EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
CONTROLLA FEDERALA DA FINANZAS

Business Continuity Management beim Bund

Querschnittsprüfung der Praxis bei neun Verwaltungseinheiten

August 2009

Impressum

Bestelladresse **Adresse de commande** **Order address**	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45, CH - 3003 Bern http://www.efk.admin.ch/
Bestellnummer **Numéro de commande**	 1.9217.100.00373.31
Zusätzliche Informationen **Complément d'informations** **Further information**	Cornelia Simmen, IT-Prüfungsexpertin Fachbereich 4 E-Mail: cornelia.simmen@efk.admin.ch Tel. +41 31 324 10 83
Originaltext **Texte original** **Original text**	Deutsch Allemand German
Zusammenfassung **Résumé** **Abstract**	Deutsch (« Das Wesentliche in Kürze ») Français (« L'essentiel en bref ») English (« Key facts »)

Business Continuity Management Bund
Querschnittsprüfung der Praxis bei neun Verwaltungseinheiten

Das Wesentliche in Kürze

BCM: Notwendigkeit oder Zeitverschwendung?

Business Continuity Management bedeutet, dass alle notwendigen Vorkehrungen getroffen werden, damit die Bundesverwaltung und der Bundesrat ihre Kernaufgaben selbst in ausserordentlichen Situationen termingerecht erfüllen können. Die Eidg. Finanzkontrolle (EFK) hat im Rahmen der vorliegenden Querschnittsprüfung festgestellt, dass sich bereits seit mehreren Jahren unterschiedliche Gremien mit dem Thema befassen.

Das Bundesamt für wirtschaftliche Landesversorgung hat in Bereichen wie Energie, Transport und Logistikdienste oder Informationstechnologie Risikoanalysen zusammen mit der Privatwirtschaft durchgeführt. In den publizierten Schlussberichten sind die Risiken, Auswirkungen und Eintretenswahrscheinlichkeiten ausführlich dargelegt. BCM wird als eine der zentralen Massnahmen genannt, um gegen die erkannten Risiken vorzubeugen. Auch die Bundeskanzlei ist zum Thema aktiv. Als zuständige Stelle für die Krisenmanagementausbildung im Bund ist sie für die alle vier Jahre stattfindende Strategische Führungsübung zuständig. Im Jahre 2009 fand eine solche Übung unter dem Motto „Stromversorgung“ statt. Aufgrund von Beschlüssen der Generalsekretärenkonferenz (GSK) wird sich die Bundeskanzlei zudem längerfristig in einem bundesweiten Projekt mit der „Einführung eines umfassenden BCM“ beschäftigen.

Das Bundesamt für Gesundheit steht zusammen mit dem Staatssekretariat für Wirtschaft im Rampenlicht aufgrund der allgemeinen Pandemie-Vorsorge. Diese betrifft nicht nur die Bundesverwaltung sondern auch die Privatwirtschaft und die ganze Schweizer Bevölkerung. BCM heisst in diesem Falle, dass lebenswichtige Versorgungen wie Medizin, Lebensmittel oder Finanzen auch mit stark reduzierten Ressourcen in genügendem Masse erfolgen können.

Die EFK hat daher in neun Verwaltungseinheiten mit grossen Finanzflüssen oder Aufsichtsfunktionen geprüft, wie weit Vorkehrungen zur Bewältigung einer ausserordentlichen Situation getroffen sind. Auch in der Bundesverwaltung besteht die Notwendigkeit, dass die wichtigsten Kernaufgaben sichergestellt sind. Die Aufwendungen für ein BCM können nicht als Zeitverschwendung bezeichnet werden. Vielmehr wird durch vorbereitete und geübte Szenarien im Falle eines unvorhergesehenen Ereignisses wertvolle Zeit gespart.

Risikoanalysen und daraus abgeleitete Pläne, wie bei Eintreten eines Risikos reagiert werden soll, sind massgebend für das Krisenmanagement

Die Geschäftsprozesse einer Verwaltungseinheit müssen erfasst und die dafür notwendigen Ressourcen bestimmt sein. Ohne diese Basisdaten lassen sich weder Risiken noch deren Auswirkungen auf die Prozesse abschätzen. Es konnte festgestellt werden, dass in allen geprüften Verwaltungseinheiten die wichtigsten Geschäftsprozesse definiert sind. Die Risikoanalysen sind jedoch unterschiedlich im Umfang und in der Methodik. Sie fokussieren aufgrund der Pandemie-Vorsorge mehrheitlich nur auf den Ausfall von Personal. Szenarien zu anderen Risikobereichen (z.B. Elementarereignisse, Ausfall von Informatikmitteln) sind dagegen wenig oder unvollständig vorhanden.

Entsprechend fehlen in diesen Bereichen die Überlegungen zu den Auswirkungen oder notwendigen Ressourcen, was sich nachfolgend auch in der Planung niederschlägt.

Beim Business Continuity Planning (BCP) sollten konkrete Vorgehensweisen zu den einzelnen erfassten und beurteilten Risikoszenarien definiert werden. Die Informatik steht unbestritten bei vielen Verwaltungseinheiten im Vordergrund. Es musste aber festgestellt werden, dass bei hohen Anforderungen an die Verfügbarkeit teilweise ungenügende Vereinbarungen mit den Leistungserbringern erfolgt sind. Die beim Bundesamt für Informatik und Telekommunikation üblichen Standardverträge beinhalten keine Katastrophen-Vorsorge-Optionen, diese müssen separat vereinbart werden. Auch bezüglich Ausweicharbeitsplätze wird das für die Immobilienverwaltung zuständige Bundesamt für Bauten und Logistik nur beschränkt helfen können. Die allenfalls vorhandenen verfügbaren Arbeitsplätze sind weder an einem einzigen Standort noch ist gewährleistet, dass diese mit der notwendigen Infrastruktur ausgerüstet sind. Es müssen daher durch die Verwaltungseinheiten entsprechende Überlegungen erfolgen und Ausweichmöglichkeiten abgeklärt werden, bevor ein Ereignis solche notwendig macht.

Die Pandemie-Vorsorge hat in den letzten Monaten dazu geführt, dass alle geprüften Verwaltungseinheiten ihre Kernprozesse und die dafür notwendige Anzahl Mitarbeitende definiert haben. Diese Festlegungen stellen einen wichtigen Teil des BCP dar und können auch für andere Krisenszenarien (z.B. Ausfall eines Gebäudes) weiterverwendet werden. Insgesamt wird aber zu sehr darauf vertraut, dass bei einem ausserordentlichen Ereignis situativ reagiert und entschieden werden kann. Planungen sind teilweise gar nicht vorhanden oder es fehlen wichtige Elemente und die Verantwortlichkeiten sind nicht klar geregelt.

Um eine eintretende Krise oder Katastrophe wirksam und zeitgerecht meistern zu können, bedarf es einer separaten Organisation ausserhalb der normalen Tagesgeschäfte, d.h. eines Krisenstabes. Jedes Mitglied des Krisenstabes muss seinen Aufgaben- und Verantwortlichkeitsbereich kennen sowie über die notwendigen Kompetenzen verfügen. Benötigte Hilfsmittel (z.B. Alarmierungslisten, Notebooks, Sitzungszimmer, usw.) müssen gerade in einer ausserordentlichen Situation innert nützlicher Frist am richtigen Ort zur Verfügung stehen. Krisenmanagement bedeutet, dass die definierten wichtigen Geschäftsprozesse möglichst ohne oder wenigstens mit dem kleinst möglichen Unterbruch weitergeführt werden und schrittweise zu einem Normalbetrieb zurückgekehrt wird. Ein solches Vorgehen muss im dafür bestimmten Gremium regelmässig geübt werden. Beim Krisenmanagement sind noch einige Arbeiten zu erledigen.

In der Bundesverwaltung sind positive Ansätze vorhanden, die EFK sieht jedoch einigen Handlungsbedarf

Aufgrund der Resultate lässt sich festhalten, das teilweise schon fast ausgereifte Analysen und Pläne sowie funktionierende Krisenstäbe bestehen. Die Sensibilität für ein BCM ist durch die Pandemie-Vorsorge in den Führungsebenen sicher verstärkt worden. Dennoch kommt die EFK zum Schluss, dass zum heutigen Zeitpunkt in einer ausserordentlichen Lage nicht alle kritischen Geschäftsprozesse innerhalb der Bundesverwaltung korrekt weitergeführt werden könnten. Die GSK hat beschlossen, die Empfehlung der EFK bezüglich eines Minimalstandards nicht umzusetzen, da BCM eine Aufgabe der Ämter und Departemente sei. Gemäss GSK werden die Departemente prüfen, welches die strategisch wichtigen Bereiche sind und ob Handlungsbedarf besteht.

Business Continuity Management dans la Confédération
Audit transversal de neuf unités administratives

L'essentiel en bref

BCM: nécessité ou perte de temps?

La gestion BCM désigne toutes les mesures qu'il convient de prendre pour s'assurer que l'administration et le Conseil fédéral puissent remplir leurs tâches essentielles selon le calendrier fixé aussi dans des situations extraordinaires. Dans le cadre de l'audit transversal qu'il a effectué, le Contrôle fédéral des finances (CDF) a constaté que la gestion BCM est traitée depuis plusieurs années déjà par divers organismes.

L'Office fédéral pour l'approvisionnement économique du pays a procédé, en collaboration avec le secteur privé, à des analyses de risques dans des domaines tels que l'énergie, les transports, les services logistiques et les technologies de l'information. Dans les rapports finaux publiés, les risques potentiels, leurs effets et leur taux de probabilité sont décrits en détail. Ils indiquent que la gestion BCM constitue l'un des principaux instruments permettant de prévenir les risques encourus. La Chancellerie fédérale se penche elle aussi activement sur le sujet. Responsable de la formation en matière de gestion des crises à l'échelon fédéral, elle dirige l'exercice de conduite stratégique organisé tous les quatre ans. Consacrée au problème de l'approvisionnement en électricité, la dernière édition de cet exercice a eu lieu en 2009. Suite aux décisions de la Conférence des secrétaires généraux (CSG), la Chancellerie fédérale élaborera, à plus long terme, un projet d'introduction de la gestion BCM à l'échelon fédéral.

L'Office fédéral de la santé publique est actuellement sur le devant de la scène, avec le Secrétariat d'Etat à l'économie, en raison des mesures générales de prévention des pandémies. Celles-ci concernent non seulement l'administration fédérale, mais aussi le secteur privé et l'ensemble de la population suisse. Dans ce contexte, la gestion BCM a pour tâche de garantir en suffisance, même avec des moyens fortement réduits, les approvisionnements vitaux dans des domaines tels que la médecine, l'alimentation ou les finances.

Le CDF a donc examiné, dans neuf unités administratives concernées par des flux financiers importants ou exerçant une fonction de surveillance, l'étandue des mesures prises en vue de gérer une situation extraordinaire. Les tâches clés d'importance vitale doivent également être garanties à l'échelon de l'administration fédérale. C'est pourquoi la gestion BCM ne peut pas être considérée comme une perte de temps. Elle permet au contraire de gagner un temps précieux en cas d'événement imprévu, grâce à l'élaboration et à la mise en œuvre de scénarios.

Les analyses des risques et les plans des mesures à prendre en cas de survenance d'un risque sont déterminants pour la gestion des crises

Les processus de l'unité administrative doivent être enregistrés, avec l'indication des ressources nécessaires pour en assurer le bon déroulement. Ces données de base sont indispensables pour mesurer les risques et leurs effets sur les processus. Les examens effectués ont montré que toutes les unités administratives évaluées ont défini leurs principaux processus. Leurs analyses des risques varient toutefois dans leur ampleur et leur méthode. La plupart d'entre elles se concentrent

sur le risque lié à l'absence de personnel en cas de pandémie. En revanche, les analyses des risques concernant d'autres domaines (dangers naturels, pannes informatiques) sont peu présentes ou insuffisantes. Par conséquent, il manque, dans ces domaines, les réflexions relatives aux conséquences des risques ou les ressources requises pour y faire face, ce qui se répercute dans la planification.

Pour assurer la planification de la continuité des activités (PCA), il convient de définir des procédures concrètes pour chaque scénario de risque inventorié et evalué. A cet effet, de nombreuses unités administratives privilégient clairement l'informatique. Il a toutefois été constaté que, dans les cas où les exigences sont élevées vis-à-vis de la disponibilité des moyens informatiques, les conventions passées avec les fournisseurs de prestations sont parfois insuffisamment précises. Les conventions standards de l'Office fédéral de l'informatique et de la télécommunication ne comprennent pas de clauses relatives à la prévention de catastrophes, c'est pourquoi de telles clauses doivent être conclues séparément. En ce qui concerne la mise à disposition de places de travail de secours, l'Office fédéral des constructions et de la logistique, responsable de la gestion des immeubles, ne peut fournir qu'une aide limitée. En effet, il n'est pas garanti que les éventuelles places de travail libres se trouvent toutes au même emplacement, ni qu'elles sont pourvues de l'équipement requis. C'est pourquoi les unités administratives doivent mener les réflexions nécessaires à ce sujet et examiner les problèmes liés aux places de travail de secours avant d'être confrontées à une situation d'urgence.

Dans le cadre des mesures de prévention des pandémies prises au cours des derniers mois, toutes les unités administratives évaluées ont procédé à la définition de leurs processus centraux, avec l'indication du nombre de collaborateurs nécessaires à l'exécution de chaque processus. Ces informations constituent une part importante de la PCA et peuvent être utilisées pour d'autres scénarios de crise (p. ex. lorsqu'un immeuble n'est plus utilisable). Toutefois, la croyance selon laquelle, en cas d'événement extraordinaire, les décisions et les mesures requises pourront être prises en fonction de la situation est encore beaucoup trop répandue. Une partie des unités administratives n'ont pas élaboré de planification en la matière ou des éléments importants manquent ainsi qu'une définition claire des responsabilités.

Pour assurer la maîtrise efficace et rapide d'une crise ou d'une catastrophe, il importe que l'unité administrative se dote d'une organisation spéciale d'intervenir en dehors du processus ordinaire des affaires quotidiennes, à savoir d'un état-major de crise. Chaque membre de l'état-major de crise doit connaître ses tâches et responsabilités et être investi des compétences requises. Dans une situation extraordinaire, les instruments nécessaires (listes d'alarme, « notebook », salles de séances, etc.) doivent être disponibles le plus rapidement possible et à l'emplacement approprié. Maîtriser une crise implique d'assurer un déroulement continu des processus importants prédéfinis ou un déroulement affecté par le moins d'interruptions possible, suivi par un retour progressif à la normale. Une telle procédure doit être exercée régulièrement par l'équipe définie. En matière de gestion des crises, certains éléments doivent encore être mis au point.

L'administration fédérale est sur la bonne voie, mais le CDF estime que des mesures sont encore nécessaires

Les résultats des examens montrent que les unités administratives disposent en partie d'analyses de risques et de planifications presque complètes ainsi que d'états-majors de crise prêts à l'intervention. Avec la prise des mesures de prévention de la pandémie, les directions d'office ont été sensibilisées de manière accrue à la nécessité de la gestion BCM. Le CDF parvient toutefois à la conclusion que, à l'heure actuelle, les processus d'importance cruciale de l'administration fédérale ne pourraient pas tous se poursuivre adéquatement en cas de situation extraordinaire. La CSG a décidé de ne pas appliquer la recommandation du CDF concernant la mise en œuvre d'une norme minimale en la matière étant donné que la gestion BCM est une tâche incombant aux offices et aux départements. Selon la CSG, les départements s'emploieront à identifier les domaines d'importance stratégique et examineront s'il convient de prendre des mesures.

Business Continuity Management at the Confederation
Cross-section audit of practices in nine administrative units

Key facts

BCM: Necessity or waste of time?

Business Continuity Management is a process whereby all necessary measures are taken to ensure that the Federal Administration and Federal Council can accomplish their core tasks on time even in extraordinary situations. During this cross-section audit, the Swiss Federal Audit Office (SFAO) found that various bodies have been addressing the issue for several years already.

The Federal Office for National Economic Supply has carried out risk analyses together with the private sector in areas such as energy, transport and logistics, as well as information technology. The risks, ramifications and probabilities of occurrence are set out in detail in the final reports published. BCM is cited as a key measure for guarding against the recognised risks. The Federal Chancellery is also active in this area. As the body in charge of crisis management training within the Confederation, it is responsible for the strategic leadership exercise that takes place every four years. Such an exercise on the topic of power supply took place in 2009. Based on the decisions of the General Secretaries Conference, the Federal Chancellery will also work longer term on a national project regarding the introduction of comprehensive BCM.

The spotlight has been on the Federal Office of Public Health, together with the State Secretariat for Economic Affairs, because of the general pandemic precautionary measures. These concern not only the Federal Administration, but also the private sector and the entire Swiss population. In this case, BCM refers to the fact that sufficient quantities of vital supplies such as medicine, food and financial means can be ensured even with drastically reduced resources.

The SFAO thus checked the extent to which measures for coping with extraordinary situations are implemented in nine administrative units with large flows of funds or with supervisory functions. Also in the Federal Administration, it is necessary to guarantee the most important core tasks. BCM expenditure cannot be seen as a waste of time. On the contrary, valuable time can be saved in the case of an unforeseen event by having prepared and practised scenarios.

Risk analyses and the associated response plans for when a risk occurs are decisive for crisis management

The business processes of an administrative unit must be entered, and the necessary resources determined. Without this basic data, neither the risks nor their impact on processes can be assessed. It was found that the most important business processes have been defined in all the administrative units audited. The risk analyses, however, differ in terms of scope and methodology. Because of the pandemic precautionary measures, they focus largely on absenteeism. In contrast, scenarios regarding other areas of risk (e.g. natural hazards, IT resource outages) are scarce or incomplete. Accordingly, reflections on the consequences or necessary resources are lacking in these areas, which is subsequently reflected also in planning.

Business Continuity Planning (BCP) should define concrete courses of action for the individual risk scenarios that have been entered and assessed. The focus is undoubtedly on information technology in many administrative units. However, it was found that there were somewhat insufficient

agreements with the service providers in the case of high demands being made on availability. The usual standard contracts applied by the Federal Office of Information Technology, Systems and Telecommunication do not contain any disaster recovery options; these must be agreed separately. Also regarding alternative work areas, the Federal Office for Buildings and Logistics, which is responsible for real estate management, can provide only limited assistance. Any work areas that may be available are not at a single location and there is no guarantee that they are equipped with the necessary infrastructure. Therefore, the administrative units must give due consideration to this matter and clarify the alternative options before an event makes this a necessity.

The pandemic precautionary measures have resulted in all audited administrative units having defined their key processes and the necessary numbers of employees in recent months. These determinations constitute an important part of BCP and can also be used for other crisis scenarios (e.g. loss of a building). On the whole, however, there is too much reliance on the assumption that it will be possible to react and take decisions based on the situation at hand in the case of an extraordinary event. In some incidents, there are no plans at all, and in others important elements are missing and responsibilities are not clearly defined.

A separate organization outside of normal day-to-day business, i.e. a crisis management team, is needed in order to be able to ultimately handle a crisis or catastrophe in an effective and timely manner. Each member of the crisis management team must know his or her area of activity and responsibility, and must also have the necessary expertise. The requisite resources (e.g. alarm checklists, notebooks, meeting rooms, etc.) must be available at the right place within a reasonable time in the event of an extraordinary situation. Crisis management means that the important business processes defined are continued with no, or minimal, interruptions and gradually return to normal. Action of this nature must be practised regularly within the relevant body. Some work remains to be done as regards crisis management.

There are some positive signs in the Federal Administration, but the SFAO still sees a need for action

Based on the results, it can be established that some almost complete analyses and plans, as well as functioning crisis management teams already exist. BCM awareness has certainly increased at management level with the pandemic precautionary measures. Nevertheless, the SFAO has reached the conclusion that, at the current time, not all critical business processes could be maintained correctly within the Federal Administration in an extraordinary situation. The General Secretaries Conference has decided not to implement the SFAO's recommendations, as BCM is the responsibility of the offices and departments. According to the General Secretaries Conference, the departments will check which are the strategically important areas and whether there is a need for action.

Inhaltsverzeichnis

Anhänge

1 Auftrag und Prüfungsdurchführung

1.1 Auftrag

Die EFK führte von Mai bis Juli 2009 eine Querschnittsprüfung zum Thema „Business Continuity Management“ (BCM) in neun Verwaltungseinheiten (VE) des Bundes durch. Diese wurden ausgewählt aufgrund

- ihrer gesetzlichen Aufsichtsfunktion (Bundesamt für Gesundheit, Bundesamt für Polizei, Bundesamt für Zivilluftfahrt),
- ihrer finanziellen Relevanz, d.h. hohe Einnahmen oder Ausgaben (Eidg. Finanzverwaltung, Eidg. Steuerverwaltung, Eidg. Zollverwaltung, Staatssekretariat für Wirtschaft / Bereich Arbeitsmarkt/Arbeitslosenversicherung, Zentrale Ausgleichsstelle),
- ihrer Stabsfunktion für den Bundesrat (Bundeskanzlei).

Der Prüfauftrag lautete:

- Ist bei den Leistungsbezügern (LB) ein BCM vorhanden, welches die Aufrechterhaltung und zeitgerechte Wiederherstellung der kritischen Geschäftsfunktionen im Krisen-/Katastrophenfall sicherstellt?

Das Revisionsteam hat daraus folgende Fragen abgeleitet und dahingehende Dokumentationen von den VE erwartet:

- Sind die kritischen Geschäftsprozesse und die dafür notwendigen Ressourcen festgelegt und priorisiert?
- Verfügt die Verwaltungseinheit über eine Risikobeurteilung, welche auch die Auswirkungen auf die Geschäftsprozesse berücksichtigt (Business Impact Analysis)?
- Besteht in der Verwaltungseinheit eine Strategie zur Geschäftsweiterführung (Business Continuity Strategy)?
- Besteht eine Notfallplanung (Business Continuity Planning)?
- Bestehen ein Krisenmanagement und die entsprechende Krisenorganisation?

Ein umfassendes BCM beinhaltet weitere Schwerpunkte wie

- die Umsetzung und Überprüfung der Wirksamkeit des Business Continuity Planning,
- die Berichterstattung zu den Aktivitäten und dem Stand der Vorbereitungen,
- die fachliche Ausbildung der Mitarbeitenden.

Auf eine detaillierte Prüfung dieser Bereiche wurde verzichtet, da dies den zur Verfügung stehenden Zeitrahmen gesprengt hätte.

1.2 Rechtsgrundlagen

- Finanzhaushaltverordnung vom 5. April 2006 (FHV, SR 611.01)
- Bundesgesetz über die Eidgenössische Finanzkontrolle vom 28. Juni 1967, Stand am 1. Januar 2008 (Finanzkontrollgesetz, FKG, SR 614.0)
- Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung vom 26. September 2003, Stand am 1. August 2007 (Bundesinformatikverordnung, BinfV, SR 172.010.58)
- Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung vom 27. September 2004, Stand 1. November 2007 (WIsB)
- Risikopolitik, Grundlagen für das Risikomanagement beim Bund vom Dezember 2004

Zusätzlich wurden die Vorgaben der FINMA[1] und der internationale Standard zum Thema BCM verwendet:

- Empfehlungen für das Business Continuity Management (BCM) vom November 2007 (herausgegeben von der Bankiervereinigung, SwissBanking, von der FINMA als Mindeststandard anerkannte Selbstregulierung)
- British Standard BS25999, Betriebliches Kontinuitätsmanagement Teil 1 und Teil 2

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von den IT-Prüfungsexperten Markus Künzler, Hans-Jörg Uwer und Cornelia Simmen (Revisionsleitung) sowie dem Prüfungsexperten Peter König durchgeführt.

In der Bundesverwaltung besteht nur in den Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung (WIsB) im Anhang 1, Kapitel 7, eine verbindliche Regelung bezüglich „der Geschäftsfortführung (Business Continuity) im Stör-, Not- oder Katastrophenfall“. Dieser Absatz gibt keinen Hinweis über das Vorgehen oder die notwendige Tiefe und Dokumentation. Die EFK hat daher die Empfehlungen der FINMA und den BS25999 als Vorlage verwendet, um das BCM in der notwendigen Tiefe zu prüfen und eine möglichst gleichwertige Beurteilung bzw. vergleichbare Resultate erreichen zu können. Der BS25999 ist ein international anerkannter Standard und beinhaltet Vorgaben, wie ein BCM aufgesetzt werden sollte.

[1] Finanzmarktaufsicht (am 1. Januar 2009 wurden das Bundesamt für Privatversicherung BPV, die Eidg. Bankenkommission EBK und die Kontrollstelle für die Bekämpfung der Geldwäscherei Kst GwG in der Eidgenössischen Finanzmarktaufsicht zusammengeführt)

Basis für die Prüfung bildete ein detaillierter Fragebogen, der in enger Zusammenarbeit mit der Internen Revision des Eidg. Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) entwickelt wurde. Im VBS wird BCM durch die Interne Revision ebenfalls geprüft. Der Fragebogen umfasst die Teilgebiete

- Business Impact Analysis (BIA),
- Business Continuity Strategy (BCS),
- Business Continuity Planning (BCP),
- Krisenmanagement und Krisenorganisation.

Die von den VE zu den verschiedenen Bereichen gelieferten Dokumentationen wurden beurteilt. In vertiefenden Interviews mit den verantwortlichen Schlüsselpersonen für das BCM, das Risk- bzw. Krisenmanagement und die Gebäudesicherheit sind die notwendigen Details abgeklärt worden.

Zur Bewertung der Dokumente sowie der Resultate aus den Interviews wurde das Maturity Model aus COBIT 4.1 verwendet (siehe Anhang 1). COBIT ist ein Framework, das sich u.a. an professionelle IT-Prüfer richtet. Das eingesetzte Maturity Model basiert auf einer Skala von 0-5, diese wurde auf jede einzelne Frage ausgerichtet. In den nachfolgenden Kapiteln werden die Resultate gesamthaft pro Teilgebiet anhand der angewendeten Skala mit Hilfe von Kreisen dargestellt, wobei die auf eine Kommastelle genauen Daten auf-/abgerundet worden sind. Die Grafik ist wie folgt zu interpretieren:

Skala-Stufen	**Farbe**	**Bedeutung**	**Kreisgrösse**
0 + 1	rot	Grosser Handlungsbedarf, grundlegende Basisdaten fehlen, Management hat Leitplanken nicht festgelegt	Die Grösse des Kreises entspricht der Anzahl VE mit diesem Resultat (Ziffer zeigt genaue Anzahl)
2	gelb	Handlungsbedarf vorhanden, wichtige Elemente, Standardisierung und/oder Dokumentation fehlen	
3 - 5	grün	Kleiner Handlungsbedarf, ergänzende oder formelle Verbesserungen, Einhaltung überwachen und messen, Awareness trainieren	

Jede Direktion der geprüften VE hat einen Teilbericht mit der Beurteilung des Ist-Zustandes im Vergleich zu den genannten Standards erhalten. Die in diesen Teilberichten grafisch und deskriptiv dargestellten Differenzen sollen den Berichtsempfängern allfällige Schwachstellen gegenüber „best practice“ aufzeigen. Da keine bundesweiten verbindlichen Rechtsgrundlagen bestehen, kann die EFK keine Forderungen in Form von Empfehlungen stellen. Dennoch sind die Verbesserungsmöglichkeiten in den Berichten dargelegt worden. Eine generelle Empfehlung an die Generalsekretärenkonferenz ist im Kapital 7 dieses Berichtes formuliert.

1.4 Unterlagen und Auskunftserteilung

Die vorhandenen Unterlagen sind dem Revisionsteam in genügender Tiefe und termingerecht zur Verfügung gestellt worden. In den Interviews wurde überall offen und kompetent Auskunft über die tatsächliche Situation gegeben. Die EFK hat festgestellt, dass mehrheitlich eine positive Einstellung gegenüber dem geprüften Gebiet herrschte und die Beurteilungen der EFK mit Interesse zur Kenntnis genommen wurden. Die Pandemiewarnungen dürften Einiges dazu beigetragen haben, dass die Sensibilität bezüglich BCM sowohl auf operativer Ebene wie auch bei den Führungskräften in den letzten Monaten stark zugenommen hat.

2 Verschiedene Gremien und Verwaltungseinheiten beschäftigen sich seit längerer Zeit mit Krisen- und Katastrophenszenarien

2.1 Das Bundesamt für wirtschaftliche Landesversorgung hat Risikoanalysen für verschiedene Sektoren erstellt und Massnahmen festgelegt

Das Bundesamt für wirtschaftliche Landesversorgung (BWL) hat seit 2005 mehrere sektorspezifische Risikoanalysen (z.B. Energie, Transport und Logistikdienstleistungen, Informationstechnologie) in Zusammenarbeit mit der Privatwirtschaft und Vertretern von Bundesämtern durchgeführt. Diese Bundesämter decken sich teilweise mit denjenigen der vorliegenden Prüfung. In allen publizierten Schlussberichten[2], die sehr ausführlich die Risikofaktoren, die Auswirkungen und die Eintretenswahrscheinlichkeit aufzeigen, sind BCM und BCP als prominente Massnahmen zu finden. Die EFK kann daher erwarten, dass die an den Studien beteiligten Bundesstellen zur Sicherstellung der definierten kritischen Ressourcen in ihrem Verantwortungsbereich, die notwendigen Vorkehrungen seit längerer Zeit getroffen haben.

2.2 Die Bundeskanzlei ist beauftragt, für die Krisenmanagementausbildung im Bund zu sorgen

Die Bundeskanzlei (BK) ist gemäss Weisungen des Bundesrates[3] für die Krisenmanagementausbildung im Bund (KMA) zuständig. Der Auftrag lautet konkret, dass die BK für die Durchführung von Aus- und Weiterbildung ihres eigenen Krisenstabes und derjenigen der Departemente sorgt. Die alle vier Jahre stattfindenden strategischen Führungsübungen – diese sind für die obersten

---

[2] http://www.bwl.admin.ch/themen/00507/00520/index.html?lang=de

[3] Weisungen des Bundesrates über die organisatorischen Massnahmen in der Bundesverwaltung zur Bewältigung besonderer und ausserordentlicher Lagen vom 24. Oktober 2007

Führungskräfte des Bundes vorgesehen – sind zentraler Bestandteil dieser Aufgabe. Im Jahre 2005 stand das Thema „Epidemie in der Schweiz“, in diesem Jahr die „Stromversorgung“ im Vordergrund. Der Behelf "Grundsätze der Führung in, nach und vor der Krise" ebenfalls aus dem Jahre 2005 enthält alles Wissenswerte zum Krisenmanagement und wurde in allen Departementen verteilt. Weiter ist die Alarmorganisation des Bundes ebenfalls unter der Federführung der BK etabliert. Aufgrund dieser vielfältigen Aktivitäten zieht die EFK den Schluss, dass nicht nur die Departementsleitungen, sondern auch die Führungsgremien der einzelnen VE über genügend Sensibilität bezüglich der eigenen Krisen- und Katastrophenvorsorge verfügen sollten.

2.3 Das Bundesamt für Gesundheit trifft Vorkehrungen für den Pandemiefall

Seit Ende April 2009 zum ersten Mal das Virus der Grippe A(H1N1) auf dem nordamerikanischen Kontinent festgestellt wurde, orientieren die Medien fast täglich über die fortschreitende Ausbreitung und die Gefahr einer bevorstehenden weltweiten Pandemie. Die World Health Organisation (WHO) hat bereits am 11. Juni 2009 die höchste Alarmstufe 6 ausgelöst und alle Länder aufgerufen, Vorkehrungen zur Bekämpfung des Virus und zum Schutz ihrer Bevölkerung zu treffen. In der Bundesverwaltung ist in der ausserparlamentarischen „Arbeitsgruppe Influenza“ bereits im November 2007 aufgrund der Vogelgrippegefahr der „Pandemieplan; Handbuch für die betriebliche Vorbereitung“ erstellt und vom Bundesamt für Gesundheit (BAG) in Zusammenarbeit mit dem Staatssekretariat für Wirtschaft (SECO) publiziert worden. Die Schweizer Bevölkerung kann auf den Internetseiten dieser beiden VE alle notwendigen und aktuellen Informationen zum Thema Pandemie abholen. In der Bundesverwaltung sind die Departementsvorsteher/-innen und die Direktionen aller VE für den Pandemie-Vorsorgeplan verantwortlich.

2.4 Die Generalsekretärenkonferenz nimmt die Departemente in die Pflicht

Die Generalsekretärenkonferenz (GSK) hat bereits im Juni 2007 im Zusammenhang mit der „Vogelgrippe“ den Auftrag an alle Departemente erteilt, dass Betriebssicherheitsplanungen für den Pandemiefall zu erstellen seien. Im März 2008 hat die GSK aufgrund der zu unterschiedlichen Planungen entschieden, eine überdepartementale Arbeitsgruppe einzusetzen. Diese sollte die Betriebsplanungen vereinheitlichen, so dass eine departementsübergreifende Auflistung der Kernprozesse erfolgt und Doppelspurigkeiten vermieden werden. Die Arbeiten haben sich aus verschiedenen Gründen verzögert und die Resultate sind nicht wie geplant im Herbst 2008 der GSK präsentiert worden. Mit den ersten Warnungen der WHO bezüglich des Grippevirus A(H1N1) wurde nachfolgend der Sonderstab Pandemie im April 2009 aktiviert. Die BK ist nun verantwortlich, dass in erster Priorität die rasche Erstellung und Umsetzung betrieblicher Pandemiepläne und längerfristig die „Projektierung und Initialisierung eines Arbeitsprozesses zur Einführung eines umfassenden BCP/BCM“ bundesweit erfolgen. Die EFK begrüsst diese Absichten unter der Schirmherrschaft der GSK. Wie die Resultate aus der Querschnittsprüfung zeigen, herrscht zurzeit noch einiger Handlungsbedarf bezüglich Weiterführung der Kerngeschäfte in Krisen- oder Katastrophensituationen.

2.5 Die Querschnittsprüfung der Eidg. Finanzkontrolle soll aufzeigen, welchen Umsetzungsstand das Business Continuity Management bei den Leistungsbezügern hat

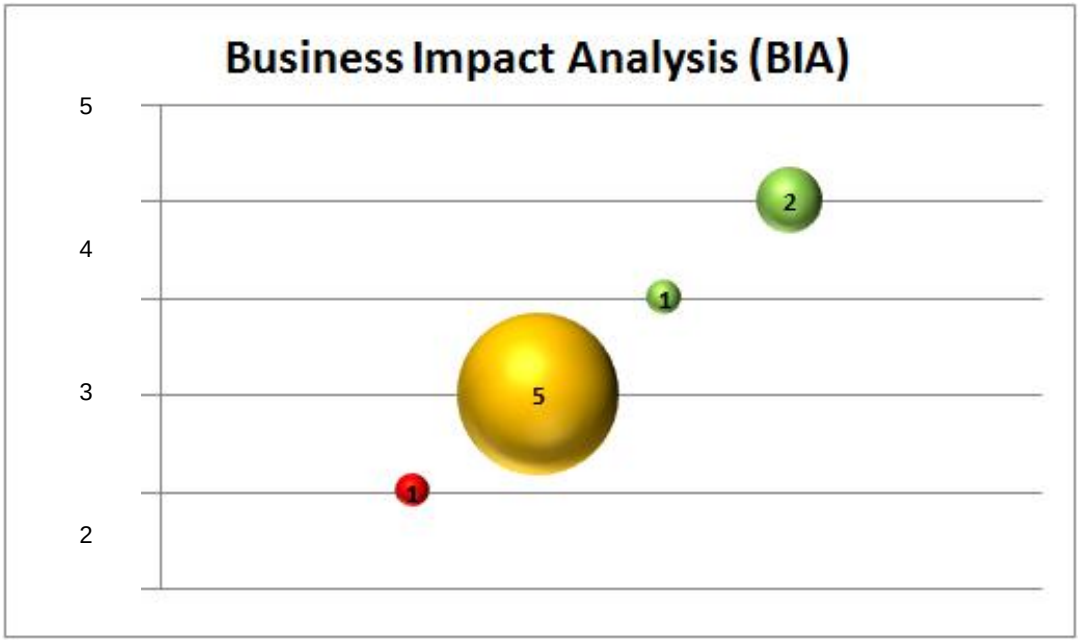
In verschiedensten Prüfungen der letzten Jahre hat die EFK immer wieder festgestellt, dass in Bezug auf Vorkehrungen zur Krisen-/Katastrophenbewältigung unterschiedliche Vorstellungen bei den Leistungsbezügern (LB) und Leistungserbringern (LE) von IT-Dienstleistungen bestehen. Die LB neigen dazu, die Risiken alleine auf die Informatik zu konzentrieren und damit alle Verantwortung auf die LE abzuschieben. Dieses Bild wird durch die alle zwei Jahre stattfindenden Erhebungen des Informatikstrategieorgans des Bundes (ISB) unter dem Titel „Katstrophenvorsorge Bund“ verstärkt. Die zahlreichen IT-Anwendungen gehören unbestritten in vielen Bundesämtern zu den kritischsten Ressourcen. Wie die aktuelle Pandemie-Vorsorgeplanung zeigt, können aber in grosser Anzahl ausfallende Mitarbeitende für die VE genauso problematisch werden. Auch Elementarereignisse wie Brand, Überschwemmung oder längere Stromunterbrüche führen zu Krisensituationen. Die definierten unverzichtbaren Geschäftsprozesse in jeder Situation zeitgerecht weiterführen zu können, liegt in der Verantwortung jeder einzelnen VE. Entsprechend müssen primär dort die notwendigen Vorkehrungen getroffen werden, damit auf eine Krise im festgelegten zeitlichen Rahmen reagiert werden kann. Für Dienste, die durch Dritte erbracht werden, müssen die Anforderungen definiert und notwendige Vereinbarungen getroffen werden. Das sind die grundsätzlichen Definitionen unter dem Titel „Business Continuity Management“, wie sie im BS25999 oder auch in anderen einschlägigen Dokumenten nachzulesen sind.

3 Die Festlegung möglicher Risiken und die Beurteilung der Auswirkungen auf die Geschäftsprozesse und Ressourcen im Eintretensfall

3.1 Warum braucht es eine Business Impact Analysis (BIA)?

Um überhaupt eine Risikoanalyse durchführen zu können, muss die VE zuerst die Geschäftsprozesse erheben und diese anschliessend priorisieren, d.h. festlegen welche Prozesse aufgrund bestimmter Anforderungen (zeitliche, juristische, wirtschaftliche) kritisch sind und welche nicht. Da jeder Geschäftsprozess Ressourcen verwendet, sind diese ebenfalls zu definieren. Ausgehend von dieser Basis kann danach beurteilt werden, welche Risikoszenarien möglich sind und welche Auswirkungen diese auf die Prozesse haben können. Die Einschätzungen sollten auch beinhalten, ob allenfalls Minimallösungen über eine gewisse Zeit möglich sind und welche Mindestressourcen dafür benötigt werden.

3.2 Die Risikoanalysen sind teilweise unvollständig, es besteht unterschiedlicher Handlungsbedarf



Die Grafik zeigt, dass ein Drittel der geprüften VE bereits einen guten Stand erreicht hat und mit wenig Aufwand eine vollständige BIA erstellen kann. Bei den übrigen 2/3 ist Handlungsbedarf vorhanden, sei es weil

- nicht alle Geschäftsprozesse definiert und priorisiert sind,
- wichtige Elemente in der BIA fehlen bzw. unvollständig sind (z.B. Risikokatalog, Ressourcen, Auswirkungen),
- formelle Anforderungen nicht oder nur teilweise erfüllt sind (Freigabe, Aktualisierung, Verfügbarkeit der Dokumente).

Die wichtigsten Geschäftsprozesse sind im Grossen und Ganzen definiert. Einige Verwaltungseinheiten haben alle Geschäftsprozesse mittels eines entsprechenden Managementsystems dokumentiert. Die anderen haben mindestens die kritischen Kernaufgaben im Zusammenhang mit den laufenden Pandemie-Planungen erhoben.

In der Bundesverwaltung wird unter der Federführung der Eidg. Finanzverwaltung (EFV) die Anwendung „risk to chance (R2C)“ für das Risikomanagement eingesetzt. Mit diesem Werkzeug können in verschiedenen Kategorien Risiken mit den Elementen Ursachen, finanzielle Auswirkungen, Eintretenswahrscheinlichkeit, Massnahmen und Verantwortliche erfasst werden. Das Risikomanagement des Bundes sieht vor, dass dieser Katalog jährlich überarbeitet werden muss. In dieser Anwendung fehlen jedoch die Möglichkeiten, Ressourcen zu erfassen und für deren Ausfall die Auswirkungen einzustufen. Auch können die Risiken nicht mit den Geschäftsprozessen und allfälli-

gen Abhängigkeiten (z.B. Lieferanten, Schnittstellen) verknüpft werden. Daher eignet sich R2C nur als Basis für eine BIA, weitergehende Dokumente müssen erstellt werden.

Es konnte festgestellt werden, dass in allen VE Risiken erfasst und beurteilt werden, jedoch in vielen Fällen nur auf die Kernaufgaben fokussiert. Somit fehlen die Risiken, welche zu einer eigenen Krisen-/Katastrophensituation führen könnten wie z.B. Elementarereignisse. Entsprechend sind auch die Auswirkungsanalysen und die Zuteilung der kritischen Ressourcen unvollständig (siehe dazu auch das Kapitel 3.1 im publizierten Bericht „Querschnittsprüfung Risikoanalyse auf Stufe Amt und Bund, 07/2008“ unter www.efk.admin.ch/Publikationen).

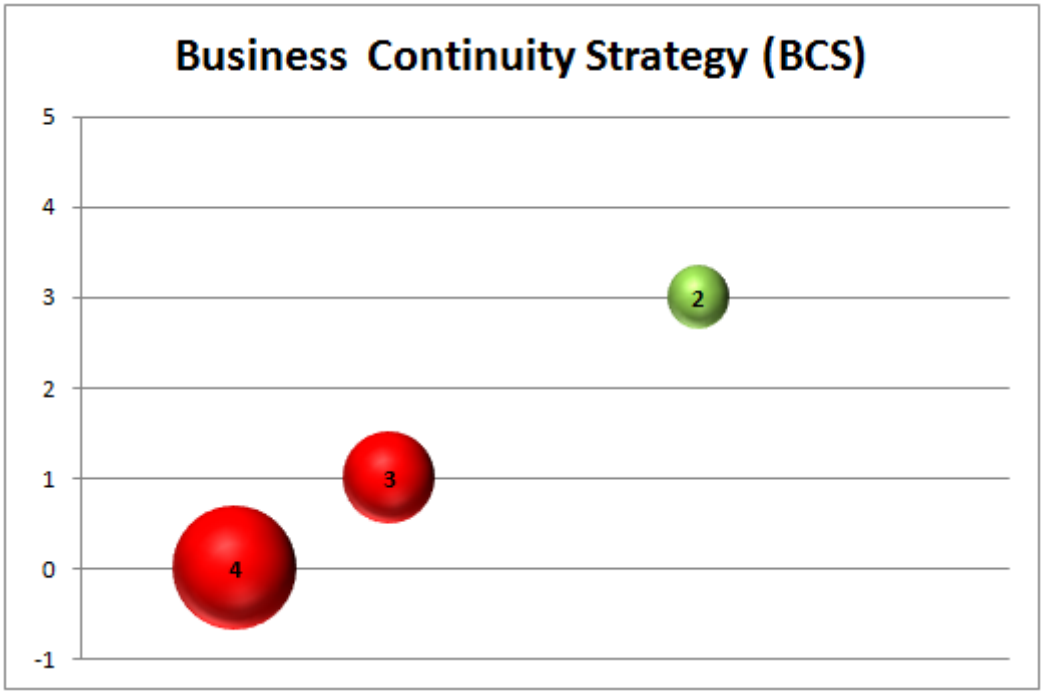
Eine BIA sollte in regelmässigem Rhythmus durch eine verantwortliche Person oder Stelle auf Aktualität geprüft werden. Diese Prüfungen müssten festgelegt und nachvollziehbar dokumentiert sein. Auch die Verteilung von neuen Versionen an die notwendigen Mitarbeitenden ist Bestandteil dieses formellen Vorgehens. Mit wenigen Ausnahmen herrscht hier grundsätzlicher Handlungsbedarf.

4 Die Mitarbeitenden sollten die Absichten des Management kennen

4.1 Was bezweckt eine Business Continuity Strategy (BCS)?

Auf der operativen Ebene sind alle Mitarbeitenden im Rahmen ihrer Aufgaben mit ausserordentlichen Situationen konfrontiert. Diese werden im Tagesgeschäft problemlos gemeistert, wenn die Kompetenzen erteilt und die notwendigen Hilfsmittel vorhanden sind. In einer Krisen- oder Katastrophensituation können dagegen wichtige Ressourcen ausfallen und Routineabläufe dadurch plötzlich nicht mehr funktionieren. Entscheidungen müssen auf höherer Ebene gefällt, Aktivitäten zurückgestellt bzw. priorisiert und Arbeiten mit ungewohnten Hilfsmitteln erledigt werden. Daher sollte das Management in einer Absichtserklärung die wichtigsten Eckpfeiler für eine solche Situation festlegen. In einer BCS wird das grundlegende Vorgehen festgehalten, wie ein Unternehmen seine kritischen Geschäftsprozesse in allen Krisenlagen sicherstellt. Dabei müssen Wiederanlaufziele, dafür notwendige Ressourcen und die Verantwortlichkeiten klar kommuniziert werden. Es wird nicht ein Handbuch erwartet, sondern ein kurzes prägnantes Dokument, das allen Mitarbeitenden zugänglich ist und die Unterschrift der Direktion trägt.

4.2 Der Stellenwert von Strategien zur Geschäftsweiterführung scheint gering zu sein



Das Revisionsteam hat lediglich von zwei VE Dokumente erhalten, in denen die BCS zu Krisensituationen definiert sind. Bei allen anderen wurde festgestellt, dass eine Strategie entweder nicht existent ist oder höchstens erste Anzeichen bestehen, eine solche zu erstellen.

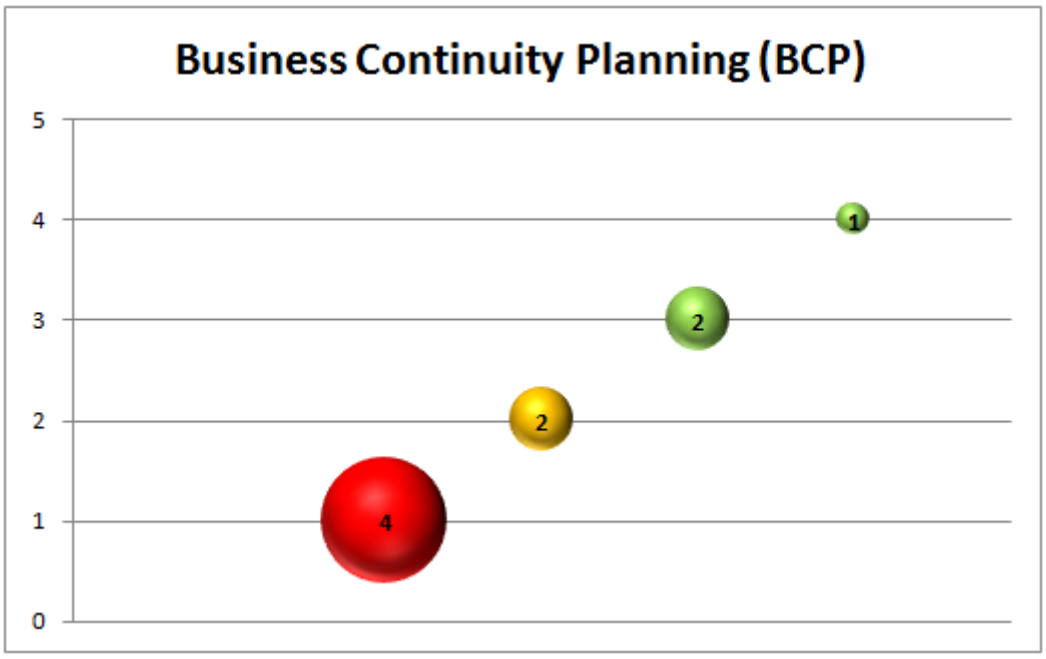
Die formale Dokumentation einer BCS kann im Gesamtkontext des BCM untergeordnet sein, die Strategie selber stellt aber dennoch ein wichtiges Element dar. Daher sollte sich das Management über grundsätzliche Vorgehensweisen im Krisen-/Katastrophenfall Gedanken machen und diese auch gegenüber den Mitarbeitenden kommunizieren. Nur so kann nach Ansicht des Revisionsteams sichergestellt werden, dass auf der operativen Ebene alle notwendigen und vor allem sinnvollen Vorkehrungen getroffen werden. Ohne festgelegte Prioritäten und Leitplanken besteht das Risiko, dass in einer Krisensituation die Kräfte nicht auf die wirklich wichtigen Prozesse und Aktivitäten konzentriert sondern auf Unwichtiges verzettelt werden. Ohne klar festgelegte Verantwortlichkeiten wartet zudem jede(r) auf den/die Anderen und die Zeit verrinnt damit ungenutzt.

5 Die Planung eines Krisen- oder Katastrophenfalls kann darüber entscheiden, ob wichtige Geschäftsprozesse weiter funktionieren

5.1 Business Continuity Planning (BCP) soll die Geschäftsweiterführung in allen ausserordentlichen Lagen sicherstellen

Um sich auf einen möglichen Krisen- oder Katastrophenfall vorzubereiten, müssen Pläne zur Wiederherstellung bzw. Fortsetzung von geschäftskritischen Prozessen erstellt werden. Notwendige oder zwingende Vorgehensweisen aber auch Verantwortlichkeiten sind festzulegen und zu dokumentieren. Mögliche Ersatzlösungen (z.B. manuelle Arbeiten, Ausweichstandorte) und mindestens benötigte Ersatzressourcen (z.B. Notebooks, Arbeitsplätze) können in der Regel nicht erst bei Eintreten einer Krise definiert oder organisiert werden, dazu ist in den meisten Fällen die Zeit zu knapp. Da sowohl auf technischer wie auch auf personeller Seite laufend Veränderungen stattfinden, muss zudem ein BCP von einer dafür bestimmten Person oder Stelle regelmässig überprüft und angepasst werden. Alle Schlüsselpersonen müssen auf die aktuelle Version des BCP in jeder Situation zurückgreifen können.

5.2 Bei der Notfall-Planung herrscht akuter Handlungsbedarf



Das Revisionsteam hat lediglich von drei VE Dokumente erhalten, die den Anforderungen an ein BCP einigermassen genügen und den Eindruck hinterlassen, dass eine Krise ohne grössere Verzögerungen bewältigt werden könnte. In den meisten Fällen ist eine Planung heute nur auf den Pandemiefall ausgerichtet und auch da teilweise noch unvollständig. Lediglich im Bereich der Gebäudesicherheit konnten überall „Notfallpläne“ vorgewiesen werden, so dass mindestens die Sicherheit der Mitarbeitenden bei einem Brandfall oder auch bei anderen Szenarien (z.B. Bomben-

drohung, Geiselnahme usw.) gewährleistet sein sollte. Hingegen haben sich die meisten VE bisher wenig bis gar keine Gedanken dazu gemacht, was nach der notfallmässigen Evakuation eines Gebäudes geschehen sollte. Es ist nicht festgelegt, wer dann über das weitere Vorgehen Entscheidungen trifft und vor allem auch in welchem Zeitrahmen. Allgemein herrscht die Meinung, dass die für den Normalbetrieb zuständigen Linienverantwortlichen auch im Krisenfall ihre Aufgaben wahrnehmen. Dabei wird übersehen, dass in einer Notsituation unvorhergesehene Umstände auftauchen können, die auch die Führungsebene treffen. Wenn Geschäftsprozesse innerhalb eines bestimmten Zeitrahmens ausgeführt werden müssen, so dürfen keine weiteren Verzögerungen aufgrund unklarer Vorgehensweisen eintreten. Sind aber die Verantwortlichkeiten, das Vorgehen, die zeitlichen und hierarchischen Eskalationsstufen sowie die erforderlichen Ressourcen nicht im Voraus definiert, so besteht die Gefahr, dass wertvolle Zeit verrinnt und kritische Geschäftsprozesse nicht mehr den Anforderungen entsprechend wahrgenommen werden.

Das Revisionsteam erachtet die erstellten Pandemie-Vorsorgepläne als wichtigen und guten Bestandteil eines umfassenden BCP, da in diesen die personellen Ressourcen genau bestimmt worden sind. Diese Basis kann ebenso dazu dienen, den Minimalbedarf an Arbeitsplätzen zu definieren, sollte z.B. ein Gebäude infolge eines Elementarschadens über längere Zeit nicht mehr benutzbar sein. Die notwendige Anzahl von Ersatzarbeitsplätzen zu ermitteln und diese auch mit einem allfälligen Partner (Bund oder privat) abzusichern ist ein Teil des BCP. Das Bundesamt für Bauten und Logistik (BBL), als zentrale Immobilienverwalterin des Bundes, hat zwar immer einige Raumeinheiten in Reserve. Eine konkrete Anfrage der EFK anlässlich einer Revision im Jahre 2008 hat aber gezeigt, dass es sich dabei lediglich um etwas mehr als 200 Arbeitsplätze handelt, die auf mehrere geografische Orte und auch Gebäude verteilt sind. Hier kann also nur mit bedingter Hilfe gerechnet werden. Im Zusammenhang mit Ausweichstandorten müsste durch das BBL auch einmal geklärt und vor allem darüber informiert werden, wo geschützte Plätze in Zivilschutzanlagen für die Mitarbeitenden des Bundes vorhanden sind, wenn aufgrund eines regionalen Alarmes solche aufgesucht werden müssten.

Auch im Bereich der Informatik hat das Revisionsteam festgestellt, dass eine grosse Erwartungshaltung gegenüber dem Bundesamt für Informatik und Telekommunikation (BIT) besteht, die Anforderungen aber nicht überall auch mit entsprechenden Vereinbarungen abgesichert sind. Das BIT bietet für IT-Anwendungen mit sehr hoher Verfügbarkeitsanforderung eine zusätzliche kostenpflichte Option „KaVor“ (Katastrophenvorsorge) an. Ohne diese Vereinbarung kann und darf nicht davon ausgegangen werden, dass bei einem Katastrophenfall im BIT die IT-Anwendungen mit nur einem Standardvertrag innerhalb von Stunden wieder verfügbar sind. Die Klauseln besagen ausdrücklich, dass die vereinbarten Wiederanlaufzeiten in 80% der Fälle garantiert sind. Bei vereinbarter Option „KaVor“ dagegen muss das BIT die vereinbarten Zeiten einhalten und entsprechende Doppelsysteme an verschiedenen Standorten betreiben, damit es dieser Verpflichtung nachkommen kann. In wichtigen Bereichen der Finanzeinnahmen oder beim Zoll sind solche Vereinbarungen vorhanden. In diesem Zusammenhang darf erwähnt werden, dass das BIT im Jahr 2008 sein damaliges Ausweich-Rechenzentrum aufgegeben hat und alle dort gelagerten Systeme in das neue Rechenzentrum zügeln musste. Mit diesem Umzug war ein Echttest verbunden, d.h. die redundanten Systeme inkl. Backup mussten ausgeschaltet und am neuen Standort wieder in

Betrieb genommen werden. Die Prüfung der EFK kurz nach dem Umzug hat gezeigt, dass dieses Vorgehen dank einer detaillierten vorgängigen Planung (BCP) sehr gut funktioniert hat.

Im Rahmen der aktuellen Pandemie-Vorsorgen hat die EFK ein Risiko vorgefunden, das nicht überall wahrgenommen wird. Bei allen VE bestehen Überlegungen und zum Teil auch fortgeschrittene Planungen, dass die Mitarbeitenden ihre Aufgaben von zu Hause aus erledigen könnten. Hierzu benötigen sie einen sicheren Remote-Anschluss (RAS) auf das Netzwerk des Bundes. Diese Zugriffe sind bereits heute in unterschiedlicher Anzahl bei allen VE im Einsatz, werden jedoch eher selten oder nur von einzelnen Mitarbeitenden regelmässig benutzt. Das Revisionsteam hat aufgrund der Angaben aus den geprüften VE die Annahme getroffen, dass im Schnitt 30-50 Mitarbeitende pro Amt auf eine solche Verbindung zurückgreifen könnten oder vielmehr möchten. Auf die rund 75 VE des Bundes hochgerechnet, würden somit zwischen 2‘000 und 4‘000 RAS-Verbindungen benötigt. Nach Abklärungen mit dem BIT verfügte dieses zum Zeitpunkt der Revision über 1‘000 Lizenzen, die im Durchschnitt zu ca. 50% benutzt werden. Die kurzfristige Beschaffung von weiteren Lizenzen wäre gemäss Auskunft der Verantwortlichen innert kurzer Frist möglich, jedoch stösst die Infrastruktur irgendwann an eine Grenze. Es muss auch berücksichtigt werden, dass für eine RAS-Verbindung das Internet funktionieren muss, was von externen Providern und Netzbetreibern ausserhalb des Bundes abhängt. Auch diese Unternehmen können unter Umständen nicht mehr innerhalb der normalen Fristen reagieren, wenn ihnen die Mitarbeitenden infolge der Pandemie in grosser Anzahl ausfallen.

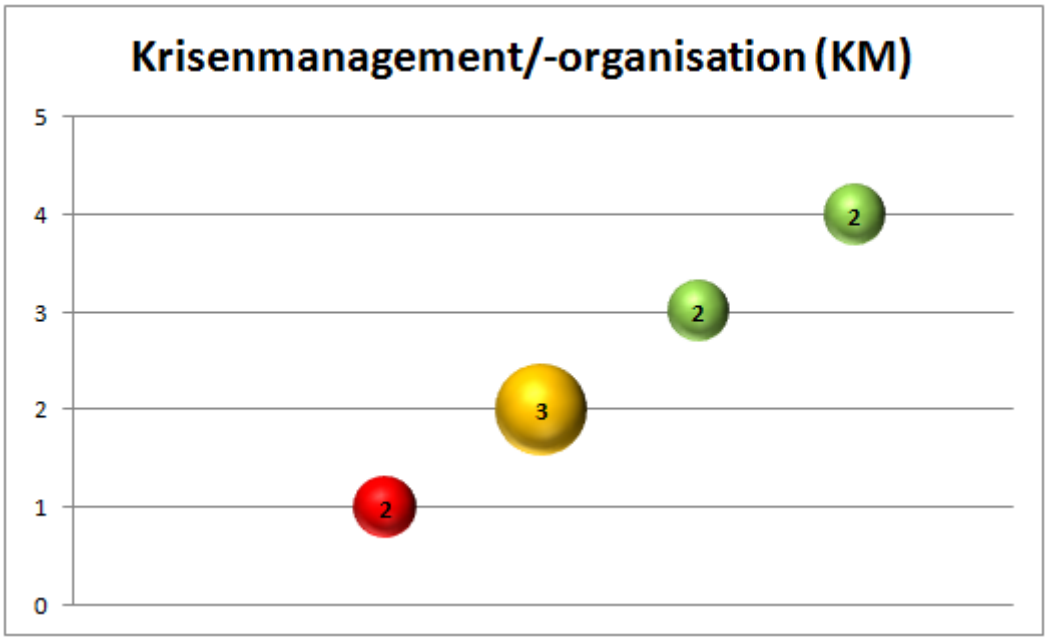
Insgesamt erachtet die EFK das BCP bei den meisten geprüften VE als ungenügend, weil zu sehr auf ad hoc-Lösungen vertraut wird und wichtige Details nicht geregelt sind. In den Köpfen von Schlüsselpersonen mag das genaue Vorgehen vorhanden sein und im Ernstfall auch funktionieren. Fällt aber eine Schlüsselperson aus, dann entsteht ein Vakuum, das durch die übrigen Mitarbeitenden nur mit Zeitaufwand und unter Begehung von unnötigen Fehlern aufgefangen werden kann. Daher müssen die wichtigsten Daten zu Papier gebracht und allen notwendigen Personen verfügbar gemacht werden.

6 Krisenmanagement und Krisenorganisation sind wichtige Elemente zur Bewältigung von ausserordentlichen Situationen

6.1 Nur wer seine Aufgaben kennt, kann in Krisensituationen seine Verantwortung wahrnehmen und notwendige Entscheidungen termingerecht treffen

Unter Krisenmanagement (KM) werden alle Vorkehrungen verstanden, die dazu dienen, dass eine Krisensituation wirksam und zeitgerecht bewältigt werden kann. Wenn auftauchende Probleme nicht innerhalb des Tagesgeschäftes gelöst werden können, muss eine separate Organisation (Krisenstab) eingesetzt werden, die sich der Bewältigung einer möglicherweise beginnenden Krise annimmt bis der Normalzustand wieder erreicht ist. Die Sicherheit der Mitarbeitenden muss dabei im Vordergrund stehen und über institutionalisierte Kommunikationskanäle der Informationsfluss gewährleistet sein. Jedes Mitglied eines Krisenstabes muss seine Aufgaben, Kompetenzen und Verantwortlichkeiten kennen und über die notwendigen Hilfsmittel rasch verfügen können. Regelmässige Übungen mit dem Krisenstab gehören daher genauso zu einem Krisenmanagement wie die mindestens jährliche Überprüfung und Aktualisierung der vorhandenen Dokumente.

6.2 Die „Fitness“ lässt zu wünschen übrig, weil zu wenig definiert ist und ungenügend geübt wird



Es hat sich gezeigt, dass VE mit Aufsichtsfunktionen im Bereich Krisenmanagement eingespielt sind. Diese Erkenntnis überrascht grundsätzlich nicht, da die Bewältigung von ausserordentlichen Situationen, ausgelöst durch bundesexterne Ereignisse, zu den Kernaufgaben dieser VE gehören. Überrascht haben daher mehr die übrigen VE, bei denen ganz wesentliche Elemente nicht oder

nur ansatzweise vorhanden waren. Im Falle der Bundesverwaltung dürfte die Bedrohung der Existenz nicht im Vordergrund stehen, trotzdem kann bei bestimmten VE durch einen Zeitverlust wirtschaftlicher Schaden entstehen, der grosse Nachwirkungen zeigen könnte. In der operativen Ebene sind überall verantwortliche Schlüsselpersonen am Werk, die sehr genau wissen, wie in einem Krisenfall vorzugehen ist. Dieses Vorgehen ist jedoch nur auf einen kleinen eingeschränkten Wirkungskreis fixiert und oft weder niedergeschrieben noch an Stellvertretende weitergegeben. Auch auf der Führungsebene sind Vorstellungen oder teilweise Erfahrungen vorhanden, wie in einer Krisensituation reagiert werden sollte. Aber auch hier können wichtige Aspekte übersehen werden, wenn nicht systematisch vorgegangen wird.

Krisenmanagement kann mit einer Uhr verglichen werden, die nur dann gut läuft, wenn jedes einzelne Zahnrad genau auf die anderen abgestimmt ist und reibungslos ineinander gleitet. Blockiert nur ein einziges dieser Rädchen, so bleiben auch die Zeiger stehen. Genauso verhält es sich in einem Krisen- oder Katastrophenfall. Viele einzelne Mitarbeitende müssen dazu beitragen, dass ein Problem gelöst werden kann. Der Krisenstab muss die generelle Übersicht behalten und entscheiden, wo die Prioritäten gesetzt werden. Die operative Ebene sorgt anschliessend dafür, dass ausgefallene Zahnräder ersetzt und die Uhr wieder zum Laufen gebracht wird. Eine solche Zusammenarbeit muss dokumentiert und vor allem regelmässig geübt werden. Nur wer sich fit hält, ist auf ein unvorhergesehenes Ereignis vorbereitet und kann entsprechend reagieren.

Die EFK beurteilt jene VE, die sich gemäss Grafik im gelben oder sogar roten Bereich befinden als zu wenig fit, um zum heutigen Zeitpunkt eine Krisensituation den eigenen oder gesetzlichen Anforderungen entsprechend meistern zu können. Auch die bundesweiten Strategischen Führungsübungen zeigen Handlungsbedarf hauptsächlich in der Führungsebene. Diese trägt schlussendlich die Verantwortung für die Bewältigung einer Krisen- oder Katastrophensituation und muss dafür sorgen, dass die definierten kritischen Kernaufgaben über alle ausserordentlichen Lagen hinweg im geforderten zeitlichen Rahmen ausgeführt werden können.

7 Lässt sich aufgrund der beurteilten Verwaltungseinheiten ein Gesamtbild für die Bundesverwaltung ableiten?

7.1 Die neun durchgeführten „Stichproben“ lassen eine bundesweite Beurteilung zu

Wie im Kapitel 1.1 dargelegt, wurden die VE für die Querschnittsprüfung aufgrund verschiedener Kriterien durch die EFK ausgewählt. Mit dieser Auswahl werden wichtige und zentrale Kernaufgaben des Bundes abgedeckt. In den einzelnen VE wurden hauptsächlich im Rahmen der Pandemie-Vorsorge jene Geschäftsprozesse definiert, die über alle ausserordentlichen Situationen hinweg ausgeführt werden müssen. Aufgrund der bundesweiten Vorgaben müsste jede VE diese Planung vornehmen und mindestens die notwendige Anzahl Mitarbeitende zur Aufgabenerfüllung festlegen. Das Revisionsteam geht daher davon aus, dass zum heutigen Zeitpunkt in allen VE Basisarbeiten ausgeführt worden sind und eine Gesamtprüfung ähnliche Resultate zeigen könnte. Dabei muss aber berücksichtigt werden, dass nicht jede VE gleich kritische Aufgaben hat und die VE auch unterschiedlich gross sind. Dadurch ist das Schadenspotential mindestens im finanziellen Bereich ebenso unterschiedlich.

Gesamthaft beurteilt schneiden die BIA und das Krisenmanagement am Besten ab, gefolgt vom BCP, vernachlässigt steht dagegen die BCS da. Von allen beurteilten VE fällt das BAG positiv auf. Hier hat das Revisionsteam aufgrund der Resultate eine direkte Bestätigung erhalten, dass sich die Vorgaben des BS25999 – der eingesetzte Fragebogen basiert darauf – inhaltlich und formell in der Praxis erfüllen lassen. Auch wenn vorläufig die Geschäftsleitung des BAG ihr BCM bewusst nur auf die Pandemievorsorge ausgerichtet hat, sind alle vom Revisionsteam erwarteten Dokumente vorhanden, inklusive der allgemein verpönten BCS. Die zusammen mit einer externen Firma erarbeiteten Grundlagen lassen sich mit wenig Aufwand erweitern, so dass alle möglichen Krisenszenarien abgebildet sind und für das BCM in kurzer Zeit ein Reifegrad 4 gemäss Maturity Model erreicht werden kann.

7.2 Die EFK sieht Handlungsbedarf

Die Grafiken der Kapitel 3-6 zeigen den Handlungsbedarf pro Themengebiet deutlich auf. Viele Basisarbeiten und auch vorgewiesene Dokumentationen sind erst in den letzten Monaten entstanden, was zeigt, dass das Thema BCM bisher nicht eine hohe Priorität hatte. Das Revisionsteam konnte aber allgemein feststellen, dass die drohende Pandemie eine Sensibilisierung vor allem in den Führungsgremien bewirkt hat. Entsprechend sind überall „Baustellen“ vorhanden, die in ein paar Wochen bis spätestens in ein paar Monaten abgeschlossen sein sollen. Die an die VE abgegebenen Teilberichte zeigen den involvierten Geschäftsleitungen, wo noch Handlungsbedarf besteht und die „Baustellen“ etwas grösser gestaltet werden sollten.

Die EFK wurde punktuell positiv überrascht von teilweise schon fast ausgereiften Analysen und Plänen sowie Krisenstäben, die einwandfrei zu funktionieren scheinen. Bundesweit müssen aber weitere Anstrengungen unternommen werden. Die EFK begrüsst daher das Vorgehen der GSK (siehe Kapitel 2.4) mit dem an die BK delegierten Projekt, sieht aber zusätzlichen Handlungsbedarf bei den heute fehlenden verbindlichen Vorgaben zum Thema BCM.

Die EFK empfiehlt der GSK, das Thema BCM bundesweit zu vertiefen und dabei zu prüfen, ob und welche Minimalstandards für die Bundesverwaltung als verbindlich erklärt werden müssen.

8 Schlussbesprechung

Die Schlussbesprechung fand am 12. August 2009 mit den delegierten Mitarbeitenden der geprüften VE statt. Die Schlussbesprechung ergab Übereinstimmung bezüglich des dargestellten Ist-Zustandes und der daraus abgeleiteten Verbesserungsmöglichkeiten.

Allen Mitarbeiterinnen und Mitarbeitern sei für die gewährte Unterstützung bestens gedankt.

Anlässlich der GSK-Sitzung vom 14. Dezember 2009 wurde der Bericht bzw. die Empfehlung mit Direktionsmitgliedern der EFK diskutiert. Nach kontroverser Diskussion wurde beschlossen, die Empfehlung nicht umzusetzen mit der Begründung, dass BCM eine Aufgabe der Ämter und Departemente sei. Die Departemente werden in ihrem Bereich prüfen, welches die strategisch wichtigen Bereiche sind und ob Handlungsbedarf besteht. Die Vertreter der EFK nahmen dieses Ergebnis zur Kenntnis und teilten mit, dass für die EFK kein weiterer Handlungsbedarf besteht.

Anhang 1: Erläuterungen zum Maturity Model

Die EFK hat sich bei der Beurteilung des Prozessreifegrades am nachfolgenden Maturity Model orientiert. Damit soll erreicht werden, dass bei der Beurteilung der einzelnen Themen für alle Ämter derselbe transparente Massstab angewendet wird. Die Prozessreife lässt sich dabei nicht immer auf einzelne Detailfragen herunter brechen; viel mehr muss sie im Gesamtzusammenhang betrachtet werden. Die EFK hat diesem Umstand Rechnung getragen, indem das grafisch dargestellte Ergebnis durch ergänzende Kommentare ergänzt wurde.

Level	Beschreibung
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 soweit 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

Anhang 2: Abkürzungen

BAG	Bundesamt für Gesundheit
BBL	Bundesamt für Bauten und Logistik
BCM	Business Continuity Management
BCP	Business Continuity Planning
BCS	Business Continuity Strategy
BIA	Business Impact Analysis
BIT	Bundesamt für Informatik und Telekommunikation
BS	British Standard, z.B. BS25999
BVerw	Bundesverwaltung
BWL	Bundesamt für wirtschaftliche Landesversorgung
COBIT	Control Objectives for Information and Related Technology (Herausgeber IT Governance Institute)
EFK	Eidgenössische Finanzkontrolle
EFV	Eidgenössische Finanzverwaltung
FINMA	Finanzmarktaufsicht
GSK	Generalsekretärenkonferenz
IRB	Informatikrat des Bundes
ISB	Informatikstrategieorgan des Bundes
IT	Information Technology
KM	Krisenmanagement
KMA	Krisenmanagementausbildung
LB	Leistungsbezüger
LE	Leistungserbringer
RAS	Remote Access Service (sicherer Zugriff auf das Netzwerk des Bundes)
SECO	Staatssekretariat für Wirtschaft
VBS	Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport
VE	Verwaltungseinheit
WHO	World Health Organisation
WIsB	Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung