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

Prüfung des Business Continuity Managements im Leistungsbereich Betrieb

Bundesamt für Informatik und Telekommunikation

EFK-16150 / inkl. Stellungnahmen / 13. September 2016

Impressum

Bestelladresse **Adresse de commande** **Indirizzo di ordinazione** **Order address**	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45, CH - 3003 Bern http://www.efk.admin.ch
Bestellnummer **Numéro de commande** **Numero di ordinazione** **Order number**	1.16150.609.00215.006
Zusätzliche Informationen **Complément d'informations** **Informazioni complementari** **Additional information**	E-Mail: info@efk.admin.ch Tel. +41 58 463 11 11
Originaltext **Texte original** **Testo originale** **Original text**	Deutsch Allemand Tedesco German
Zusammenfassung **Résumé** **Riassunto** **Summary**	Deutsch (« Das Wesentliche in Kürze ») Français (« L'essentiel en bref ») Italiano (« L'essenziale in breve ») English (« Key facts »)

Prüfung des Business Continuity Managements im Leistungsbereich Betrieb Bundesamt für Informatik und Telekommunikation

Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) hat geprüft, ob der Leistungsbereich Betrieb (BTR) des Bundesamtes für Informatik und Telekommunikation (BIT) über alle wesentlichen Krisensituationen die Kerngeschäfte seiner Kunden gemäss vertraglichen Vereinbarungen sicherstellen kann. Insgesamt haben der BTR und das BIT mit ihren Vorkehrungen im Falle einer Krise einen guten Eindruck hinterlassen. Werkzeuge, Prozesse und Dokumente ermöglichen eine systematische und kontrollierte Wiederherstellung des Normalbetriebes nach einem Vorfall.

Die Geschäftsleitung hat nach zwei schwerwiegenden Vorfällen in den Jahren 2011 und 2013 das Business Continuity Management (BCM) auf Stufe Amt in Form einer Politik und Strategie geregelt. Die möglichen Ausfallszenarien sind kategorisiert und die Krisenorganisation festgelegt worden. Daraus ergeben sich für den BTR die Rahmenbedingungen innerhalb derer die präventiven Massnahmen definiert werden müssen. Der BTR arbeitet grundsätzlich serviceorientiert nach ITIL[1]. Entsprechend ist die Reaktion auf Störungen bzw. der Wiederanlauf über das IT Service Continuity Management (ITSCM) geregelt. ITSCM ist im Gesamtkontext des BCM BIT ein Teil des Business Continuity Planning (BCP). Sobald eine Störung (Incident) nicht mehr innerhalb eines einzigen Fachbereichs gelöst werden kann, wird zum Major Incident (MI) eskaliert. Ein verantwortlicher MI-Manager übernimmt damit die Koordination und Überwachung der Aktivitäten zur Behebung des Vorfalles bis dieser abgeschlossen werden kann. Treten weitere Schwierigkeiten auf, so wird zusätzlich eine Task Force eingesetzt. Diese ist bevollmächtigt, bereichsübergreifend Fachspezialisten abzuziehen, um bei der Lösung der Probleme mitzuhelfen. In beiden Fällen ist das BIT als Amt immer noch im Normalbetrieb. Erst wenn auch die Task Force keine zeitgerechte Lösung für ein aufgetretenes Problem finden kann, wird der Direktor des BIT bzw. dessen Stellvertreter den Krisenmodus BCM auslösen.

Die Checklisten oder Abläufe sind teilweise noch nicht ganz vollständig, die Termine zur Beendigung der Arbeiten jedoch gesetzt. Verbesserungspotenzial sieht die EFK bei der Vollständigkeit der Testszenarien. Eine grössere Übung hat zwar im Mai 2016 anlässlich eines Kaderworkshops stattgefunden. Was fehlt ist die mehrjährige Planung von weiteren Tests, damit alle Bereiche im mittelfristigen Turnus abgedeckt werden können. Die EFK hat eine entsprechende Empfehlung abgegeben.

[1] IT Infrastructure Library ist eine Sammlung von vordefinierten und standardisierten Prozessen, Funktionen und Rollen, wie sie typischerweise in jeder IT-Infrastruktur von mittleren und grossen Unternehmen vorkommen.

Audit de la gestion de la continuité des affaires au sein de la division Exploitation Office fédéral de l'informatique et de la télécommunication

L'essentiel en bref

Le Contrôle fédéral des finances (CDF) a examiné si la division Exploitation de l'Office fédéral de l'informatique et de la télécommunication (OFIT) est en mesure d'assurer l'essentiel des activités de ses clients lors de situations de crise majeures, selon les dispositions contractuelles. Dans l'ensemble, les mesures en cas de crise prévues par la division et l'OFIT ont fait bonne impression. Les divers outils, processus et documents garantissent le retour systématique et contrôlé à la normale après un incident.

Après deux incidents graves en 2011 et en 2013, la direction a réglé la gestion de la continuité des affaires (*Business Continuity Management*) au niveau de l'office en adoptant une politique et une stratégie. Les scénarios de panne envisageables ont été classés par catégories et l'organisation de crise a été définie. Ces données fixent le cadre dans lequel la division Exploitation doit appliquer les mesures préventives. La division axe en principe son travail sur les prestations fournies selon l'ITIL[1]. La réaction face à une panne ou la relance du système est par conséquent régie par la gestion de la continuité des services informatiques (*IT Service Continuity Management*). Cette dernière fait partie intégrante du plan de continuité des affaires (*Business Continuity Planning*) de l'OFIT. Dès qu'une panne (*Incident*) ne peut plus être gérée par une seule unité, elle devient un incident majeur (*Major Incident*). Un gestionnaire d'incident majeur assume alors la coordination et la surveillance des activités afin de remédier à la panne jusqu'à ce que l'incident soit clos. Si d'autres difficultés surviennent, une task force est en outre mise en place. Elle est habilitée à faire appel à des spécialistes de différents domaines pour qu'ils contribuent à résoudre les problèmes. Dans les deux cas, l'OFIT continue de fonctionner normalement. Ce n'est que si la task force ne parvient pas à résoudre le problème à temps que le directeur de l'office ou son suppléant activera le mode «crise» de la gestion de la continuité des affaires.

Certaines listes de contrôle ou procédures ne sont pas encore tout à fait prêtes, mais des délais ont été fixés pour l'achèvement des travaux. Le CDF estime qu'il serait possible d'améliorer les scénarios tests en les complétant. Un vaste exercice a certes été mené en mai 2016 à l'occasion d'un atelier de travail pour les cadres. Cependant, une planification sur plusieurs années fait encore défaut pour assurer, à moyen terme, que tous les domaines soient testés à tour de rôle. Le CDF a formulé une recommandation allant dans ce sens.

Texte original en allemand

[1] IT Infrastructure Library est un ensemble de processus, de fonctions et de rôles prédéfinis et standardisés, dont est typiquement dotée toute infrastructure informatique d'une entreprise moyenne à grande.

Verifica della gestione della continuità operativa nel settore di prestazioni Esercizio Ufficio federale dell'informatica e della telecomunicazione

L'essenziale in breve

Il Controllo federale delle finanze (CDF) ha svolto una verifica per accertare se il settore di prestazioni Esercizio dell'Ufficio federale dell'informatica e della telecomunicazione (UFIT) è in grado di garantire, in situazioni di crisi di considerevole portata, le attività principali dei propri clienti secondo quanto stabilito nei relativi accordi contrattuali. Nel complesso le misure adottate dal settore Esercizio e dall'UFIT in situazioni di crisi hanno incontrato l'approvazione del CDF. Strumenti, processi e documenti permettono di ristabilire in modo sistematico e controllato la normale operatività dopo un incidente.

Dopo due gravi incidenti verificatisi nel 2011 e nel 2013, la direzione dell'UFIT ha istituito il (Business Continuity Management (BCM) a livello di Ufficio, tracciandone la politica e la strategia. Sono stati categorizzati i possibili scenari di incidenti ed è stata definita l'organizzazione in situazioni di crisi. In tal modo il settore Esercizio dispone di condizioni quadro all'interno delle quali occorre definire misure preventive. Il settore oggetto di verifica lavora in modo orientato ai servizi e si attiene all'ITIL[1]. In quest'ottica la reazione agli incidenti e il ripristino della normale operatività vengono regolati sulla base dell'IT Service Continuity Management (ITSCM). Nel contesto generale del BCM dell'UFIT, l'ITSCM è parte integrante del piano di continuità aziendale (Business Continuity Planning, BCP). Se un incidente (Incident) non può essere risolto all'interno di un unico settore specialistico diventa Major Incident (MI). Il manager MI responsabile assume il coordinamento e la supervisione delle attività di risoluzione dell'incidente finché la situazione critica non rientra. In caso di ulteriori difficoltà viene introdotta una task force, incaricata di far intervenire specialisti a livello trasversale per risolvere il problema. In entrambi i casi l'UFIT, in qualità di Ufficio, continua a essere normalmente operativo. Se anche la suddetta task force non è in grado di trovare una soluzione tempestiva al problema, il direttore dell'UFIT o il suo sostituto dichiareranno lo stato di crisi del BCM.

Le liste di controllo e i processi non sono ancora completi, ma sono state fissate delle scadenze entro le quali concludere i lavori. Il CDF ravvisa un potenziale di miglioramento nella completezza degli scenari oggetto dei test. Nel mese di maggio 2016, i quadri dell'UFIT hanno partecipato a una simulazione durante un workshop. Ma manca una pianificazione pluriennale di ulteriori test che permetta di coprire a rotazione e nel medio termine tutti i settori. Il CDF ha formulato una raccomandazione in questo senso.

Testo originale in tedesco

[1] L'IT Infrastructure Library è un insieme di linee guida che raccoglie processi, funzioni e ruoli predefiniti e standardizzati, basati sull'organizzazione prototipica dell'infrastruttura IT di medie e grandi imprese.

Audit of business continuity management in the operations service sector Federal Office of Information Technology, Systems and Telecommunication

Key facts

The Swiss Federal Audit Office (SFAO) checked whether or not the operations service sector of the Federal Office of Information Technology, Systems and Telecommunication (FOITT) can ensure the core business of its customers in all major crisis situations in accordance with the contractual agreements. Overall, the operations service sector and the FOITT made a good impression with their measures in the event of a crisis. Tools, processes and documents allow a systematic and controlled restoration of normal operations after an incident.

After two serious incidents in 2011 and 2013, management regulated business continuity management (BCM) at office level in the form of a policy and strategy. The possible failure scenarios were categorised and the crisis organisation was determined. The framework conditions for the operations service sector within which the preventive measures are defined are derived from this. In principle the operations service sector is service-oriented in accordance with the IT infrastructure library[1]. Accordingly, the response to incidents and restarts are regulated via IT service continuity management (ITSCM). In the overall context of FOITT BCM, ITSCM is part of business continuity planning. As soon as an incident can no longer be resolved within a specialist sector, it is escalated to a major incident (MI). A responsible MI manager takes over so that coordination and monitoring of the activities to resolve the incident can be completed. Should further problems emerge, a task force will be deployed in addition. The task force is authorised to assign experts across units to provide assistance with problem solving. In both cases, the FOITT as an office will still operate normally. Only when the task force cannot find a timely solution for a problem which has occurred will the FOITT director or his deputy trigger the BCM crisis mode.

The checklists and procedures are not yet entirely complete. The deadlines for finishing the work have been set, however. The SFAO sees room for improvement with regard to completing the test scenarios. A major training exercise took place in May 2016 during a management workshop. What is lacking is multiannual planning of further tests so that all sectors can be covered in the medium-term cycle. The SFAO has made corresponding recommendations.

Original text in German

[1] IT infrastructure library is a collection of predefined and standardised processes, functions and roles as they typically occur in every IT infrastructure in medium-sized and large-scale companies.

Generelle Stellungnahme des BIT zur Prüfung:

Das BIT nimmt das Resultat der Prüfung zustimmend zur Kenntnis.

Inhaltsverzeichnis

1	**Auftrag und Vorgehen**	**9**
1.1	Ausgangslage	9
1.2	Prüfungsziel und -fragen	9
1.3	Prüfungsumfang und -grundsätze	9
1.4	Unterlagen und Auskunftserteilung	10
2	**Faktenlage**	**10**
2.1	Gravierende Sicherheitsvorfälle haben zu Aktivitäten geführt	10
2.2	Geschäftsfortführung auf Stufe BIT und Stufe Betrieb	10
2.3	IT Service Continuity Management als Antwort auf die Anforderungen	10
2.4	Tests und Schulungen finden laufend statt	11
2.5	Leistungsbezüger erhalten Unterstützung bei der Erarbeitung ihres BCM	12
3	**Beurteilung**	**12**
3.1	Das BIT hat eine gute Basis geschaffen	12
3.2	Beim Wiederanlauf haben nicht Anwendungen sondern Services Priorität	13
3.3	Trotz guten Noten sind Verbesserungen möglich	13
4	**Schlussbesprechung**	**15**
Anhang 1: Rechtsgrundlagen		**16**
Anhang 2: Abkürzungen, Glossar, Priorisierung der Empfehlungen		**16**
Anhang 3: Maturitätslevel nach Cobit		**17**

1 Auftrag und Vorgehen

1.1 Ausgangslage

Das Bundesamt für Informatik und Telekommunikation (BIT) ist mit über 1100 Mitarbeitenden der grösste interne Leistungserbringer (LE) der Bundesverwaltung. Es betreibt im Auftrag des Informatiksteuerungsorgan des Bundes (ISB) zahlreiche Standarddienste, die von zentraler Bedeutung für die meisten Verwaltungseinheiten (VE) sind. Wichtige Anwendungen von unterschiedlichen Leistungsbezügern (LB) sind ebenfalls dem BIT anvertraut. Der Leistungsbereich Betrieb (BTR), ist für Plattformen, Infrastrukturen und Services verantwortlich. Die LB bestimmen über die vertraglichen Vereinbarungen mit dem BIT, wie hoch die Verfügbarkeitsanforderungen für ihre Daten und Anwendungen sind. BTR ist damit gefordert, diese Dienstleistungen über allfällige Krisenlagen hinweg zu erfüllen.

1.2 Prüfungsziel und -fragen

Die EFK hat überprüft, ob BTR über die wesentlichen Krisensituationen sicherstellt, dass die Kerngeschäfte gemäss vertraglichen Vereinbarungen mit den Kunden gewährleistet werden können. Die grundlegenden Fragen waren:

- Ist klar definiert, welche Kerngeschäfte gemäss vertraglichen Vereinbarungen mit den Kunden gewährleistet werden müssen?
- Besteht eine Auswirkungsanalyse, welche die möglichen Krisenszenarien und deren Auswirkungen darlegt sowie die notwendigen Ressourcen aufzeigt zur Sicherstellung der Kerngeschäfte?
- Steht die für den Betrieb notwendige IT-Infrastruktur im Katastrophenfall innert nützlicher Frist wieder zur Verfügung?
- Besteht ein Kontinuitätsplan zur zeitgerechten Wiederherstellung nach einem Katastrophenfall?
- Gibt es regelmässige Übungen zu den möglichen Krisenszenarien?

Im Weiteren interessierte, ob das BIT seine Kunden bei deren Business Continuity Planning (BCP) bzw. entsprechenden Tests unterstützt.

Die Prüfung hatte nicht das übergeordnete BCM des BIT im Fokus, sondern die Vorkehrungen zur Aufrechterhaltung der Leistungsfähigkeit von BTR, d.h. das IT Service Continuity Management (ITSCM) in der vom BIT angewendeten Terminologie.

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Cornelia Simmen (Revisionsleitung) und Stefan Wagner, IT-Prüfer durchgeführt. Zur Erfüllung des Auftrages wurden Interviews mit Schlüsselpersonen geführt, Prozesse und Dokumente sowie die vorhandenen Überwachungs- und Incident-Management-Systeme beurteilt. Als Basis diente der EFK der Standard ISO-Standard 22301 „Business Continuity Management“.

1.4 Unterlagen und Auskunftserteilung

Die Prüfung fand vom 15. Juni - 7. Juli 2016 statt. Die EFK hat von allen Beteiligten in offener und konstruktiver Art Auskunft erhalten. Die notwendigen Unterlagen standen termingerecht und umfassend zur Verfügung.

2 Faktenlage

2.1 Gravierende Sicherheitsvorfälle haben zu Aktivitäten geführt

Das BIT musste 2011 und 2013 zwei schwerwiegende Störfälle bewältigen. Aufgrund eines Stromunterbruchs fiel beide Male eines der Rechenzentren komplett aus. Die Auswirkungen waren ähnlich gelagert und führten zu längeren Unterbrüchen bei wichtigen Anwendungen. Bereits 2011 war analysiert worden, welche Probleme aufgetreten waren bis zur Rückkehr in den Normalbetrieb. Die danach ergriffenen Massnahmen haben dazu geführt, dass der Wiederanlauf 2013 koordinierter ablief. Es traten jedoch erneut bisher nicht erkannte Schwierigkeiten auf. Die Geschäftsleitung hat daraus die Lehren gezogen. In den letzten 3 Jahren sind die Grundlagen zum Business Continuity Management (BCM) BIT erarbeitet und ein Verantwortlicher für den Unterhalt dieses Regelwerks ernannt worden. Das BCM BIT richtet sich am Standard ISO22301 aus ohne dass eine entsprechende Zertifizierung angestrebt wird.

2.2 Geschäftsfortführung auf Stufe BIT und Stufe Betrieb

Die Geschäftsleitung des BIT hat die Politik und Strategie zum BCM festgelegt. Die Szenarien, welche zu einem Katastrophenfall führen könnten sind dokumentiert. Im Krisenhandbuch sind die Prozesse, Verantwortlichkeiten, Schnittstellen und Logistik festgehalten. Zur Krisenorganisation sind ebenfalls Vorgaben vorhanden. Die Entscheidungskompetenzen und die Kommunikation im Krisenfall sind definiert. Damit sind die Rahmenbedingungen vorhanden, nach welchen sich alle Bereiche des BIT auszurichten haben. Oberstes Ziel ist, dass BTR so weit als möglich Vorkehrungen trifft, damit ein Katastrophenfall auf Stufe BIT erst gar nicht eintrifft. BTR ist der Bereich, welcher den Grossteil des Business Continuity Planning (BCP) BIT bestreitet.

2.3 IT Service Continuity Management als Antwort auf die Anforderungen

Der Bereich BTR antwortet auf die Anforderungen aus den BCM Vorgaben mit einem Vorgehen nach ITIL. Zentral sind dabei die Services, welche zur Verfügung stehen müssen, damit die Gesamtheit der Dienstleistungen erbracht werden kann. Das IT Service Continuity Management (ITSCM) als Prozess von ITIL beinhaltet - ähnlich wie BCM – Anforderungen, Strategie, Planung, Tests, Schulung und Unterhalt. Es ist ein in sich geschlossenes Vorgehen, damit auf Störungen rasch und strukturiert reagiert werden kann. Erhält das Help-Desk BIT Hinweise auf mögliche Probleme oder zeigen die Überwachungssysteme solche an, so wird nach den in der BCM-Strategie vorgegebenen Eskalationsstufen gearbeitet. Kann eine Störung (Incident) durch einen Fachbereich nicht innert definierter Frist behoben werden, so wird zum Major Incident (MI) eskaliert. Dies heisst, dass bereichsübergreifende Aktivitäten erforderlich sind oder ein Potential besteht, dass sich das Problem ausweiten könnte.

Der MI-Manager wird bestimmt und koordiniert bzw. überwacht mit einem eigens dafür vorhandenen Werkzeug die Tätigkeiten der unterschiedlichen Fachbereiche. Die vorbereiteten Krisenräume stellen sicher, dass alle notwendigen Instrumente und Dokumente auch im worst case verfügbar sind. Dazu gehört auch eine Offline-Version des Werkzeuges zur Überwachung der Wiederherstellung. Je nach Lage werden gemäss Masterplan die Stufen des SCM (SCM10-SCM70) systematisch abgearbeitet. Muss bei SCM10 begonnen werden, ist in einem der Rechenzentren die Stromversorgung ausgefallen. SCM70 stellt am Ende aller Aktivitäten sicher, dass alle Anwendungen wieder im Normalbetrieb funktionieren. Dazwischen liegen hunderte von Aktivitäten, welche anhand von Checklisten in allen Fachbereichen von BTR abgearbeitet werden. Sind alle Arbeiten innerhalb einer SCM-Stufe erledigt, so wird diese vom MI Manager mit einer grünen Ampel freigegeben. Erst danach darf mit der nächsten SCM-Stufe begonnen werden. Treten während eines MI zusätzliche Schwierigkeiten auf, so kommt als weitere Eskalationsstufe eine Task Force zum Einsatz. Hier werden dedizierte Spezialisten hinzugezogen, um gezielt an der Lösungssuche mitzuhelfen.

Das beschriebene Vorgehen nach ITSCM ist immer innerhalb von BTR. Nur dieser Bereich hat erstinstanzlich eine Ausnahmesituation, der Rest des BIT läuft im Normalbetrieb weiter, bis BTR fallweise einzelne Bereiche oder Spezialisten beizieht. Die Kunden sind zwar mehr oder weniger von einer Störung betroffen, es liegt jedoch kein Krisenfall BIT vor. Erst wenn auf Stufe Task Force keine Lösung gefunden werden kann, würde der Direktor des BIT bzw. dessen Stellvertretung das ganze Amt in den Krisenmodus versetzen. Unter Krisenführung werden die normalen Geschäftsprozesse und -prioritäten übersteuert. Primäres Ziel ist dabei, das vorhandene Problem zu lösen, damit die Funktionsfähigkeit der Organisation wieder sichergestellt werden kann. Ab Zeitpunkt eines BIT BCM Falles gilt für alle LB das Service Level Element 6 (SLE) „Business Continuity Management“, welches alle vorgängig definierten SLE ausser Kraft setzt. Damit werden die vertraglich vereinbarten Service-, Support-, Wartungs- und Verfügbarkeitszeiten so lange sistiert, bis das BIT wieder in den Normalbetrieb zurückgekehrt ist.

2.4 Tests und Schulungen finden laufend statt

Das unter ITSCM beschriebene Vorgehen wird beim BIT auch eingesetzt um z. B. Patches einzuspielen oder bei Wartungsarbeiten. Es werden dieselben Checklisten abgearbeitet wie bei Vorliegen einer Störung. Dadurch werden einerseits das Vorgehen bzw. die Dokumente auf Aktualität getestet, andererseits üben die Mitarbeitenden dadurch deren Handhabung. Daneben gibt es gezielte Ausbildungsaktivitäten, für die MI Manager und für neue Mitarbeitende. Im Mai 2016 hat zudem ein 2tägiger Workshop stattgefunden bei dem ein MI mit Einsatz einer Task Force mit dem Kader des BIT simuliert wurde. Die minutiös vorbereitete Übung hat gezeigt, dass in verschiedenen Gebieten noch Unsicherheiten vorhanden sind. Die daraus abgeleitete Pendenzenliste wird nachfolgend abgearbeitet und die Unterlagen sowie Prozesse werden präzisiert bzw. ergänzt.

Das BIT hat regelmässig kleinere Störfälle wie z. B. vor kurzem der Ausfall des Swisscom-Netzes, welcher auch Auswirkungen auf die Bundesverwaltung hatte. Vom kleinsten Incident bis zum MI wird konsequent dokumentiert, wie das Problem behoben wurde. Bei jedem MI wird zudem analysiert, ob noch Verbesserungspotential vorhanden ist, ob die Dokumente vollständig und korrekt waren. Auch damit wird sichergestellt, dass ITSCM laufend verbessert und aktualisiert wird.

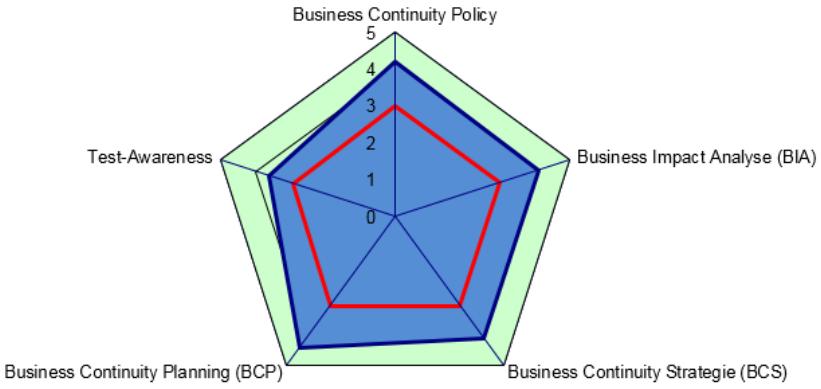
2.5 Leistungsbezüger erhalten Unterstützung bei der Erarbeitung ihres BCM

Das BIT bietet den LB nicht grundsätzlich eine Dienstleistung an, um sie bei der Erarbeitung ihres eigenen BCM zu unterstützen. Jedoch gibt es seine Erfahrungen bei Anfrage jederzeit an die LB weiter. VE mit kritischen Anwendungen sind gemäss Aussagen des BIT beim BCM grundsätzlich aktiver und interessierter, als solche mit weniger heiklen Anwendungen. Mit ersteren hat das BIT auch regelmässigen Kontakt und diese Kunden kennen die Abläufe rund um ITSCM. Da das BIT für die meisten LB Lieferant der Arbeitsplatzsysteme ist, wäre es bei einem BCM-Vorfall in einer VE ebenfalls stark involviert. Dies könnte das BIT selber in den Krisenmodus führen, da wie beschrieben Fachspezialisten abgezogen werden müssten, um dem betroffenen Amt zeitgerecht helfen zu können.

3 Beurteilung

3.1 Das BIT hat eine gute Basis geschaffen

Das BIT hat aus zwei schwerwiegenden Vorfällen die Lehren gezogen. Die in den letzten 3 Jahren erarbeiteten Grundlagen zum BCM BIT und das aufgebaute ITSCM hinterlassen einen guten Eindruck. Es wird methodisch und systematisch gearbeitet. Der Wille zu einer kontinuierlichen Verbesserung ist klar erkennbar. Die Dokumente und Instrumente stehen im Intranet des BIT allen Beteiligten zur Verfügung. Eine erste grössere Simulationsübung hat unlängst stattgefunden. Diese wurde von mehreren interviewten Mitarbeitenden als sehr lehrreich dargestellt. Die EFK beurteilt die Vorkehrungen und Instrumente des BIT als gut. Die aus dem Standardfragebogen resultierende Grafik zeigt einen Maturitätslevel[5] von etwas über 4 auf der Skala von 1-5 (Legende siehe Anhang 3). Die rote Linie stellt den von der EFK festgelegten Mindestwert 3 dar.



Einschränkungen gab es, weil die Unterlagen teilweise noch nicht fertig sind oder die regelmässige Aktualisierung nicht überprüfbar war. Ein Grossteil der Dokumentation vor allem bei ITSCM ist innerhalb der letzten 1-2 Jahre erstellt worden.

[5] In Analogie zu COBIT, dem führenden Framework für Führung und Steuerung von Geschäfts-IT

3.2 Beim Wiederanlauf haben nicht Anwendungen sondern Services Priorität

Im Rahmen des ISO-Standards 22301 zum BCM wird davon ausgegangen, dass ein Unternehmen seine kritischen Kerngeschäfte kennt. Für diese Kerngeschäfte wird eine Business Impact Analyse erstellt und nachfolgend die Gegenmassnahmen bzw. der Wiederanlauf im BCP geregelt. Das BIT hat Verträge mit seinen LB in welchen die verschiedenen SLE vereinbart werden. Entsprechend ergeben sich daraus unterschiedliche Verfügbarkeitsanforderungen, welche das BIT über alle Krisenlagen hinweg zu erfüllen hat. Tritt nun bei BTR ein unvorhergesehenes Ereignis ein wie z. B. der Ausfall eine Rechenzentrums infolge eines Stromunterbruchs, so werden nach Masterplan nicht einzelne Anwendungen sondern zuerst alle notwendigen Services nacheinander, teilweise auch parallel wieder hergestellt. Sobald die Betriebssysteme und Datenbanken wieder verfügbar sind, werden die Anwendungen automatisiert gestartet. Im Normalfall stehen diese danach wieder für die Benutzenden zur Verfügung. Wenn bei diesem Hochfahren Probleme auftreten, wird priorisiert gearbeitet. Dann erhalten jene Anwendungen Vorrang, welche gemäss Liste des BIT aufgrund vertraglicher Vereinbarungen die höchsten Verfügbarkeitsanforderungen haben. Dies sind weniger als ein Dutzend Anwendungen, die meisten von der Eidg. Zollverwaltung.

Das Vorgehen macht im Umfeld von BTR Sinn und es ist nachvollziehbar, dass bei hunderten von Servern und Anwendungen nicht einzelne Elemente herausgeschält werden können. Viel mehr wird mit Nachdruck daran gearbeitet, dass in der richtigen Reihenfolge alle notwendigen Komponenten möglichst rasch wieder verfügbar sind. Erst danach können als Letztes auch die Anwendungen wieder gestartet werden. Im Gesamtkontext gesehen, ist „Anwendungen starten“ nur etwa 20 % aller Aktivitäten, die beim Wiederanlauf stattfinden. Wie mehrere MI in den letzten Jahren zeigen, bewährt sich dieses Vorgehen und mehrheitlich musste keine Priorisierung bei den Anwendungen stattfinden.

3.3 Trotz guten Noten sind Verbesserungen möglich

Aus Sicht EFK wäre es für das BIT von Vorteil, wenn auch weniger aktiven LB die Abläufe und Prozesse von ITSCM in geeigneter Form näher gebracht werden könnten, z. B. über den „Eisbrecher“ oder mittels Präsentation in den zahlreichen Gremien des Bundes.

Bei den Wiederanlaufplänen wurde festgestellt, dass noch nicht alle SCM-Dokumente vollständig sind. Es fehlen einzelne Checklisten und teilweise auch Abläufe oder die Grundlagen sind nicht freigegeben. Das BIT arbeitet jedoch mit einer Arbeitsgruppe an der Finalisierung aller Unterlagen, die Endtermine sind vom Leiter BTR gesetzt und werden überwacht.

Wie die Grafik unter Kapitel 3.1 zeigt ist der Maturitätswert bei Test und Awareness unterhalb von vier. Das BIT hab bisher keine mehrjährige Testplanung. Die EFK hat erwartet, dass im Zeitraum von 4 - 5 Jahren alle relevanten Teilbereiche des ITSCM einmal durchgetestet werden. Der im Mai 2016 durchgeführte Kaderworkshop kann als positiver Start gewertet werden. Weitere solche Aktivitäten müssen nun kontinuierlich stattfinden. Nur was getestet wurde und funktionierte, kann im Ernstfall mit hoher Wahrscheinlichkeit wieder hergestellt werden. Die EFK sieht hier noch Verbesserungsmöglichkeiten.

Empfehlung 1 (Priorität 1):

Die EFK empfiehlt dem BIT eine mehrjährige Planung zum Testen aller Bereiche des ITSCM zu erstellen. Der Plan sollte auch alle relevanten Krisenszenarien berücksichtigen.

Stellungnahme des BIT: Das BIT teilt die Analyse und wird eine Planung für die kommenden Jahre aufsetzen.

4 Schlussbesprechung

Ein mündliches Feedback zu den Resultaten hat am 7. Juli 2016 stattgefunden. Teilgenommen haben der Direktor des BIT, der Leiter Betrieb und ein weiterer Mitarbeiter, seitens EFK waren der Leiter Fachbereich 4 und die Revisionsleiterin vertreten. Aufgrund der insgesamt positiven Resultate verzichtet das BIT nach Zustellung des Berichtsentwurfs auf eine Schlussbesprechung.

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

EIDGENÖSSISCHE FINANZKONTROLLE

Anhang 1: Rechtsgrundlagen

Finanzkontrollgesetz (FKG, SR 614.0)
Finanzhaushaltgesetz (FHG, SR 611.0)
Finanzhaushaltverordnung (FHV, SR 611.01)
Bundesinformatikverordnung (BinfV, SR 172.010.58)

Anhang 2: Abkürzungen, Glossar, Priorisierung der Empfehlungen

Abkürzungen

BCM	Business Continuity Management – Geschäftsfortführung im Krisenfall
BCP	Business Continuity Planning
BIT	Bundesamt für Informatik und Telekommunikation
BTR	Leistungsbereich Betrieb
EFK	Eidg. Finanzkontrolle
ISB	Informatiksteuerungsorgan des Bundes
ITSCM	IT Service Continuity Management
LB	Leistungsbezüger
LE	Leistungserbringer
MI	Major Incident
SLE	Service Level Element
VE	Verwaltungseinheit

Priorisierung der Empfehlungen

Die EFK 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 3: 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 findet 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. 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.