

3.6 Sicherheits- und BCM-Anforderungen sollen in die agile Projektwelt integriert werden

Mit dem Programm «DaziT» vereinfacht das BAZG bis Ende 2026 den Geschäftsverkehr mit den Bürgern und Unternehmen grundlegend. Dabei werden die Zoll-, Abgabenerhebungs- und Kontrollprozesse vereinfacht, optimiert und digitalisiert. Dies führt zu einer Gesamttransformation auf allen Ebenen der Organisation. Die Digitalisierung soll die neuen Geschäftsprozesse vereinfachen, sie wird aber auch die Abhängigkeiten von den IT-Systemen deutlich erhöhen. Die EFK hat 2020 eine DTI-Schlüsselprojektprüfung[12] dieses Digitalisierungsvorhaben durchgeführt und in diesem Kontext eine Empfehlung ausgesprochen.

Durch die agile Projektabwicklung und Programmierung sind die klassischen, phasenbedingten Sicherheitsüberprüfungen bzw. -freigaben nicht mehr praktikabel. Dennoch ist es von grosser Wichtigkeit, dass die Anforderungen hinsichtlich der IKT-Sicherheit und des BCM bereits in der Planung und Entwicklung neuer Systeme berücksichtigt werden. Dabei zeigt sich die Implementierung der BCM- und Sicherheitsanforderungen in den Entwicklungsprozess als Herausforderung. Das BAZG hat eine Methodik zur systematischen Einbindung der Anforderungen und der Überwachung von deren Wirkung entwickelt. Zum Prüfzeitpunkt fanden erste Gespräche zwischen den Vertretern des BCM und dem Projektteam statt.

Beurteilung

Die EFK begrüsst das Vorgehen einer frühzeitigen Integration der Sicherheits- und BCM-Anforderungen in den Projekten. Nur so kann eine durchgängige und nachhaltige Resilienz der Anwendungen und Systeme erreicht werden. Es ist unabdingbar, dass die verschiedenen Aspekte der IKT-Sicherheit berücksichtigt werden und die Anspruchsgruppen über den gesamten Entwicklungszyklus in engem Austausch stehen. Das BAZG verfolgt mit dem geplanten Vorgehen einen zielführenden Ansatz.

[12] Der Bericht zur «Prüfung des IKT-Schlüsselprojektes DaziT» (PA 20287) ist auf der Website der EFK abrufbar (www.efk.admin.ch).

4 Eidgenössische Steuerverwaltung

Zum Zuständigkeitsbereich der ESTV gehören sämtliche Arten von Steuern. Diese umfassen sowohl die Mehrwertsteuer als auch die direkte Bundessteuer, die Verrechnungssteuer und sonstige Abgaben des Bundes. Sie setzt die Doppelbesteuerung im Steuerbereich um, leistet internationale Amtshilfe in Steuerangelegenheiten, kassiert staatsvertraglich vereinbarte Quellensteuern für andere Staaten und erstellt Steuerstatistiken.

Mit den rund 1200 Mitarbeitenden beschafft die ESTV den Grossteil der Bundeseinnahmen und spielt eine unentbehrliche Rolle bei der Finanzierung von öffentlichen Aufgaben. Sie sorgt für eine rechtsgleiche und effiziente Erhebung aller Arten von Steuern und Abgaben.

Die ESTV erstellt die Erlasse im Bereich des Steuerrechts und gewährleistet mit den Kantonen zusammen die formelle Harmonisierung der direkten Steuern von Bund, Kantonen und Gemeinden.

Das Risikomanagement und das BCM sind im Direktionsstab angegliedert.

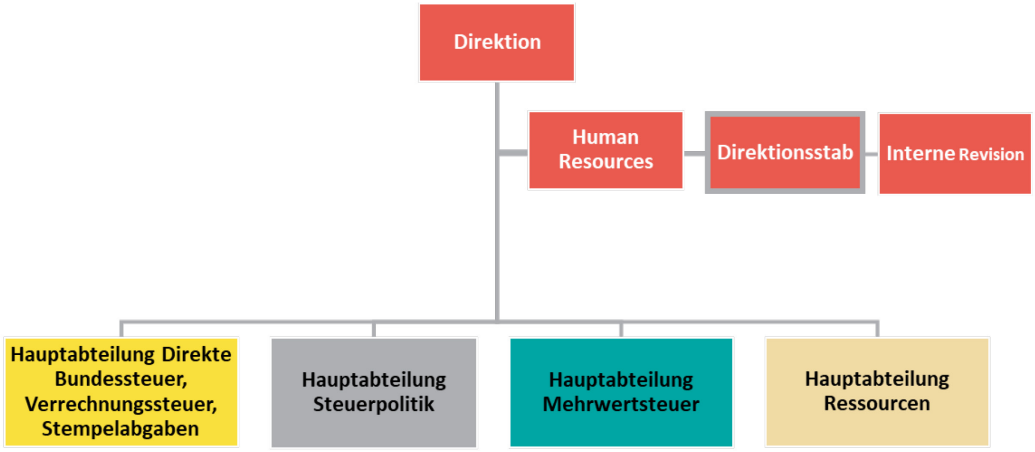

Abbildung 5: Organisatorische Angliederung des BCM in der ESTV

4.1 Wesentliche Fortschritte wurden erzielt, weitere Arbeiten sind noch zu leisten

Das BCM der ESTV ist nach dem Standard ISO 22301 aufgebaut. Die BCM-Dokumente sind aktuell und von der Geschäftsleitung genehmigt. Die Dokumente sind teilweise generisch gehalten, insbesondere die BIA. Aufgaben, Kompetenzen und Verantwortungen sind beschrieben und den entsprechenden Rollen zugewiesen. Eine Grobplanung sieht vor, die Aktualisierung der BCM-Strategie durch den Risikocoach in einem Turnus von fünf Jahren grundlegend zu überarbeiten. Die nächste Aktualisierung soll 2023 erfolgen. Die Dokumente und Schulungsunterlagen stehen den Mitarbeitenden im Intranet zur Verfügung.

Die Aktualität der übrigen BCM-Unterlagen soll jährlich überprüft und bei Bedarf angepasst werden. Die vorgefundenen Unterlagen stammten jedoch aus dem Jahr 2019. Das Risikoupdate wird durch den Leiter Qualitätssteuerung zweimal pro Jahr durchgeführt. Allfällige Änderungen sind in den halbjährlich verfassten Controlling Berichten ersichtlich. Es fehlt zwar eine formelle Prozessbeschreibung für das BCM und die Überarbeitung der Dokumente, aber die Elemente für eine regelmässige Aktualisierung sind vorhanden.

In der Selbstdeklaration zum Stand des BCM meldet die ESTV dem Departement 2019 einen Erfüllungsgrad von 100 % über alle Disziplinen. Seither erfolgten keine Meldungen mehr.

Die nachfolgenden Grafiken zeigen die Maturität[13] des BCM in der ESTV anlässlich der Prüfung 16564 im Jahr 2016 (Abbildung 6) und anlässlich der vorliegenden Prüfung (Abbildung 7).

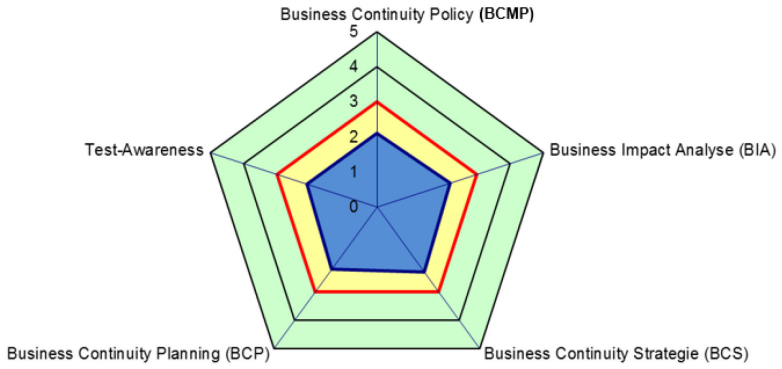

Abbildung 6: Übersicht der Maturitäts-Level in den fünf Prüfbereichen (Stand 2016)

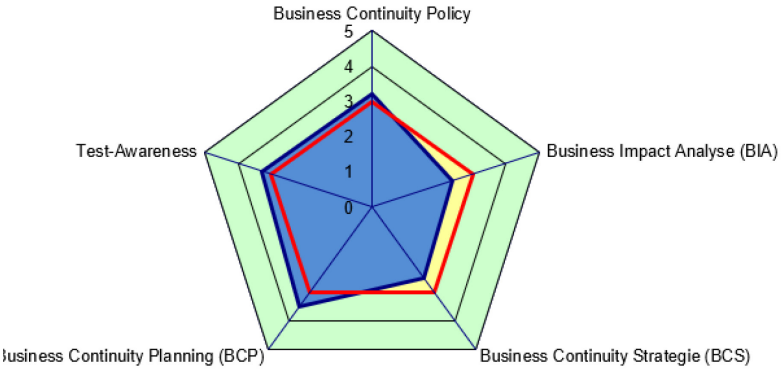

Abbildung 7: Übersicht der Maturitäts-Level in den fünf Prüfbereichen (Stand 2022)

Im Vergleich zur Prüfung von 2016 konnte in allen Bereichen eine Steigerung des Reifegrades erreicht werden. Das BCM der ESTV entspricht weitgehend den departementalen Vorgaben sowie dem ISO-Standard. In den Teilbereichen BIA und BCS besteht noch Handlungsbedarf (siehe Kapitel 4.2).

Beurteilung

Die Entwicklung des BCM bei der ESTV hat wesentliche Fortschritte erzielt und die Empfehlung 16564.002 ist umgesetzt. Die geforderten Dokumente sind vorhanden, jedoch fehlen teilweise wichtige Informationen oder sie sind nicht aktuell. Zum Prüfzeitpunkt wurden bereits ausgetretene Mitarbeitende noch in Dokumenten aufgeführt. Dies wurde durch die ESTV noch während der Prüfung korrigiert.

[13] Darstellung der erreichten Maturität in den Teilbereichen des BCM (rote Linie: von der EFK festgelegter Mindestwert von 3, blaue Fläche: Gesamterreichungsgrad; Beschreibung der Maturitätsstufen in Anhang 4)

Die ESTV sollte die Aktualisierung resp. Überarbeitung der BCM-Dokumente stärker überwachen. In Anbetracht der bevorstehenden Überarbeitung 2023 sieht die EFK von einer Empfehlung ab.

Die halbjährliche Neubeurteilung der Risiken und die Erhebung der daraus resultierenden Massnahmen erachtet die EFK als zielführend. Die Sensibilisierungs- und Schulungsmassnahmen werden den Mitarbeitenden stufengerecht vermittelt.

4.2 Die Sicherheitsstrategie muss überarbeitet werden

Die BIA ist Bestandteil des Dokumentes zur BCM-Strategie. Die kritischen Prozesse und Ressourcen sind definiert, jedoch fehlt eine Priorisierung. Auch werden nicht alle aufgeführten Prozesse in der Umsetzungsplanung weiterbehandelt. Prozesse und Ressourcen werden ohne differenzierte Beschreibung der Kritikalität in den Dokumenten aufgeführt. Wiederkehrende präventive und detektive Massnahmen sind festgehalten.

Die Risiken und Ereignisse werden als Szenarien in der Business-Continuity-Strategie aufgeführt. Diese sind generisch gehalten und beziehen sich ausschliesslich auf monetäre Aspekte. Eine Auswirkungsanalyse zu jedem kritischen Kernprozess existiert nicht.

Beurteilung

Die BIA entspricht noch nicht in allen Punkten den Anforderungen aus der Richtlinie des EFD respektive dem ISO 22301. Es fehlen die Auswirkungen über die Zeit, die maximal tolerierbaren Ausfallszeiten, die Zeit bis zur Wiederherstellung des normalen Levels sowie die Priorisierung. Nur durch diese Angaben kann eine Organisation sicherstellen, dass sie über angemessene Mittel und Massnahmenpläne verfügt, um ihre kritischen Prozesse aufrechtzuerhalten bzw. wiederherzustellen.

Kritisch eingestufte Geschäftsprozesse müssen zwingend in der BIA beschrieben und in der BCP weiterbehandelt werden. Dies beinhaltet unter anderem die Auswirkungsanalyse pro Kernprozess und die Priorisierung der kritischen Ressourcen und Prozesse in Bezug auf eine Wiederherstellung bei einem Ausfall.

Die BIA stellt die Basis für die Sicherheitsstrategie dar und sollte daher mit einer hohen Aufmerksamkeit behandelt werden.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt der ESTV, die Business–Impact-Analyse gemäss den Anforderungen des Departements zu überarbeiten. Insbesondere müssen die als kritisch eingestuften Geschäftsprozesse konsequent behandelt werden.

Die Empfehlung ist akzeptiert.

Stellungnahme der ESTV

Die ESTV wird die BIA im Jahr 2023 gemäss Empfehlung überarbeiten und die darauf basierenden weiteren Dokumente (Strategie und Planung) entsprechend aktualisieren. Es wird zudem ein Änderungsprozess definiert und damit die periodische Aktualisierung der Dokumente überwacht und dokumentiert.

4.3 Die Planung weist noch Lücken auf

Die ESTV hat einen Plan für das Management der Geschäftskontinuität eingeführt. Er beschreibt die Umsetzung von präventiven, unmittelbaren und strategischen Massnahmen im Detail. In diesem Plan werden unter anderem die verschiedenen Rollen, Ressourcen und Fristen sowie die Prozesse festgelegt. Hingegen fehlt ein Hinweis auf die Dokumente mit den detaillierten Informationen über die Sicherheit von Personen oder Sofortmassnahmen zur Sicherung kritischer Ressourcen, wie Gebäude, Personal, Informatik usw.

Die ESTV hat vier Szenarien und deren spezifische Gegebenheiten beschrieben. Für jedes Szenario wird eine Reihe von Sofort- sowie strategischen Massnahmen nach dem Auftreten eines aussergewöhnlichen Ereignisses definiert. Das Szenario «Cyber-Kriminalität» befindet sich noch in der Entwicklung.

Notfall- und Krisenmanagement

Die Krisen- und Katastrophenorganisation KKO ist im Rahmen der BCP dokumentiert und die erforderlichen Ressourcen stehen bereit. Während einer Krise steht ein Primärraum mit erforderlicher Ausrüstung sowie bei Bedarf ein Sekundärraum zur Verfügung. Neben der üblichen Stabsarbeit ist der Krisenstab verantwortlich, die Geschäftsleitung rechtzeitig und in hoher Qualität mit den für die Bewältigung der Krise notwendigen Informationen zu versorgen. Sofern Notfallmassnahmen ergriffen werden, konzentriert sich die ESTV auf die kritischen Geschäftsprozesse und bindet die verantwortlichen Personen eng ein. Um sicherzustellen, dass im Krisenfall alles reibungslos abläuft, werden die Mitarbeitenden regelmässig geschult.

Beurteilung

Die Planung für das Management der Geschäftskontinuität ist gut strukturiert und enthält weitergehend die erforderlichen Informationen. Die kritischen Geschäftsprozesse sind festgehalten und Sofortmassnahmen festgelegt.

Die Krisenorganisation und -infrastruktur sind zweckmässig aufgebaut. Die Stabsmitarbeitenden kennen ihre Aufgaben und Verantwortlichkeiten und konnten im vergangenen Jahr durch eine Übung (siehe Kapitel 4.4) und durch die pandemiebedingte ausserordentliche Lage Erfahrungen sammeln.

Schulungen und Sensibilisierungsmassnahmen für das Personal werden mittels unterschiedlicher Medien sichergestellt. Dies ist essenziell, um das Personal auf dem aktuellsten Stand zu halten.

4.4 Ein Übungskonzept und eine Mehrjahresplanung fehlen

Sämtliche Informationen und Schulungsunterlagen zum BCM stehen den Mitarbeitenden der ESTV auf einer Intranetseite zur Verfügung. Die Inhalte werden dabei teilweise durch Videos vermittelt. Wichtige Informationen, beispielweise zur Evakuierung, werden zudem als Faltblatt ausgehändigt. Darüber hinaus wird an internen Veranstaltungen über aktuelle BCM-Themen informiert.

Die ESTV verfügt über kein Übungs- und Testkonzept, auch fehlt eine mittel- bis langfristige Planung von Übungen. Einzelne Übungen werden situationsabhängig und nach Schwerpunktthemen, in Absprache mit dem Direktor und der Geschäftsleitung festgelegt. Dies war

beispielsweise 2019 der Fall, als die Krisen- und Katastrophenorganisation (KKO) eine Stabsübung durchführte. Hierfür liegt ein detailliertes Konzept mit dem Szenario «Cyberangriff» vor. Der Übungsablauf wurde festgehalten und verschiedene Erkenntnisse führten zu Massnahmen. Deren Umsetzung wurde den verantwortlichen Rollen zugewiesen. In den darauffolgenden zwei Jahren konnte die KKO während der Pandemie wertvolle Erfahrungen sammeln und es wurden verschiedene Verbesserungsmassnahmen festgehalten.

Evakuierungsübung

Im Frühling 2022 wurde nach einer sechsjährigen Pause eine Evakuationsübung am Standort Eigerstrasse 61/65 durchgeführt. Die Übung verlief ruhig und geordnet und das Gebäude konnte innert Minuten evakuiert werden. Die Übungsziele wurden weitgehend erreicht und der Schlussbericht weist ein positives Resultat aus. Aus Sicht der BCM-Massnahmen haben sich aber gewisse Mängel gezeigt. So wurden beispielsweise Notebooks teilweise in den Räumlichkeiten zurückgelassen, was ein Weiterarbeiten ausserhalb des Gebäudes verunmöglicht hätte. Die Evakuierungsübung wurde vom Bereich Logistik geplant, durchgeführt, ausgewertet und analysiert. Die Berichterstattung erfolgte in Zusammenarbeit mit dem Bereich RM.

Beurteilung

Die Sensibilisierungs- und Schulungsmassnahmen der ESTV sind stufengerecht und zweckmässig. Die Vermittlung der Inhalte erfolgt auf verschiedenen Kanälen und mittels unterschiedlicher Medien. Die EFK erachtet die Massnahmen im Bereich der Kommunikation als zielführend.

Das Testkonzept für die Stabsübung der KKO weist einen angemessenen Detaillierungsgrad auf. Auch die Auswertung und die getroffenen Massnahmen sind für die Weiterentwicklung der Funktionalität der Organisation von grosser Bedeutung. Hingegen gibt es kein generisches Testkonzept, das beispielsweise die Strategie, die unterschiedlichen Übungs- und Testarten, die Anspruchsgruppen sowie die Vor- und Nachbereitung regelt. Um sicherzustellen, dass in einem regelmässigen Turnus alle Bereiche des BCM geübt werden, ist eine längerfristige Planung erforderlich.

Evakuierungsübungen dienen der Sicherheit der Mitarbeitenden und müssen regelmässig und an allen Standorten einer VE durchgeführt werden. Mit der letzten Übung wurde diese Thematik von der ESTV nach längerer Pause wiederaufgenommen. Durch die fehlende Rollen- bzw. Aufgabentrennung bei der Übungsorganisation kann die Unabhängigkeit der Beurteilung nicht sichergestellt werden. Mindestens die Rolle des Übungsleitenden muss durch eine Person wahrgenommen werden, die nicht aktiv an der Übung teilnimmt.

Empfehlung 2 (Priorität 2)

Die EFK empfiehlt der ESTV, ein generisches BCM-Testkonzept zu erstellen, das mindestens die Strategie, die unterschiedlichen Übungs- und Testarten, die Anspruchsgruppen, die Funktionstrennung sowie die Vor- und Nachbereitung regelt. Eine Planung der Tests und Übungen für die nächsten Jahre sollte dabei Bestandteil des Konzepts sein.

Die Empfehlung ist akzeptiert.

Stellungnahme der ESTV

Die ESTV wird im Sinne der Empfehlung im Jahr 2023 sowohl ein generisches BCM-Testkonzept als auch eine mehrjährige Übungs-Planung erarbeiten.

4.5 Längere Systemausfälle sind verkraftbar

DIFAS

Das Fachanwendungssystem DIFAS bündelt alle fachlichen und allgemeinen Funktionen zur Unterstützung der Mitarbeitenden der Hauptabteilung «Direkte Bundessteuer, Verrechnungsteuer, Stempelabgaben» bei der Vorbereitung und Bearbeitung der relevanten Geschäftsfälle. Die Funktionen von DIFAS werden auf einer Dokumentenmanagement-Plattform bereitgestellt und mithilfe der technischen Fähigkeiten «Geschäftsfallverwaltung», «Dokumentenmanagement» und «Workflowmanagement» zum grossen Teil auch dort erbracht. Die übrigen Funktionen werden, für die Anwender transparent, von Nachbarsystemen erbracht, wie etwa die Kundenbuchhaltung, die Verwaltung der Partnerstammdaten und eGovernment-Anwendungen.

MEFAS

MEFAS stellt die zwei Hauptfunktionen Dossier- und Pendenzenverwaltung im Bereich Mehrwertsteuer zur Verfügung. MEFAS bildet mit den Komponenten Dokumenten- und Casemanagement, sowie dem System für die Fachfunktionalitäten, die zentralen Systeme für die Geschäftsverwaltung der Mehrwertsteuer. Alle anderen Funktionen und Daten werden in Nachbarsystemen gehalten und über Schnittstellen ausgetauscht.

Für MEFAS und DIFAS sind Dokumentationen und Architekturskizzen vorhanden. Redundanzen sind nicht vorhanden. Nach Ausfällen sollen Backups der virtuellen Maschinen und der Datenbanken innerhalb von acht Stunden wiederhergestellt werden können. Nach der Wiederherstellung wird die Konfiguration überprüft und es werden Funktionstests durchgeführt. Es gibt keine Notfallpläne seitens der ESTV, falls die Anwendungen nicht innerhalb von acht Stunden wiederhergestellt werden kann. Sollte dies der Fall sein, würde die Situation analysiert und entsprechende Massnahmen ergriffen.

Notfallpläne zur Weiterarbeit ohne Systeme sind nicht vorhanden. Der Betrieb kann ohne diese Systeme nicht mehr gewährleistet werden. Jedoch ist der Zeitfaktor für beide Prozesse wenig kritisch, da ein längerer Ausfall aus Sicht der ESTV in Kauf genommen werden kann.

Beurteilung

Die Anwendungen MEFAS und DIFAS sind zweckmässig dokumentiert und die Abhängigkeiten der Systeme sind ersichtlich. Die heutige Anwendungsarchitektur weist generell keine Redundanzen auf und somit können Störungen unmittelbar zu Arbeitsunterbrüchen führen. Die ESTV plant eine Studie zur Implementierung einer redundanten Architektur. Die EFK begrüsst dieses Vorgehen.

Bei einem längeren Systemausfall helfen Notfallpläne, wichtige Geschäftsprozesse weiterzuführen. Für beide Systeme sind keine Pläne für alternative Betriebsabläufe definiert. Die EFK kann dies nachvollziehen, da einerseits ein «manueller» Betrieb unverhältnismässig aufwendig wäre und andererseits eine längere Ausfalldauer von der ESTV akzeptiert wird.

5 Backup-Verwaltung BIT: Sicherheit und Betrieb der Anwendung «NetBackup»

Die Marktleistung «Backup und Recovery» des BIT schützt vor Datenverlust und ermöglicht das Wiederherstellen von Informationen. Das Backup wird auf speziell dafür vorgesehenen, in sich abgeschlossenen Speichersystemen erstellt und verbleibt dort. Eine Auslagerung von Speichermedien ist im Basisangebot nicht vorgesehen.

Mit der Option «Backup-Kopie» kann daher eine zusätzliche und identische Kopie des Backups an einem tertiären und sicheren Standort erstellt werden. Die zusätzliche Backup-Kopie stellt sicher, dass auch bei einem Total- oder Teilausfall der Rechenzentren alle notwendigen Daten für einen Wiederanlauf, ein sogenanntes Disaster Recovery, zur Verfügung stehen.

Bei einem Datenverlust kann für die Wiederherstellung der Daten auf die letzte gültige Sicherung zurückgegriffen werden. Bei der Wiederherstellung von Systemen und Datenbanken kann mithilfe der zusätzlich erstellten Sicherungskopien der Stand bis zum letzten Sicherungszyklus wiederhergestellt werden.

Die Verantwortung für die erforderliche Datensicherung ist Sache des Leistungsbezügers (LB), dies beinhaltet auch die Wahl der entsprechenden Marktleitung.

5.1 Die Sicherheit ist angemessen, der Schutz von Malware muss priorisiert werden

Eine angemessene Sicherheit und Resilienz sind sichergestellt

Die Sicherungssoftware «NetBackup» ist georedundant in den Rechenzentren (RZ) «PRIMUS» und «CAMPUS» aufgebaut. Um die Integrität der Daten sicherzustellen, ist ein Integritätsmonitor im Einsatz. Dieser prüft nach der Übertragung mittels einer Checksumme, ob die Daten unverändert übermittelt wurden. Damit wird eine fehlerfreie Synchronisation zwischen den Standorten überwacht und sichergestellt. Bei einer fehlerhaften Übertragung wird der Vorgang automatisch wiederholt. Nach mehreren gescheiterten Versuchen wird das zuständige Team automatisch alarmiert und kann entsprechend intervenieren. Bei den täglich generierten 40 000 – 60 000 Backups liegt die Fehlerquote unter einem Prozent.

Die Anwendung «NetBackup» verfügt über eine Möglichkeit, Daten bei der Sicherung zu verschlüsseln. Diese wird aktuell jedoch nur im Bereich der digitalen Zertifikate (Public-Key-Infrastruktur) und dem Logdatensammler des BIT eingesetzt. Die Verschlüsselung der Daten wird in der Marktleistung «Backup und Recovery» grundsätzlich nicht angeboten. Daher müssen die sensiblen Daten in der jeweiligen Herkunftsapplikation verschlüsselt werden.

Beurteilung

Durch die konstante Synchronisierung der Daten und der georedundanten Speicherung ist die Verfügbarkeit der Daten sichergestellt. Die Prüfung der Daten mittels des Integritätsmonitors ist aus Sicht der EFK zweckmässig.

Die Vertraulichkeit der Daten liegt in der Verantwortung des Leistungsbezügers. Die Marktleistung stellt nur die fehlerfreie Sicherung und zeitgerechte Wiederherstellung der Informationen sicher. Entsprechend ist der Leistungserbringer (LE) auch nicht für die Sicherstellung der Vertraulichkeit der Daten zuständig. Aus Sicht der EFK ist dieses Vorgehen legitim, da es in der Marktleistung nicht angeboten wird.

Der Schutz vor Ransomware muss verbessert werden

Ein wichtiger Aspekt ist der Schutz der Backups gegen Verschlüsselungstrojaner, sogenannte Ransomware. Dabei muss sichergestellt werden, dass keine mit Ransomware verseuchten Inhalte gesichert werden. Sollte dies trotzdem geschehen, besteht das Risiko, dass bei einer Wiederherstellung der Daten die Ransomware erneut installiert wird.

Die Problematik ist dem BIT bewusst und die Erarbeitung eines Backup- und Restore-Konzepts unter dem Aspekt Ransomware soll die künftige Behandlung der Datensicherung regeln. Ein externes Assessment ist geplant und soll Aufschluss über mögliche Ansätze geben.

Die heute im Einsatz stehende Softwareversion hat bereits gewisse Funktionalitäten, die den Schutz vor Ransomware erhöhen könnte. Unter anderem bietet sie eine Erkennung von Anomalien an, um Daten schneller und effizienter zu verarbeiten und abnormale Ereignisse, Änderungen in Datensätzen zu erkennen. Diese Anomalieerkennung stützt sich auf künstliche Intelligenz. Ziel ist, eine Vorwarnung vor einem Ransomware-Ereignis zu erhalten. Des Weiteren ist ein Malware-Scanner zum Scannen von Backup-Images auf dem Mediaserver vor der Integration der Daten ins Backup verfügbar.

Es ist zu beachten, dass bei den Servern des BIT regelmässige Verwundbarkeitsscans durchgeführt werden. Zudem verfügen alle Windows sowie die meisten Linux-Server bereits über einen Virenschutz.

Beurteilung

Da Ransomware eine der häufigsten Bedrohungen darstellt, begrüsst die EFK die Absicht des BIT, ein externes Gutachten zu Verbesserungen des Schutzes der Datensicherungen durchzuführen. Die Arbeiten sollten entsprechend rasch in Auftrag gegeben werden. Die Ergebnisse sollten danach genutzt werden, um eine Verbesserung der Resilienz gegen Ransomware in der BV herzustellen. Des Weiteren sollte ein auf den Massnahmen aufgebautes Backup- und Restore-Konzept erarbeitet werden.

Die Erhöhung der Softwareversion und damit die Nutzung der zusätzlichen Sicherheitsfunktionen ist zielführend. Dabei ist zu klären, welchen Mehrnutzen der zusätzliche Virenscan von «NetBackup» gegenüber den bereits installierten Virenscannern auf den Quellsystemen bietet.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt dem BIT, zeitnah weitere geeignete Massnahmen zum Schutz vor Ransomware zu implementieren.

Die Empfehlung ist akzeptiert.

Stellungnahme des BIT

Im Zuge der aktuell laufenden Arbeiten für die Implementation einer Offline-Backup Lösung werden auch Themen wie Erkennung von Ransomware-Befall im Datenstrom / Backup angegangen. In einem Workshop mit den entsprechenden Spezialisten wird ein dem NIST-

Standard (National Institute of Standards and Technology) angelehnte Gesamt-Lösung erarbeitet. Diese beinhaltet auch die Möglichkeit, einen Ransomware-Befall frühzeitig zu erkennen und bei Bedarf auch wieder auf einen sauberen Stand zurück zu fahren. Diese Lösung wird die bereits implementierten Viren- und Ransomware-Schutzmassnahmen auf allen vorgelagerten Stufen wie Netzwerk / Server um eine Erkennung auf Ebene Datenströme / Backup erweitern.

Zusammen mit dem Offline-Backup ergibt dies ein Gesamtpacket zur allgemeinen Verbesserung der Sicherheit und zur Umsetzung des NIST-Standards.

Anfang 2023 soll dazu ein PoC aufgebaut werden und parallel dazu werden die Mittel für die (schrittweise) Umsetzung nacherfolgreichem PoC beantragt.

Eine Offline-Backup-Strategie muss noch erstellt werden

Gemäss «Si001 – IT-Grundschutz in der Bundesverwaltung[14]» muss die verantwortliche VE über eine Backup-Strategie verfügen und diese auch umsetzen. Diese Strategie muss ein Mehrgenerationen-Prinzip und eine Offline-Speicherung wichtiger Datenbestände vorsehen, sodass Daten auch im Falle von datenverschlüsselnder Malware wiederhergestellt werden können. Diese Version des IT-Grundschutzes ist seit März 2022 in Kraft und die Umsetzung unterliegt einer Übergangsfrist. Im Rahmen des Life Cycles eines Schutzobjekts oder aber spätestens innerhalb von fünf Jahren muss die Anforderung umgesetzt werden.

Das BIT muss die Marktleistung entsprechend anpassen und definieren in welcher Form Offline-Kopien angeboten werden können. Dabei stehen verschiedene Varianten zur Auswahl. «NetBackup» verfügt über eine Funktion, bei der eine Kopie der Backups auf den Laufwerken ist, jedoch nicht erreicht werden kann (Soft-Offline). Offen ist, ob dies reicht, um die Anforderungen des IT-Grundschutzes zu erfüllen.

Nach der klassischen Definition der Offline-Backups auf abgeschotteten Systemen müsste das BIT erst die erforderlichen Ressourcen aufbauen. Das BIT macht dies jedoch nicht proaktiv, sondern wartet die Nachfrage der VE ab.

Die Aspekte der Offline-Sicherungen muss auch Gegenstand des zu überarbeitenden Backup- und Restore-Konzepts sein.

Beurteilung

Grundsätzlich ist die Erstellung einer Backup-Strategie gemäss IT-Grundschutz Sache des LB.

Der Grundschutz ist erst seit März 2022 in Kraft und es ist nicht genauer spezifiziert, was unter den Begriff Offline-Backup fällt. Die LB und LE haben also einen gewissen Spielraum bei der Erarbeitung ihrer Backup-Strategien. Ungeachtet dessen muss ein LE über eine Strategie verfügen, diese kann von den LB akzeptiert und für ihre Anwendungen übernommen werden.

Das BIT muss die Marktleistung Offline-Backups definieren und den Ressourcenbedarf planen. Es ist nachvollziehbar, dass zum heutigen Zeitpunkt und ohne messbaren Kundenbedarf noch keine Investitionen getätigt werden.

Aus diesem Grund verzichtet die EFK auf eine Empfehlung ans BIT.

[14] https://intranet.ncsc.admin.ch/ncscintra/de/home/vorgaben-hilfsmittel/sicherheitsverfahren/grundschutz.html

Unbenutzte Konten müssen gelöscht werden

Der Zugriff auf die Administration der Sicherungsumgebung ist zum Prüfzeitpunkt auf das siebenköpfige «Backup- und Storage»-Team beschränkt. Dieses deckt sowohl den Betrieb, das Engineering und auch den Support ab. Aufgrund des kleinen Kreises von Administratoren wurde darauf verzichtet, ein Rollenkonzept zu erstellen. Mit der Einführung der neuen Version von «NetBackup» beabsichtigt das BIT, ein Rollenkonzept einzuführen und den Administratoren mehr Rechte zu gewähren.

Im Rahmen der Prüfhandlungen wurde festgestellt, dass zwei der konfigurierten Accounts nicht mehr gebraucht wurden. Diese wurden durch das BIT umgehend entfernt.

Beurteilung

Bei insgesamt sieben Administratoren eines Systems ist ein Rollenkonzept nicht zwingend erforderlich. Trotzdem müssen die Accounts aktuell gehalten werden. Insbesondere dürfen keine ungenutzten Konten mit privilegierten Rechten auf den Systemen vorhanden sein. Werden weitere Benutzer mit zusätzlichen und unterschiedlichen Rechten Zugriff haben, ist es umso wichtiger die Zugriffe kontrolliert zu vergeben und ein Rollenkonzept wird zwingend. Nicht benötigte Accounts müssen erkannt und umgehend gelöscht werden. Da eine Ausweitung der Zugriffsberechtigten und der Rollen zum Zeitpunkt der Prüfung nicht geplant ist, verzichtet die EFK auf eine Empfehlung.

Service Level Agreements regeln die Anforderungen an die Datensicherung

Die Anforderungen zur Sicherung und Wiederherstellung der Daten ist in den SLA geregelt. Die Einhaltung dieser ist jedoch von der Menge der wiederherzustellenden Daten abhängig. Die Restriktionen dafür sind nicht im Factsheet «Backup und Recovery», sondern in den entsprechenden SLA der Applikationen mittels der Verfügbarkeitsklassen (VK) geregelt. So ist zum Beispiel im Factsheet «ORACLE DB Enterprise» festgehalten, dass eine maximale Ausfallzeit von acht Stunden pro Ausfall (VK2) nur angeboten werden kann, wenn die Datenmengen nicht grösser als 4 Terabyte (TB) sind. Wird diese Limite überschritten, sind die Applikationsverantwortlichen der LB in der Pflicht, kompensierende Massnahmen zu planen. Diese sind beispielsweise redundante Systeme und Datenbanken oder die längere Wiederherstellungszeit wird formell akzeptiert.

Das Spektrum der SLA wird vom BIT bewusst klein gehalten, um mit standardisierten Verträgen den betrieblichen Aufwand in Grenzen zu halten. Bei Bedarf können jedoch zusätzliche Vereinbarungen getroffen werden. Neue Anforderungen können zudem im Rahmen der regelmässig durchgeführten Sitzungen des IKT-Gremiums «Führung Standarddienste» beantragt werden.

Das BIT stellt die Verfügbarkeit der Backups sicher. Die Anwendung «NetBackup» wurde im Dezember 2020 im RZ «CAMPUS» während eines Restore-Tests gemäss Wiederanlaufplan vollständig wiederhergestellt. Ein weiterer Restore-Test des RZ «CAMPUS» war für Juni 2022 geplant, wurde jedoch auf den September 2022 verschoben. Ziel ist es, danach auch einen kompletten Restore-Test im RZ «PRIMUS» durchzuführen. Hierfür gibt es ein Testkonzept und eine Teststrategie. Flächendeckende Restores aller Applikationen, die mit «NetBackup» gesichert sind, werden vom BIT nicht durchgeführt. Pro Jahr werden drei bis vier Applikationen ausgewählt und davon testweise eine Wiederherstellung geübt. Die Applikationsverantwortlichen der LB können jedoch einen Restore ihrer Anwendungen beauftragen. Diese werden dann entsprechend durchgeführt, dokumentiert und verrechnet.

Im täglichen Betrieb wird zum Aktualisieren der Software laufend zwischen den verschiedenen Standorten und Umgebungen umgeschaltet. Zudem werden Redundanz-Tests durchgeführt. Diese Tests sind immer angekündigt und werden im Changemanagement geplant.

Beurteilung

Die Gestaltung der SLA mit den entsprechenden Factsheets und VK weist den Umfang der Leistungen nicht auf den ersten Blick transparent aus. Mittels weiterer Factsheets kann jedoch festgestellt werden, ab wann beispielsweise VK nicht mehr eingehalten werden können. Allerdings ist es in diesem Fall den Applikationsverantwortlichen überlassen sicherzustellen, dass sie die richtigen Massnahmen ergreifen. Die Möglichkeit, zusätzliche Anforderungen zu stellen oder gesonderte Vereinbarungen abzuschliessen, wird wenig genutzt.

Der durchgeführte Restore-Test im RZ «CAMPUS» ist aus Sicht der EFK sinnvoll und sollte periodisch wiederholt werden. Nur so kann sichergestellt werden, dass bei einem Vorfall alles wie geplant in den Normalbetrieb überführt werden kann.

Die vom BIT durchgeführten jährlichen Restore-Tests von Applikationen erachtet die EFK im Vergleich zur Gesamtmenge der Backups als gering. Der LB trägt jedoch die Verantwortung für seine Anwendungen und kann bei Bedarf für diese solche Tests bestellen.

Aus diesen Gründen verzichtet die EFK hier auf eine Empfehlung.

5.2 Die redundante Architektur erlaubt eine hohe Verfügbarkeit

Sicherung und Wiederherstellung der Anwendung «e-dec»

Gemäss dem SLA beträgt die maximale Ausfallzeit für «e-dec» vier Stunden. Die Systeme sind in zwei synchronisierten Umgebungen in zwei georedundanten Rechenzentren aufgebaut. Da zwischen den Umgebungen und Rechenzentren bei Softwareaktualisierungen regelmässig umgeschaltet wird, besteht laut LE keine Notwendigkeit für weitere Tests. Sollten beide Rechenzentren ausfallen, würden die vier Stunden aufgrund der Datenmenge jedoch nicht reichen, um das System in der vereinbarten Zeit wiederherzustellen. Dies ist dem BAZG bewusst und mitigierende Massnahmen sind geplant (siehe Kapitel 3.5).

Beurteilung

Da die Anwendung «e-dec» redundant in verschiedenen Rechenzentren aufgebaut ist und zwischen den Umgebungen regelmässig umgeschaltet wird, ist ein kontinuierlicher Betrieb sichergestellt. Nur mittels Restore-Tests kann sichergestellt werden, dass das gesamte System von Grund auf wiederaufgebaut werden kann. Zudem würde so ersichtlich, wie lange ein Unterbruch tatsächlich dauern würde. Das System befindet sich in der Ablösungsphase und angesichts der Aufwände und Risiken eines solchen Tests verzichtet die EFK hier auf eine Empfehlung.

Sicherung und Wiederherstellung der Anwendung «ELS»

Auch bei der Anwendung «ELS» beträgt die maximale Ausfallzeit gemäss SLA vier Stunden. Bei «ELS» wurde eine Abnahmeumgebung aufgebaut, die identisch zur Produktionsumgebung ist. Das System ist redundant aufgebaut mit insgesamt vier Servern, wovon je zwei immer den Backup übernehmen. Jeden Monat erfolgt ein Update, wobei bei zwei Servern

ein Neustart erfolgt und gleichzeitig die beiden anderen automatisch übernehmen. Dieses redundant aufgebaute Konstrukt dient als Failover-Test und wird beim BIT protokolliert, aber nicht spezifisch ausgewiesen.

Mit dem BIT wurde eine Dienstleistungsvereinbarung (DLV) erstellt, um Restores durchzuführen. Das BAZG bestellt beim BIT den Restore und danach wird eine Kopie der Produktionsumgebung auf der Abnahmeumgebung installiert. Dies wird als Change erfasst und entsprechend aufgezeichnet. Die Wiederherstellungen finden zirka alle drei Monate statt. Dabei werden die vereinbarten Wiederherstellungszeiten eingehalten.

Beurteilung

Durch den Aufbau einer identischen Abnahmeumgebung und der Redundanzen innerhalb der Systeme kann sichergestellt werden, dass auch die Produktionsumgebung innerhalb der gewünschten Zeit wiederhergestellt werden kann. Die abwechselnden Aktualisierungen der Systeme und der damit verbundenen Neustarts entsprechen implizit einem Failover-Test. Die Architektur und die regelmässige Durchführung der Restore-Tests sind hinsichtlich der Verfügbarkeit aus Sicht der EFK zielführend.

5.3 Die Wiederherstellungszeiten können nicht garantiert werden

Sicherung und Wiederherstellung der Anwendungen «DIFAS» und « MEFAS»

Bei beiden Anwendungen beträgt die maximale Ausfallzeit gemäss SLA acht Stunden. Es finden keine Wiederherstellungstests statt. Die Systeme der ESTV laufen alle auf einer Basisinfrastruktur, die auf unterschiedlichen Komponenten aufgebaut ist. Auf diesen Systemen erfolgen regelmässige Wiederherstellungstests. Die Tests werden mit der Anwendung SUFAS gemacht, die ähnlich funktioniert wie «MEFAS» und «DIFAS». Gemäss Einschätzung des BIT dauert die Wiederherstellung von DIFAS etwa vier Stunden. Bei MEFAS sind die Datenbanken zu gross, um sie in acht Stunden wieder einzuspielen.

Die Core-IT ist aktuell nicht redundant aufgebaut. Falls das RZ oder das Netzwerk ausfallen sollte, sind die Systeme nicht mehr erreichbar. Dies wurde gemäss BIT so mit der ESTV besprochen und akzeptiert. Eine Redundanz ist aber generell erwünscht und ist im Rahmen der geplanten Erneuerung der Basisinfrastruktur angedacht.

Beurteilung

Das praktizierte Vorgehen der Wiederherstellungstests mit einem ähnlichen System, jedoch mit einer kleineren Datenbank ist nachvollziehbar. Trotzdem muss sichergestellt werden, dass im Rahmen eines Komplettausfalls alle Anwendungen wiederhergestellt werden können. Die Möglichkeit, auf der Abnahme- und Referenzumgebung Wiederherstellungen zu üben, ist gemäss EFK zielführend, falls diese Umgebungen und Schnittstellen analog der Produktion aufgebaut sind.

Da die Basisinfrastruktur nicht redundant aufgebaut ist, besteht beim Ausfall eines Rechenzentrums oder des Netzwerks keine Möglichkeit, die Systeme wiederherzustellen, bis das RZ wieder operativ oder das Netzwerk wieder erreichbar ist. Entsprechend ist die ESTV in dieser Zeit nicht in der Lage ihre Leistungen zu erbringen. Die geplante Einführung von Redundanz bei der anstehenden Erneuerung der Basisinfrastruktur ist nach Ansicht der EFK zielführend. Die EFK verzichtet daher auf eine Empfehlung.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2018), SR 614.0
Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV), vom 27. Mai 2020 (Stand am 1. April 2021), SR 120.73
Vorgaben und Richtlinien
Si001 – IT-Grundschutz in der Bundesverwaltung (Version 5.0) vom 1. März 2022
Richtlinie zum Business Continuity Management (BCM) des EFD vom 1. Juli 2017

Anhang 2: Abkürzungen

BABS	Bundesamt für Bevölkerungsschutz
BAZG	Bundesamt für Zoll und Grenzsicherheit
BCM	Business Continuity Management (Betriebliches Kontinuitätsmanagement)
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analyse
BIT	Bundesamt für Informatik und Telekommunikation
BPM	Business Process Management
BSD	Bundessicherheitsdienst
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
DB	Direktionsbereiche
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
ESTV	Eidgenössische Steuerverwaltung
EZ	Einsatzzentrale
fedpol	Bundesamt für Polizei
GL	Geschäftsleitung
GSK	Generalsekretärenkonferenz
IKS	Internes Kontrollsystem
IRM	Integriertes Risikomanagement
ISO/IEC	International Organization for Standardization
KKO	Krisen- und Katastrophenorganisation
KVP	Kontinuierlicher Verbesserungsprozess

LB	Leistungsbezüger
LE	Leistungserbringer
NDB	Nachrichtendienst des Bundes
RM	Risikomanagement
RZ	Rechenzentrum
SLA	Service Level Agreement
TB	Terabyte
VE	Verwaltungseinheit(en)
VK	Verfügbarkeitsklasse(n) (siehe Glossar)

Anhang 3: Glossar

NetBackup	«NetBackup» ist eine Cloud-optimierte Datensicherungslösung der Firma Veritas.
Ransomware	Ransomware sind Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln.
Verfügbarkeitsklasse(n)	Die Verfügbarkeit wird in vier Klassen (VK0 – VK3) unterteilt. Der LB kann zwischen den Verfügbarkeitsklassen auswählen, die den jeweiligen Marktleistungen zugeordnet sind. Die Werte pro Verfügbarkeitsklasse sind vorgegeben und aufeinander abgestimmt.

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

Anhand des Fragenkatalogs zu den Disziplinen Policy, BIA, BCS, BCP und Test-Awareness wurde der Reifegrad der einzelnen Themen ermittelt und daraus eine Gesamtbeurteilung des BCM abgeleitet. Die Bewertung erfolgt sowohl aufgrund des Reifegrades als auch der Ja/Nein-Antworten zu den einzelnen Bereichen. Die Bewertungsskala beginnt bei 0 (nicht existent) und endet bei 5 (optimiert). Kann eine Aussage mit «Ja» oder «Nein» beantwortet werden, so ergibt «Ja» einen Wert von 5 und «Nein» den Wert 0.

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 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 eine ständige 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.