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

Business Continuity Management

Querschnittsprüfung bei der dezentralen Bundesverwaltung, der Schweizerischen Post und den Schweizerischen Bundesbahnen

November 2010

Impressum

Bestelladresse **Adresse de commande** **Indirizzo di ordinazione** **Order address**	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45, CH - 3003 Bern http://www.efk.admin.ch/I
Bestellnummer **Numéro de commande** **Numero di ordinanzione** **Order number**	1.10387.100.00373.32
Zusätzliche Informationen **Complément d'informations** **Informazioni complementari** **Additional information**	Fachbereich 4 „Informatikprüfungen“ E-Mail: cornelia.simmen@efk.admin.ch Tel. +41 31 324 10 83
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 »)
Abdruck **Reproduction** **Riproduzione** **Reproduction**	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorised (please mention the source)

Business Continuity Management
Querschnittsprüfung bei der dezentralen Bundesverwaltung, der Schweizerischen Post und den Schweizerischen Bundesbahnen

Das Wesentliche in Kürze

Welchen Stellenwert hat das Business Continuity Management (BCM)?

Business Continuity Management bedeutet, dass alle notwendigen Vorkehrungen getroffen werden, damit ein Unternehmen seine Kerngeschäfte selbst in ausserordentlichen Lagen termingerecht erfüllen kann. Die Eidg. Finanzkontrolle (EFK) hat bereits im Jahr 2009 eine Querschnittsprüfung bei neun Verwaltungseinheiten der zentralen Bundesverwaltung zum Thema BCM durchgeführt. Im Fokus der diesjährigen Prüfung lagen die dezentrale Bundesverwaltung sowie die SBB (Schienenverkehr und Billettverkauf) und Post (Postfinance, Swiss Post Solutions, PostAuto).

Die Verwaltungseinheiten der dezentralen Bundesverwaltung haben gesetzliche Aufträge als Aufsichts- oder Zulassungsbehörde. Die erbrachten Monopol-Dienstleistungen werden durch die Kunden finanziert. Die SBB und PostAuto erfüllen einen „service publique“, welcher über Leistungsaufträge definiert ist und teilweise mit Mitteln der öffentlichen Hand gestützt wird. PostFinance und Swiss Post Solutions (SPS) verkaufen dagegen ihre Dienstleistungen in einem offenen Markt. Diese unterschiedlichen Ausgangslagen haben einen direkten Einfluss darauf, wie kritisch die Geschäftsprozesse und die dafür notwendigen Ressourcen sind. Das Revisionsteam hat festgestellt, dass Konkurrenz im Markt einen wesentlichen Einfluss auf den Stellenwert von BCM in den betroffenen Organisationen/Unternehmen hat.

Ein vollständiges, in der Praxis umgesetzte BCM beginnt mit einer Policy und endet bei regelmässigen Überprüfungen

Das Management legt in einer ***Policy*** ihre Ziele zum BCM fest und definiert die Verantwortlichkeiten. Grundsätze konnten alle Organisationen vorweisen, allerdings nicht immer in Form eines von der obersten Führung freigegebenen und für alle Mitarbeitenden verbindlichen Dokumentes. Zum Zeitpunkt der Prüfung befanden sich dahingehende Projekte oder Dokumente noch in Arbeit. Die Hälfte der gesichteten Unterlagen entsprach den formellen Anforderungen an eine Policy.

Zur Erstellung einer ***Business Impact Analysis (BIA)*** müssen die Geschäftsprozesse und die dafür notwendigen Ressourcen erfasst werden. Ohne diese Basis lassen sich weder Risiken noch deren Auswirkungen auf die Prozesse einschätzen. Die Überprüfung von strategischen Risiken erfolgt bei den meisten Organisationen seit Jahren systematisch und regelmässig. Bei einigen Organisationen basiert die BIA auf diesen Daten, bei anderen fliessen die in der BIA beurteilten Risikoszenarien über Konsolidierungen in das Riskmanagement ein. Fünf Organisationen haben Musterbeispiele vorlegen können, wie eine BIA auch in einem komplexen Umfeld erfolgreich durchgeführt werden kann. Bei der BIA sind in einigen Fällen Lücken in den beschriebenen

Geschäftsprozessen bzw. den notwendigen Ressourcen sowie den Risikoszenarien festgestellt worden. Zudem sollten die zeitlichen Aspekte vermehrt in die Analysen einbezogen werden.

Aussagen zur ***Business Continuity Strategy (BCS)*** waren überall vorhanden. Bei den SBB und PostAuto sind diese sogar gesetzlich verankert. Die Organe der dezentralen Bundesverwaltung haben mehrheitlich Geschäftsprozesse, die über längere Zeit ausfallen können, ohne dass dabei der Kunde unmittelbar betroffen ist. In der Regel sind auch die damit verbundenen Ressourcen nicht zeitkritisch. Das BCS reduziert sich bei diesen Organisationen auf ein paar Kernaussagen. Bei den SBB und den geprüften Bereichen der Post sind dagegen viele Geschäftsprozesse und Ressourcen zeitkritisch. Entsprechend werden alle möglichen präventiven Massnahmen umgesetzt, damit eine Krisenlage erst gar nicht entstehen kann. Die namentlich genannten Organisationen haben mit ihren strategischen Regelungen überzeugt.

Das ***Business Continuity Planning (BCP)*** beinhaltet Regelungen und Dokumente, um im Krisenfall eine rasche Wiederherstellung der normalen Geschäftstätigkeit erreichen zu können. Insgesamt haben fünf Organisationen mit umfangreichen Vorgehensplänen und Checklisten zu differenzierten Risikoszenarien überzeugt. Verschiedene Dokumente können noch zu einem Regelwerk vereint oder einheitliche Vorgaben erstellt werden. Bei den anderen Organisationen wurde empfohlen, dass man sich trotz unkritischer Geschäftsprozesse Gedanken macht, welche Szenarien zu einem längeren Unterbruch der Geschäftstätigkeiten führen könnten und was in einem solchen Fall zu tun wäre. Alle Organisationen haben Krisenstäbe und auch das Management von Krisen definiert. Das Revisionsteam hat davon mehrheitlich einen sehr guten Eindruck erhalten.

Nur wer regelmässig übt, was im BCP festgelegt ist (***Test***), wird im Ernstfall die notwendige Fitness (***Awareness***) aufweisen, um eine Krise zeitgerecht zu überwinden. Übungen können auf unterschiedlichste Art durchgeführt werden (z.B. Dokumentenreviews, Gebäudeevakuierungen, Unterbrechung der Stromzufuhr, Risikoszenarien im Krisenstab durchgehen, usw.). Die Mehrheit der Organisationen führt solche in verschiedenen Bereichen durch. Diese basieren teilweise auf Einzeldokumenten oder werden aufgrund einer Jahres- oder Mehrjahresplanung vorgenommen. Die SBB, Postfinance und SPS gehen dabei systematisch und konsequent vor. Bei den anderen Organisationen fehlen entweder Testkonzepte/-planungen oder die Systematik. Bei der Awareness kann noch Einiges verbessert werden.

Die geprüften Organisationen/Unternehmen schneiden im Vergleich zur zentralen Bundesverwaltung gut ab

Im Vorjahr hat eine einzige Verwaltungseinheit einen durchschnittlichen Reifegrad von 3 gemäss Maturity Model (siehe Anhang 1) ausweisen können, alle anderen Einheiten lagen darunter, zur Hälfte sogar unter 2.

Dagegen haben alle nun überprüften Organisationen/Unternehmen einen Reifegrad von mindestens 3 erfüllt, fünf erreichen sogar einen Durchschnitt von 4 oder mehr. Unternehmensstrategien, der Wille der Geschäftsleitungen und ein prozessorientiertes Handeln aufgrund von Zertifizierungen nach internationalen Standards spielen dabei eine grosse Rolle.

Massgebend für ein vollständiges, formell korrektes und in der Praxis umgesetztes BCM scheint aber auch die Stellung im Markt zu sein. Je mehr Konkurrenz bei der Dienstleistung vorhanden ist, desto höher fällt der Reifegrad des aufgesetzten BCM aus. Eine Ausnahme von dieser Aussage bildet das IGE, welches trotz unkritischer Geschäftsprozesse in der höchsten Liga mitspielt.

Aufgefallen ist, dass das Thema BCM bei allen geprüften Organisationen und Geschäftsbereichen einen hohen bis sehr hohen Stellenwert hat. Entsprechend sind auch in den meisten Organisationen Verantwortliche ernannt, die sich regelmässig mit der Umsetzung der damit verbundenen Anforderungen auseinandersetzen.

Die Finanzdelegation der eidgenössischen Räte hat an der ordentlichen Sitzung im Februar 2011 vom Bericht Kenntnis genommen.

Gestion de la continuité des affaires

Audit transversal auprès de l'administration fédérale décentralisée, de La Poste suisse et des Chemins de fer fédéraux

L'essentiel en bref

Quelle est l'importance de la gestion de la continuité des affaires (*Business Continuity Management*; *BCM*)?

La gestion de la continuité des affaires signifie que toutes les dispositions sont prises pour qu'une entreprise puisse poursuivre sans interruption ses activités essentielles même dans des situations extraordinaires. Le Contrôle fédéral des finances (CDF) a déjà mené en 2009 un audit transversal sur le BCM auprès de neuf unités de l'administration centrale de la Confédération. L'audit de 2010 s'est focalisé sur l'administration fédérale décentralisée, sur les CFF (trafic ferroviaire et vente de billets) et sur La Poste suisse (PostFinance, Swiss Post Solutions, PostAuto).

Les unités administratives de l'administration fédérale décentralisée ont des mandats légaux en qualité d'autorités de surveillance ou d'homologation. Leurs prestations monopolistiques sont financées par leurs clients. Les CFF et PostAuto assurent un « service public » défini dans des mandats de prestations et partiellement financé par les pouvoirs publics. En revanche, PostFinance et Swiss Post Solutions (SPS) vendent leurs prestations sur le marché libre. Ces situations ont une influence directe sur le caractère crucial de leurs processus d'affaires et les ressources nécessaires. Le groupe de réviseurs a constaté que la concurrence du marché conditionnait dans une large mesure l'importance accordée au BCM par les diverses organisations et entreprises.

Un BCM complet et mis en pratique commence par la définition d'une politique et se termine par des examens réguliers

La direction définit une ***politique*** précisant les objectifs du BCM et attribue les responsabilités. Toutes les organisations ont fixé des principes, sans nécessairement disposer d'un document approuvé par les plus hautes instances et valables pour l'ensemble du personnel. Au moment de l'audit, des projets et documents correspondants étaient encore en phase d'élaboration. La moitié des documents consultés répondait aux exigences formelles d'une politique.

Une ***analyse d'impact sur les affaires*** (Business Impact Analysis; ***BIA***) implique que l'on saisisse les processus d'affaires et les ressources nécessaires. Sans ces pré-requis, il est impossible d'évaluer les risques et leurs effets sur les processus. La plupart des organisations évaluent depuis des années les risques stratégiques, de manière systématique et à intervalles réguliers. Dans certaines organisations, le BIA se fonde sur ces données, et dans d'autres, les scénarios étudiés sont repris dans la gestion des risques après consolidation. Cinq organisations ont pu fournir des exemples de la manière dont une BIA a été menée avec succès dans un environnement complexe. Des lacunes sont apparues pour certaines BIA en ce qui concerne la description des processus, les ressources nécessaires ou encore les scénarios de risques. De plus, il faudrait davantage tenir compte de la dimension temporelle dans l'analyse.

Toutes les organisations ont été en mesure de se prononcer sur la ***stratégie de continuité des affaires*** (Business Continuity Strategy; ***BCS***). Auprès des CFF et de PostAuto, ces considérations sont même inscrites dans la législation. La plupart des organisations de l'administration fédérale décentralisée ont des processus d'affaires susceptibles de connaître des pannes de longue durée sans que la clientèle n'en soit directement affectée. En règle générale, les ressources y afférentes ne sont pas critiques non plus sous l'angle temporel. La BCS se limite dans ces cas à quelques notions générales. Auprès des CFF et des domaines de La Poste passés en revue, de nombreux processus d'affaires et ressources sont critiques. Dès lors, on s'efforce de mettre en œuvre toutes les mesures préventives afin d'éviter une situation de crise. Les réglementations stratégiques des organisations citées sont convaincantes.

La ***planification de la continuité des affaires*** (Business Continuity Planning; ***BCP***) comporte des réglementations et des documents visant à rétablir rapidement l'activité normale en cas de crise. En tout, cinq organisations ont convaincu par leurs plans d'action exhaustifs et leurs listes de contrôle pour différents scénarios de risques. Divers documents pourraient encore être réunis en une réglementation complète ou faire l'objet de prescriptions uniformes. En ce qui concerne les autres organisations, le CDF leur a recommandé, malgré l'absence de caractère crucial de leurs processus, de réfléchir néanmoins aux scénarios qui pourraient mener à une interruption durable de leurs activités et de définir les mesures à prendre dans un tel cas. Toutes les organisations disposent d'un état-major de crise, et elles ont défini les modalités de gestion des crises. Le groupe de réviseurs a retiré une impression favorable de la plupart des dispositions prises.

Ce n'est qu'en appliquant régulièrement les préceptes du BCP (***test***) que l'on acquerra la sensibilité (***awareness***) dont on aura besoin pour maîtriser une crise en temps utile. Les exercices prennent les formes les plus diverses (par ex. familiarisation avec la documentation, évacuations de bâtiments, rupture de l'approvisionnement en électricité, passage en revue des scénarios de risques au sein de l'état-major, etc.). La plupart des organisations mènent des tests dans divers domaines. Les exercices se fondent sur des documents particuliers ou sont organisés selon une planification annuelle ou pluriannuelle. Les CFF, PostFinance et SPS privilégient à cet égard une démarche systématique et conséquente. Dans les autres organisations, on constate l'absence d'un programme de tests ou d'une systématique. En matière de sensibilité, des améliorations restent possibles.

Les organisations et entreprises auditées se positionnent mieux que l'administration fédérale centrale

L'année précédente, une seule unité administrative affichait un coefficient de maturité de 3 selon le « Maturity Model » de l'annexe 1. Toutes les autres unités se situaient en-deçà, certaines n'atteignant même pas la note 2.

En revanche, toutes les organisations et entreprises auditées en 2010 atteignaient un coefficient de maturité de 3 au moins, et cinq affichaient même une moyenne de 4 ou supérieure de 4. La

stratégie d’entreprise, la volonté de la direction et une conduite axée sur les processus, assortie de certifications selon les normes internationales, jouent un rôle important à cet égard.

La position sur le marché semble également déterminante pour un BCM complet, formellement conforme et mis en pratique. Le degré de maturité du BCM est d’autant plus élevé que les prestations sont soumises à la concurrence. L’IPI constitue une exception : malgré ses processus peu critiques, il se classe parmi les meilleurs.

On a constaté que toutes les organisations et secteurs d’activités examinés accordaient une grande importance au BCM. Il en résulte que dans la plupart des organisations, des responsables ont été désignés qui se confrontent régulièrement à la mise en œuvre du BCM et aux exigences qui y sont liées.

La Délégation des finances des Chambres fédérales a pris connaissance du rapport lors de sa séance ordinaire du mois de février 2011.

Gestione della continuità aziendale
Verifica trasversale presso l'Amministrazione federale decentralizzata, la Posta svizzera e le Ferrovie federali svizzere

L’essenziale in breve

Che importanza ha la gestione della continuità aziendale *(Business Continuity Management, BCM)?*

Con *gestione della continuità aziendale* si intende che tutte le misure necessarie vengono prese affinché un'impresa possa adempiere tempestivamente i suoi compiti essenziali anche in situazioni straordinarie. Già nel 2009 il Controllo federale delle finanze (CDF) aveva effettuato una valutazione trasversale concernente il BCM presso 9 unità amministrative dell'Amministrazione federale centralizzata. La verifica di quest’anno si concentra sull'Amministrazione federale decentralizzata, sulle Ferrovie federali svizzere FFS (traffico ferroviario e vendita di biglietti) e sulla Posta (Postfinance, Swiss Post Solutions, PostAuto).

Le unità amministrative dell'Amministrazione federale decentralizzata hanno mandati legali quali autorità di vigilanza o di autorizzazione. Le prestazioni monopolistiche fornite sono finanziate dai clienti. Le FFS e PostAuto adempiono un servizio pubblico, definito da mandati di prestazione e in parte sostenuto con mezzi dell'ente pubblico. PostFinance e Swiss Post Solutions (SPS) vendono invece le loro prestazioni sul libero mercato. Queste diverse situazioni iniziali influiscono direttamente sul grado di criticità dei processi lavorativi e delle relative risorse necessarie. Il gruppo di revisione ha constatato che la concorrenza sul mercato influisce notevolmente sull'importanza del BCM nelle organizzazioni/imprese interessate.

Un BCM completo e messo in atto inizia con una *Policy* e finisce con verifiche regolari

La direzione stabilisce i suoi obiettivi concernenti il BCM in una ***Policy*** e definisce le responsabilità. Tutte le organizzazioni hanno stabilito i loro principi, ma non sempre sotto forma di documento approvato dalla direzione suprema e vincolante per i collaboratori. Al momento della verifica i relativi progetti o documenti erano ancora in fase di elaborazione. La metà della documentazione esaminata corrispondeva ai requisiti formali di una *Policy*.

Per l'esecuzione di un’***analisi di impatto sull’operatività*** (Business Impact Analysis, ***BIA***) devono essere rilevati i processi lavorativi e le relative risorse necessarie. Senza questa base non è possibile valutare né i rischi né le loro ripercussioni sui processi. Nella maggior parte delle organizzazioni la verifica dei rischi strategici avviene da anni in modo sistematico e regolare. In alcune organizzazioni il BIA si basa su questi dati mentre in altri gli scenari di rischio valutati nel BIA confluiscono, dopo il consolidamento, nel management dei rischi. Cinque organizzazioni hanno potuto presentare esempi su come sia possibile effettuare con successo un BIA anche in un contesto complesso. Per quanto riguarda il BIA, in alcuni casi sono state rilevate lacune nella descrizione dei processi lavorativi, nelle risorse necessarie e negli scenari di rischio. Nelle analisi bisognerebbe inoltre tenere maggiormente conto degli aspetti temporali.

Tutte le organizzazioni e imprese oggetto della verifica hanno fatto considerazioni sulla ***strategia di continuità operativa*** (Business Continuity Strategy, ***BCS***). Presso le FFS e PostAuto queste considerazioni sono addirittura ancorate nella legge. La maggior parte dei processi lavorativi degli organi dell'Amministrazione federale decentralizzata può arrestarsi per lungo tempo senza che il cliente ne sia direttamente colpito. Di regola anche le relative risorse non presentano criticità nell'ottica temporale. Pertanto presso queste organizzazioni il BCS si riduce a un paio di constatazioni di base. Per contro, presso le FFS e i settori verificati della Posta molti processi lavorativi e risorse sono critici. Di conseguenza vengono attuate tutte le possibili misure preventive affinché non possa affatto sorgere una situazione di crisi. Dette organizzazioni hanno convinto con le loro regolamentazioni strategiche.

Il ***piano di continuità operativa*** (Business Continuity Planning, ***BCP***) contiene regolamentazioni e documenti per poter ripristinare rapidamente i normali processi lavorativi in caso di crisi. Complessivamente cinque organizzazioni hanno convinto con esaustive pianificazioni delle procedure e liste di controllo per differenti scenari di rischio. Diversi documenti possono essere inoltre riuniti in un quadro normativo oppure in direttive uniformi. Malgrado l'assenza di processi lavorativi critici, nelle altre organizzazioni è stato consigliato di riflettere su quali sarebbero gli scenari che provocherebbero un'interruzione prolungata delle attività lavorative e cosa bisognerebbe intraprendere in questi casi. Tutte le organizzazioni dispongono di stati maggiori di crisi e hanno definito la gestione delle crisi. Il gruppo di revisione ha ricavato per lo più un'ottima impressione.

Solo chi applica regolarmente ciò che è stabilito nel BCP (***test***) dispone della necessaria pratica (***awareness***) per superare tempestivamente una crisi in caso di emergenza. Gli esercizi possono essere effettuati nei modi più disparati (ad es. revisione dei documenti, evacuazioni dello stabile, interruzione dell'approvvigionamento elettrico, discussione degli scenari di rischio da parte dello stato maggiore di crisi ecc.). La maggior parte delle organizzazioni effettua tali esercizi nei diversi settori. Questi si basano in parte su documenti singoli oppure sono eseguiti sulla base di una pianificazione annuale o pluriennale. Le FFS, Postfinance e SPS procedono in modo sistematico e coerente. Presso le altre organizzazioni mancano i concetti/le pianificazioni dei test oppure la sistematica. In ambito di *awareness* esiste tutt'ora un potenziale di miglioramento.

Rispetto all'Amministrazione federale centralizzata le organizzazioni/imprese esaminate ottengono migliori risultati

L'anno precedente solo un'unità amministrativa ha potuto dimostrare un livello di maturità medio, ovvero 3, secondo il *Maturity Model* (vedi allegato 1) mentre tutte le altre unità erano sotto questo valore; la metà non raggiungeva addirittura il livello 2.

Tutte le organizzazioni/imprese esaminate hanno dimostrato invece di raggiungere almeno il livello di maturità 3 mentre 5 di loro hanno raggiunto o addirittura superato in media il livello 4. In questo

contesto svolgono un ruolo importante le strategie d'impresa, la volontà delle direzioni e un operato orientato ai processi sulla base di certificazioni secondo gli standard internazionali.

Anche la posizione sul mercato è determinante per un BCM completo, corretto dal punto di vista formale e messo in atto. Maggiore è la concorrenza riguardo alla prestazione, più alto è il livello di maturità del BCM. L'Istituto federale della proprietà intellettuale (IPI) costituisce l'eccezione a questa affermazione, poiché malgrado l'assenza di processi lavorativi critici rientra nella classe superiore.

Occorre rilevare che la tematica BCM riveste grande importanza in tutte le organizzazioni e in tutti i settori lavorativi esaminati. Di conseguenza nella maggior parte delle organizzazioni sono stati nominati dei responsabili che si confrontano regolarmente con l'attuazione delle pertinenti esigenze.

Le Delegazioni delle finanze delle Camere federali hanno preso atto del rapporto in occasione della seduta ordinaria del mese di febbraio 2011.

Business Continuity Management
Cross-section audit at the decentralised Federal Administration, Swiss Post and the Swiss Federal Railways

Key facts

What importance is attached to Business Continuity Management (BCM)?

Business Continuity Management is a process whereby all necessary measures are taken to ensure that a company can accomplish its core tasks on time even in extraordinary situations. The Swiss Federal Audit Office (SFAO) previously carried out a cross-section audit in 2009 on the BCM measures at nine administrative units of the central Federal Administration. This year's audit focused on the decentralised Federal Administration as well as the Swiss Federal Railways (rail transport and ticket sales) and Swiss Post (PostFinance, Swiss Post Solutions, PostBus).

The administrative units of the decentralised Federal Administration have a legal mandate as a supervisory or licensing authority. Services for which they have a monopoly are funded by their customers. The Swiss Federal Railways and PostAuto provide a public service defined by way of performance contracts and partially financed by public funds. On the other hand, PostFinance und Swiss Post Solutions (SPS) offer their services on the open market. Starting from different positions, this has a direct impact on how critical their business processes and required resources are. The audit team found that the existence of market competition significantly influenced the importance attached to BCM in the various organisations and companies.

A comprehensive BCM solution for practical use starts with a policy and ends with regular audits

Management lays down its BCM objectives in a ***policy*** and defines the various responsibilities. All organisations were found to have set out the basic principles but not always in the form of a binding document applicable to all employees and validated by senior management. Projects or documents of this nature were still in progress at the time of the audit. Half of the documents inspected met the formal requirements of a policy.

In order to perform a ***Business Impact Analysis (BIA)***, an organisation first has to identify its business processes and the resources needed to carry them out. This basic information is crucial to assessing the risks and their impact on the various processes. Most organisations have conducted a systematic and regular audit of their strategic risks for several years now. In some cases, the BIA is based on this data. At other organisations, the risk scenarios evaluated in the BIA are consolidated into the risk management process. Five organisations were able to produce model examples of how to implement a BIA successfully in a more complex environment. In some cases, the business processes or required resources and the risk scenarios outlined in the BIA were found to be deficient. Also, more attention should be given to the time scale in such analyses.

All organisations had drawn up some form of ***Business Continuity Strategy (BCS)***. At the Swiss Federal Railways and PostAuto, these are even enshrined in law. Most of the business processes within the various bodies of the decentralised Federal Administration could actually be interrupted for an extended period of time without having any direct impact on the customer. In general, the resources needed for these are not time critical either. The BCS at such organisations is defined in just a few key statements. At the Swiss Federal Railways and the audited areas of Swiss Post, however, many of the business processes and resources are time critical. These organisations thus take all possible precautions to prevent a crisis situation occurring in the first place. The strategies in place there were found to be in order.

Business Continuity Planning (BCP) comprises a set of rules and documents designed to restore normal business operations quickly in the case of a crisis situation. Five of the organisations produced comprehensive plans of action and checklists for coping with different risk scenarios. Various documents may still be combined to form a set of rules or individual guidelines drawn up. The other organisations, despite not having critical business processes, were advised to explore which scenarios could result in an extended interruption of business activities and what should be done in such situations. All of the organisations have defined crisis teams and crisis management procedures. In most cases, the auditors were very impressed with these.

Only entities that conduct regular BCP drills and ***testing*** will have the required level of ***awareness*** in a real-life situation to deal with a crisis effectively and on time. Such exercises may take a variety of forms (e.g. document reviews, building evacuation drills, simulated power cuts, going through risk scenarios in the crisis management teams). The majority of the organisations do conduct such exercises in different areas. These are based on individual documents in some cases or form part of a programme conducted annually or every few years. The Swiss Federal Railways, PostFinance and SPS take a systematic and consistent approach to this. The other organisations were found to lack either test concepts and plans or a systematic strategy. There is room for improvement in terms of awareness.

The organisations/companies audited compared well against the central Federal Administration

In the previous audit, only one administrative unit obtained an average of 3 in the Maturity Model (see Annex 1), with all others scoring below this and half of them even less than 2.

In contrast, all of the organisations/companies audited this time had a maturity level of at least 3, with five of them even scoring an average of 4 or more. This is largely a result of corporate strategies, management commitment and process-oriented certification methodologies following international standards.

Still, it would appear that the most critical factor in whether a BCM is complete, formally correct and put into practice is the organisation’s market position. The more competition that exists for a

particular service, the higher is the level of maturity of the BCM in place. The Federal Institute of Intellectual Property forms an exception here, ranking among the top performers despite having non-critical business processes.

All organisations and business areas audited were found to regard BCM issues as being important or very important. Correspondingly, most organisations have also appointed individuals responsible for dealing with implementation and the associated requirements.

The Finance Delegation noted the report in its ordinary meeting in February 2011.

Inhaltsverzeichnis

Begriffserklärungen

Business Continuity Management (BCM)	Darunter wird das gesamte Regelwerk verstanden, in welchem festgelegt ist, wie die Geschäftsweiterführung im Krisenfall gehandhabt wird.
Business Continuity Policy	In einer Policy legt das Management die Ziele und Verantwortlichkeiten zur Geschäftsweiterführung fest.
Business Impact Analysis (BIA)	Die Geschäftsprozesse und die dafür notwendigen Ressourcen werden möglichen Risikoszenarien gegenübergestellt. Dabei wird beurteilt, welchen Einfluss der Ausfall von einzelnen oder allen Komponenten auf einer bestimmten Zeitachse hat. Daraus lässt sich ableiten, welche Prozesse und Ressourcen kritisch sind.
Business Continuity Strategy (BCS)	Für die als kritisch definierten Ressourcen muss eine Strategie entwickelt werden, damit deren Ausfall möglichst verhindert wird und wie bei einem unvorhergesehenen Ereignis reagiert werden soll.
Business Continuity Planning (BCP)	Beim Planning werden Vorbereitungen getroffen, damit eine eingetretene Krisensituation bewältigt werden kann. Dies beinhaltet von Checklisten über Ersatzbeschaffungen bis zum Krisenstab alles, was dazu beiträgt, damit rasch möglichst der Normalzustand wieder hergestellt werden kann.
Test und Awareness	Anhand der Planungsunterlagen werden Testkonzepte erstellt, damit die vorbereiteten Bewältigungsszenarien soweit möglich geübt werden können. Dazu bedarf es einer kontinuierlichen Aus-/Weiterbildung (Awareness) aller involvierten Mitarbeitenden.

Anhänge

Anhang 1: Erläuterungen zum Maturity Modell

Anhang 2: Abkürzungen

1 Auftrag und Prüfungsdurchführung

1.1 Auftrag

Die EFK hat bereits im Jahr 2009 eine Querschnittsprüfung zum Thema „Business Continuity Management“ (BCM) bei neun Verwaltungseinheiten (VE) des Bundes durchgeführt.[1] Aufgrund der Resultate und zu Vergleichszwecken führte sie von April bis Oktober 2010 eine weitere Querschnittsprüfung bei vier Verwaltungseinheiten der dezentralen Bundesverwaltung mit eigener Rechtspersönlichkeit, bei einer selbständigen Anstalt des öffentlichen Rechts mit Rechtspersönlichkeit und einer spezialgesetzlichen Aktiengesellschaft durch.

Ausgewählt wurden:

- Eidg. Nuklearsicherheitsinspektorat (ENSI)
- Institut für Geistiges Eigentum (IGE)
- Eidg. Finanzmarktaufsicht (FINMA)
- Schweizerisches Heilmittelinstitut (Swissmedic)
- Die Schweizerische Post in den Geschäftsbereichen Postfinance, Swiss Post Solutions und PostAuto AG
- Schweizerische Bundesbahnen (SBB) in den Geschäftsbereichen Schienenverkehr und Billettverkauf

Der Prüfauftrag lautete:

- Ist bei den ausgewählten Organisationen ein BCM vorhanden, welches die Aufrechterhaltung und zeitgerechte Wiederherstellung der kritischen Geschäftsfunktionen im Krisen- bzw. Katastrophenfall sicherstellt?

Das Revisionsteam hat aus diesem Auftrag folgende Fragen abgeleitet:

1. Bestehen Entscheide des Managements über Ziele, Aktivitäten, Verantwortlichkeiten und Betrieb/Unterhalt eines BCM (Business Continuity Policy)?
2. Sind die kritischen Geschäftsprozesse und die dafür notwendigen Ressourcen festgelegt und priorisiert sowie die damit verbundenen Risiken und deren mögliche Auswirkungen definiert (Business Impact Analysis)?
3. Besteht in der Organisation eine Strategie zur Geschäftsweiterführung (Business Continuity Strategy), d.h. welche vorbeugenden Massnahmen werden ergriffen?
4. Verfügt die Organisation über eine Planung und Krisenorganisation zur Sicherstellung einer kontinuierlichen Geschäftstätigkeit bzw. zeitgerechten Wiederaufnahme der kritischen Geschäftsprozesse nach einem Zwischenfall (Business Continuity Planning)?
5. Wie sieht die Awareness zum BCM aus (stufengerechte Schulungen, Testing, Reporting, Kommunikation usw.)?

[1] Publikation auf http://www.efk.admin.ch/deutsch/prüfungsberichte.htm

1.2 Rechtsgrundlagen / Standards

- Bundesgesetz über die Eidgenössische Finanzkontrolle vom 28. Juni 1967 (Finanzkontrollgesetz, FKG, SR 614.0)
- Finanzhaushaltverordnung vom 5. April 2006 (FHV, SR 611.01)
- British Standard BS25999, Betriebliches Kontinuitätsmanagement Teil 1 und Teil 2
- Empfehlungen für das Business Continuity Management vom November 2007 (herausgegeben von der Bankiervereinigung, SwissBanking, von der FINMA[2] als Mindeststandard anerkannte Selbstregulierung)

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde durch die IT-Prüfungsexperten Markus Künzler und Cornelia Simmen (Revisionsleitung) sowie dem Prüfungsexperten Peter König durchgeführt. Bei den SBB wurde das Team durch Mitarbeitende der Internen Revision aktiv unterstützt. Die Interne Revision der Post hat die notwendigen Kontakte zu den verschiedenen Geschäftsbereichen hergestellt und war an den Schlussbesprechungen vertreten.

Bei den SBB ist aufgrund der Komplexität des Unternehmens in Absprache mit der Internen Revision festgelegt worden, dass nur die direkt kundennahen Bereiche Bahnverkehr und Billettverkauf geprüft wurden. Fokussiert wurde dabei auf die Verfügbarkeit der für diese Geschäftsprozesse notwendigen IT-Anwendungen.

Bei SPS (Post) beschränkte sich die Prüfung auf die Geschäftsbereiche, welche ihren Sitz in der Schweiz haben und die Dienstleistungen auch von der Schweiz aus erbringen.

Bei der PostAuto AG basieren die Beurteilungen ausschliesslich auf Interviews mit Verantwortlichen des Hauptsitzes, die regionalen Organisationen wurden nicht geprüft.

Zur Erfüllung des Prüfauftrages wurden die von den Kunden gelieferten Dokumentationen analysiert. In vertiefenden Interviews mit verantwortlichen Schlüsselpersonen sind die notwendigen Details abgeklärt worden. Einzelheiten über Art und Umfang der durchgeführten Prüfungen gehen aus den Arbeitspapieren hervor.

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, welche auf jede einzelne Frage ausgerichtet wurde. In den nachfolgenden Kapiteln werden die

---

[2] 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

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 Organisationen mit diesem Resultat (Ziffer zeigt Anzahl)
2	gelb	Handlungsbedarf vorhanden, wichtige Elemente, Standardisierung und/oder Dokumentation fehlen	
3 + 4	grün	Kleiner Handlungsbedarf, ergänzende oder formelle Verbesserungen, Einhaltung überwachen und messen, Awareness trainieren	
5	blau	Kein Handlungsbedarf, entspricht „best practice“, d.h. die Bedürfnisse des Unternehmens sind vollständig abgedeckt	

Jede Direktion der geprüften Organisationen bzw. Geschäftsbereiche 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. Insgesamt sind 10 Empfehlungen mit Priorität 1 und deren 11 mit Priorität 2 abgegeben worden, zwei Teilberichte enthielten keine Empfehlungen.

1.4 Unterlagen und Auskunftserteilung

Dem Revisionsteam standen die vorgängig verlangten Dokumente in genügender Tiefe und termingerecht zur Verfügung. Bei allen durchgeführten Interviews wurde sehr offen über die tatsächliche Situation Auskunft gegeben. Dem Revisionsteam wurde auch Einblick in Bereiche gewährt, die normalerweise nur betriebseigenen Mitarbeitenden vorbehalten sind, was zu einer möglichst objektiven Beurteilung beigetragen hat.

2 Einleitung

2.1 Gesetzliche Aufträge versus Marktanteile

Das ENSI, die FINMA, Swissmedic und IGE haben gesetzlich definierte Pflichten, die sie als Aufsichts- oder Zulassungsbehörde erfüllen müssen. Diesen Verwaltungseinheiten der dezentralen Bundesverwaltung werden die erbrachten Monopol-Dienstleistungen durch ihre Kunden entschädigt. Sie sind rechtlich verselbständigte Körperschaften und finanziell unabhängig vom Bund. Die SBB und PostAuto erfüllen einen „service publique“, welcher über Leistungsaufträge definiert ist und nebst den Verkaufseinnahmen mit Mitteln der öffentlichen Hand gestützt wird. PostFinance und SPS verkaufen dagegen ihre Dienstleistungen in einem offenen Markt. Es bestehen damit sehr unterschiedliche Ausgangslagen punkto Geschäftsweiterführung in einem Krisenfall. Das Revisionsteam hat festgestellt, dass der Markt einen wesentlichen Einfluss auf den Stellenwert von BCM im betroffenen Unternehmen hat. Die geprüften Geschäftsbereiche der SBB und Post erreichen einen entsprechend hohen Reifegrad.

2.2 Prozessorientiertes Vorgehen als Selbstverständlichkeit

Mehr als die Hälfte der geprüften Organisationen verfügt über Zertifizierungen nach internationalen Standards, z.B. für Quality Management (QM) nach ISO 9001 und/oder Information Security Management System (ISMS) nach ISO 27001. Die damit verbundene Prozessorientierung der Mitarbeitenden und die zugrunde liegenden Managementsysteme stellen sicher, dass auch das BCM mit derselben Systematik umgesetzt wird. Die Festlegung von Verantwortung und Kompetenz ist dabei genau so selbstverständlich wie die regelmässige Überprüfung und Verbesserung des Regelwerkes. Der für die Prüfung vom Revisionsteam als Basis verwendete BS25999 war in den meisten Organisationen bekannt, teilweise basieren die Basisdokumente darauf. Durch Zertifizierungen und der damit verbundenen jährlichen Prüfungen durch externe Stellen herrscht bei solchen Organisationen ein ausgeprägtes Selbstverständnis für Audits. Das Revisionsteam ist entsprechend mit einer positiven Erwartungshaltung empfangen worden.

2.3 Unterschiedliche Ansätze bei der Umsetzung

Die Informations-Technologie (IT) ist eine der zentralen, oft sogar die wichtigste aller Ressourcen. In der Regel wird diesem Bereich viel Aufmerksamkeit geschenkt, sowohl bei den präventiven Massnahmen als auch bei der Planung von unvorhersehbaren Ereignissen. Seriöse Systemverantwortliche haben sich lange bevor BCM zu einem Schlagwort geworden ist, mit Notfallmanagement beschäftigt. Daher bestehen bei der IT meistens umfangreiche Wiederherstellungspläne, auch wenn vorgängig nie eine detaillierte BIA oder eine BCS erstellt worden ist. In einigen der geprüften Organisationen wird die IT - nebst den Mitarbeitenden - als einzige kritische Ressource definiert. Läuft diese störungsfrei, so können auch alle Kernprozesse zeitgerecht erfüllt werden. Mit diesem Ansatz ist nachvollziehbar, dass dem formellen BCM weniger Bedeutung zukommt. Auch wenn diese Praxis durchaus den Zweck erfüllen kann, so erreicht ein solches BCM dennoch einen tieferen Reifegrad bei der Beurteilung. Dieses Vorgehen kann auch nur in kleineren, überschaubaren Organisationen eingesetzt werden. In einem Konzern wie den SBB oder der Post würde ein solch pragmatischer Ansatz nicht funktionieren. Es ist in Krisenlagen entscheidend, dass für alle Bereiche dieselben Spielregeln festgelegt und durchgesetzt werden, was in der Praxis auch erfolgt. Bei zwei Organisationen ist das BCM erst in den letzten Monaten aufgebaut worden, so dass die regelmässige Überprüfung und die Bewährung

in der Praxis noch nicht abschliessend beurteilt werden konnte, formell waren die Unterlagen jedoch vollständig.

2.4 Lassen sich die Resultate überhaupt vergleichen?

Obschon die Aufgaben der geprüften Organisationen völlig unterschiedlich sind, kann der Umsetzungsstand des BCM verglichen werden. Das eingesetzte Maturity Model lässt genau die wichtige Differenzierung von rein formellen Darstellungen und praxisorientierten Umsetzungen zu. Teilbereiche des BCM wie z.B. das Notfallmanagement oder die BIA lassen sich bei gleichartigen Aufgaben sehr gut vergleichen.

Bei den SBB und der Post lassen sich das formelle BCM, das BCP bei der IT und das konzernweite Krisenmanagement gegenüber stellen. In diesen Punkten haben die beiden Unternehmen nebst dem IGE einen hohen Reifegrad von über 4 erreicht. Nach Ansicht des Revisionsteams hat dies einen direkten Zusammenhang mit der Marktpositionierung. Es ist nicht nur auf dem Papier sondern auch in der Praxis nachweisbar, dass in diesen Organisationen eine Krise mit allen einsetzbaren Mitteln vermieden wird, damit der Kunde zufrieden bleibt und seine Dienstleistung weiterhin bezieht. Wenn dennoch ein unerwartetes Ereignis eintritt, so muss und wird alles getan, damit möglichst rasch zum Normalzustand zurückgekehrt werden kann.

2.5 Der Vergleich mit der Querschnittsprüfung BCM 2009

Die BCM-Prüfungen bei Verwaltungseinheiten der zentralen Bundesverwaltung im Vorjahr zeigten nicht ganz befriedigende Ergebnisse, wobei damals nur die Bereiche BIA, BCS und BCP inkl. Krisenmanagement geprüft wurden. BCM wurde oft auf die Verfügbarkeit der IT reduziert und nur in wenigen Fällen als Aufgabe des Managements für eigene Krisenlagen verstanden. Mit der vorliegenden Prüfung sollten daher Vergleichswerte in der erweiterten Bundesverwaltung erarbeitet werden und zwar anhand des vollständigen Fragenkataloges, d.h. inkl. Policy und Test/Awareness. Die vorliegenden Resultate zeigen wesentliche Unterschiede.

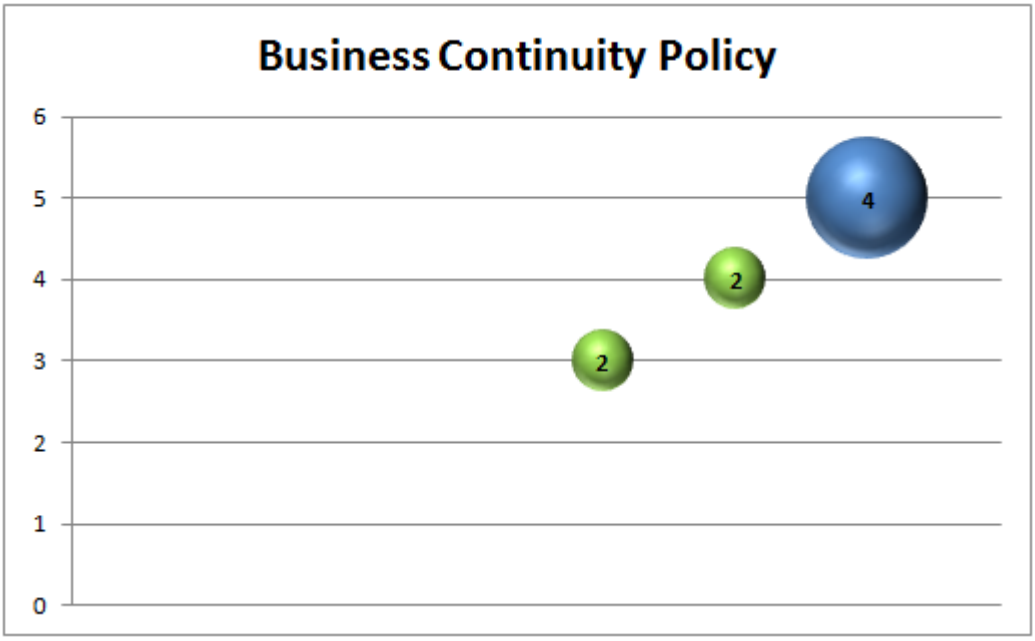
Massgebend für ein vollständiges, formell korrektes und in der Praxis umgesetztes BCM scheint der Markt zu sein. Je mehr Konkurrenz bei der Dienstleistung vorhanden ist, desto höher fällt der Reifegrad des aufgesetzten BCM aus. Im Vorjahr hat eine einzige Verwaltungseinheit einen durchschnittlichen Reifegrad von 3 ausweisen können, alle anderen Einheiten lagen darunter, zur Hälfte sogar unter 2. Dagegen haben alle nun beurteilten Organisationen einen Reifegrad von 3 erfüllt, fünf Organisationen liegen mit ihrem Durchschnitt bei 4 und mehr. Unternehmensstrategien, Vorgaben des obersten Management und ein prozessorientiertes Handeln spielen dabei eine grosse Rolle.

3 Business Continuity Policy

3.1 Die Policy ist die Absichtserklärung des Management

Mit der Erstellung und Publikation einer Business Continuity Policy (Richtlinie) dokumentiert das Management seine Ziele zum BCM und übernimmt damit die oberste Verantwortung für die Umsetzung des BCM-Prozesses. Eine Policy soll den Mitarbeitenden aufzeigen, wie mit dem Thema BCM umgegangen wird, für welche Geschäftsbereiche diese Haltung gilt und wer verantwortlich ist für den Unterhalt des Regelwerkes.

3.2 Das Management bekennt sich noch nicht überall verbindlich zum BCM



Alle geprüften Organisationen konnten Grundsätze zum BCM vorweisen, allerdings nicht überall in Form eines von der obersten Führung freigegebenen und für alle Mitarbeitenden verbindlichen Dokumentes. Dadurch ist in diesen Fällen nicht eindeutig festgelegt, wer für ein kontinuierliches BCM die Verantwortung trägt. Es wurde jedoch überall erkannt, dass BCM umfassender geregelt werden muss. Zum Zeitpunkt der Prüfung befanden sich in einigen Organisationen dahingehende Projekte oder Dokumente in Arbeit, was bei der Beurteilung mitberücksichtigt werden konnte.

Die Hälfte der gesichteten Dokumente entsprach den formellen Anforderungen an eine Policy. Bei diesen Organisationen waren entsprechend auch die nachfolgend beschriebenen Themen zum BCM weitgehend abgedeckt. In den meisten Fällen standen bezüglich Beantwortung von Fragen zur Policy aber auch zur Strategie Geschäftsleitungsmitglieder oder sogar der Geschäftsleiter persönlich zur Verfügung. Das Management zeigt damit nicht nur ein Interesse, sondern übernimmt aktiv die ihr grundsätzlich auferlegte Verantwortung für die Bewältigung von Krisenlagen. Diese Haltung war 2009 in der zentralen Bundesverwaltung nur in wenigen Fällen vorhanden.

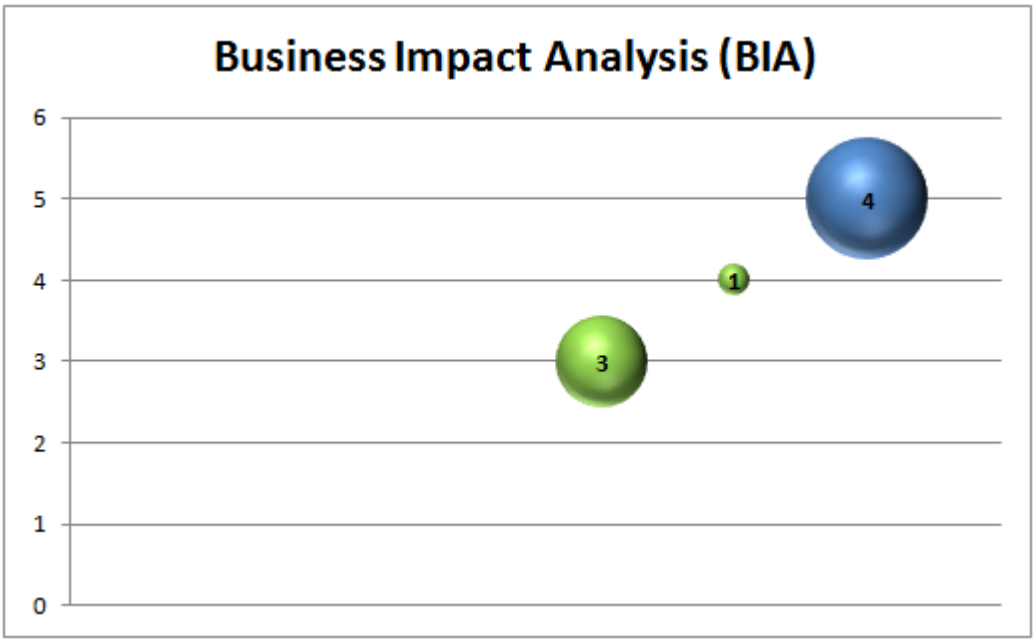
4 Business Impact Analysis (BIA)

4.1 Die BIA zeigt vor allem die Auswirkungen auf Geschäftsprozesse

In einer BIA werden die Auswirkungen bei Ausfall oder Verlust von Ressourcen und damit die Störung oder Unterbrechung von Betriebsabläufen identifiziert und bewertet. Dazu müssen die Geschäftsprozesse definiert und priorisiert werden, d.h. welche Prozesse sind aufgrund bestimmter Anforderungen (zeitliche, juristische, wirtschaftliche) kritisch und welche nicht. Anhand von Risikoszenarien werden die möglichen Auswirkungen auf die Ressourcen beurteilt. Die Einschätzungen sollten beinhalten, welche maximal tolerierbaren Ausfallzeiten für die einzelnen Prozesse gelten, ob Minimallösungen über eine gewisse Zeit möglich sind und welche Mindestressourcen dafür benötigt werden.

Eine BIA stellt die wesentliche Grundlage für die nachfolgenden Entscheide der Geschäftsleitung in der Business Continuity Strategy dar.

4.2 Riskmanagement beinhaltet noch keine Auswirkungsanalyse



Die Überprüfung von strategischen Risiken erfolgt bei den meisten Organisationen seit Jahren systematisch und regelmässig. Zur Priorisierung der Risiken dienen meistens die Kriterien Finanz- und Imageschaden. Solche Schäden können auch bei einer nicht zeitgerechten Erfüllung von Dienstleistungen entstehen. Die definierten Top-Risiken decken jedoch oftmals nur teilweise oder global die Risiken einer unterbrochenen Geschäftstätigkeit ab. Dazu das Beispiel des Top-Risikos „Ausfall der IT“: Ein solcher Ausfall kann verschiedenste Ursachen haben, welche sich auch unterschiedlich auf die Geschäftsprozesse auswirken. Es kann ein gesamtes Rechenzentrum ausfallen, ein regionaler Stromunterbruch kann Netz-Verbindungen unterbrechen, eine einzelne

Datenbank kann nicht mehr integer sein usw. Wie weit in diesen Fällen ein Schaden entstehen kann, muss daher in der weitergehenden BIA beurteilt werden.

Das Revisionsteam hat bei fünf Organisationen differenzierte Musterbeispiele vorgefunden, wie eine BIA in teilweise komplexem Umfeld erfolgreich durchgeführt werden kann. Die SBB und Postfinance sind stark von einer funktionierenden IT abhängig. Um die Abhängigkeiten zwischen den Geschäftsprozessen und den IT-Anwendungen zu erkennen, wurden entsprechende Datenbanken aufgebaut. Aus diesen können Schnittstellen, allenfalls betroffene Produkte und auch tolerierbare Ausfallzeiten entnommen werden. Mit diesen Angaben kann ein mögliches Schadensausmass beurteilt und bei einer Störung im Betrieb sofort festgestellt werden, welche Produkte/Prozesse betroffen sind. Die Systematik und Vollständigkeit dieses Vorgehens und die dazu eingesetzten Werkzeuge haben das Revisionsteam überzeugt.

Bei einigen Organisationen basiert die BIA auf dem strategischen Riskmanagement, bei anderen fliessen dagegen die in der BIA beurteilten Risikoszenarien über Konsolidierungen in das Riskmanagement ein. Diese Verbindung erscheint dem Revisionsteam wichtig, damit alle Geschäftsprozesse abgedeckt werden.

Bei der BIA sind in einigen Fällen Lücken in den beschriebenen Geschäftsprozessen bzw. den notwendigen Ressourcen sowie den Risikoszenarien festgestellt worden. Zudem sollten die zeitlichen Aspekte vermehrt in die Analysen einbezogen werden.

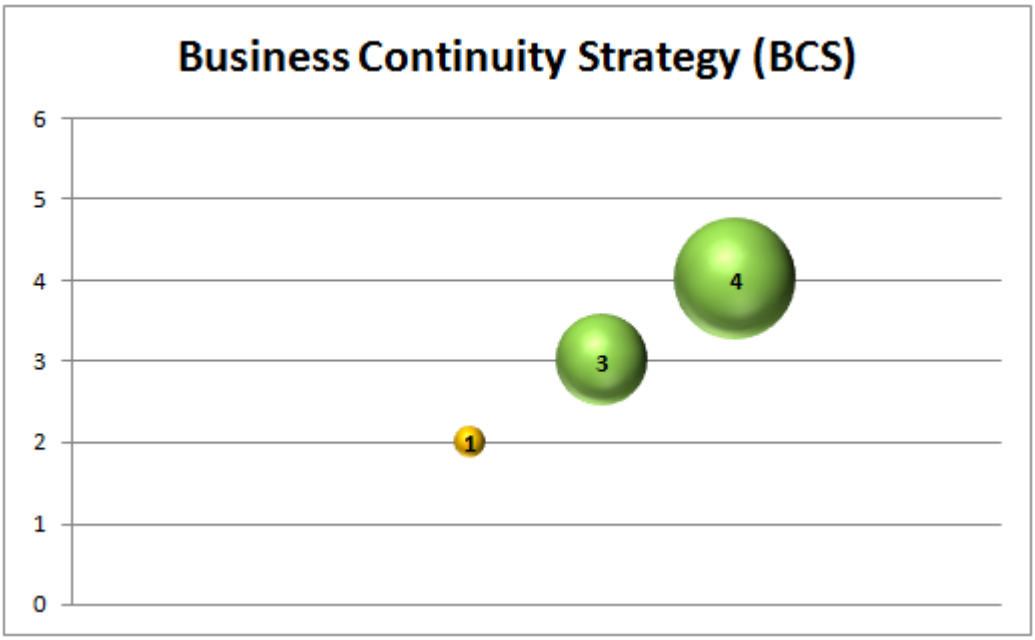
5 Business Continuity Strategy (BCS)

5.1 Die BCS zeigt auf, wie mit Störfällen umgegangen wird

In der BCS soll dargelegt werden, welche Massnahmen umgesetzt werden, um erkannten Schwachstellen/Risiken vorzubeugen bzw. solche zu überwachen. Allfällige Restrisiken sind dabei auszuweisen. Weitergehend sind alternative Betriebsabläufe zur Wiederherstellung einer minimalen bzw. reduzierten Geschäftstätigkeit bis zur Wiedererlangung der normalen Geschäftsprozesse aufzuzeigen. Geschäftsprozesse, welche in einer ersten Phase als nicht kritisch gelten, müssen überwacht werden und die zeitlich kritische Grenze muss auch für diese Prozesse festgelegt sein.

Eine formell korrekte BCS kann grundsätzlich nur dann erstellt werden, wenn vorgängig eine BIA durchgeführt wurde.

5.2 Der Umfang einer BCS wird durch den Zeitfaktor beeinflusst



Aussagen zur BCS waren überall vorhanden. Bei den SBB und PostAuto sind die Strategien sogar gesetzlich verankert, vereinfacht dargelegt müssen Bahnen und Postautos pünktlich auf den vorgesehenen Strecken fahren. Das Revisionsteam sah Verbesserungsmöglichkeiten hauptsächlich bei der formellen Darstellung oder der Vollständigkeit.

Die Organe der dezentralen Bundesverwaltung haben mehrheitlich Geschäftsprozesse, die über längere Zeit ausfallen können, ohne dass dabei der Kunde unmittelbar betroffen ist. In der Regel sind auch die damit verbundenen Ressourcen nicht kritisch. Das BCS reduziert sich bei diesen Organisationen auf ein paar Kernaussagen zu allfälligen alternativen bzw. reduzierten Betriebsabläufen und der Wiederherstellung des Normalzustandes. Präventive, kostspielige

Massnahmen stehen meistens in keinem Verhältnis zu den Kosten im Schadensfall. Allerdings darf nicht vergessen werden, dass vorerst unkritische Geschäftsprozesse auf der Zeitachse irgendwann auch kritisch werden können. Das IGE, welches auch keine kritischen Geschäftsprozesse ausweist, hat dennoch im Frühjahr 2010 ein vollständiges BCM nach BS25999 aufgebaut, welches sehr gut bewertet werden konnte.

Bei den SBB und den geprüften Bereichen der Post sind gegenüber der dezentralen Bundesverwaltung viele Geschäftsprozesse und Ressourcen zeitkritisch. Entsprechend werden alle möglichen präventiven Massnahmen umgesetzt, damit eine Krisenlage erst gar nicht entstehen kann. Wenn dennoch ein unvorhergesehenes Ereignis eintritt, so ist es von entscheidender Wichtigkeit, dass Prioritäten, Alternativen und reduziert mögliche Tätigkeiten im Voraus festgelegt und die Restrisiken bekannt sind. Allenfalls notwendige Ressourcen müssen im Detail definiert und deren termingerechte Wiederbeschaffung geregelt sein. Die genannten Organisationen haben mit ihren strategischen Regelungen überzeugt.

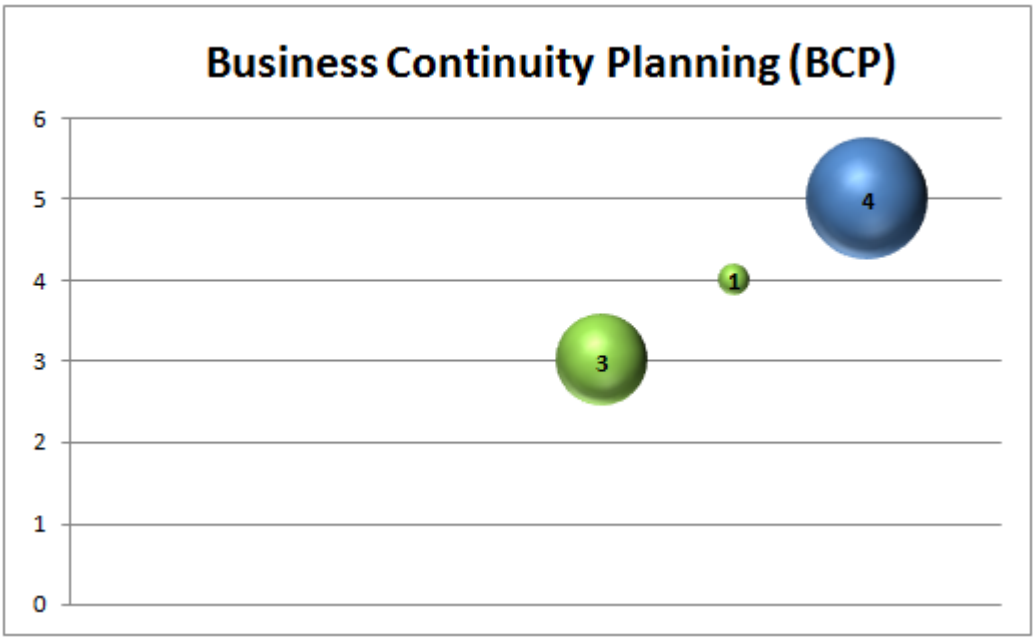
6 Business Continuity Planning (BCP)

6.1 Das BCP legt fest, wie im Krisen-/Katastrophenfall vorgegangen wird

Pläne zur Wiederherstellung bzw. Fortsetzung der kritischen Geschäftsprozesse beinhalten die mögliche Ersatzlösungen (z.B. manuelle Arbeiten, Ausweichstandorte) und mindestens benötigte Ersatzressourcen (z.B. Notebooks, Arbeitsplätze). Ebenso muss die Alarmorganisation definiert und organisiert sein. Wenn Probleme nicht innerhalb eines definierten Zeitrahmens durch die operativen Bereiche gelöst werden können, muss ein spezieller Krisenstab einberufen werden, der sich unabhängig vom Tagesgeschäft um die Rückführung in den Normalzustand und eine einheitliche Kommunikation kümmert.

Der Detaillierungsgrad des BCP hängt davon ab, wie zeitkritisch die Geschäftsprozesse und die dazu verwendeten Ressourcen sind.

6.2 Die Vorbereitungen zur Bewältigung eines Krisenfalls haben mehrheitlich überzeugt



Insgesamt haben fünf Organisationen mit umfangreichen Vorgehensplänen und Checklisten zu differenzierten Risikoszenarien überzeugt. Lieferantenverzeichnisse waren vorhanden und die Alarmorganisation sowie Kommunikationswege waren schriftlich festgelegt. Teilweise wurde empfohlen, dass verschiedene Dokumente zu einem Regelwerk vereint oder einheitliche Vorgaben erstellt werden sollten. Generell sind die immer mehr aufkommenden mobilen Arbeitsmittel mit Anschlussmöglichkeiten von irgendeinem Standort eine wirkungsvolle Alternative, damit Schlüsselpersonen ihre Arbeiten jederzeit erfüllen können. Von dieser Möglichkeit profitieren auch die SBB und Post, was viel zur raschen Einsatzfähigkeit in Krisenlagen vor allem im Bereich IT beiträgt.

Verschiedene Organisationen haben eine institutionalisierte Meldepflicht über sicherheitsrelevante Vorfälle. Diese werden zentral gesammelt, ausgewertet und auf mögliche Zusammenhänge untersucht. Anhand dieser Daten lassen sich einerseits entstehende Krisensituationen frühzeitig erkennen, andererseits lassen sich daraus Rückschlüsse auf allenfalls nicht erkannte oder neue Risiken ziehen. Solche Erkenntnisse fliessen nachfolgend in die BIA ein und führen schlussendlich zu einer Anpassung beim BCP.

Beim BCP gelten für die Organisationen der dezentralen Bundesverwaltung grundsätzlich dieselben Aussagen wie im Kapitel 6.2. Wenn die Zeit nicht drängt, so können Ausweicharbeitsplätze und andere Ressourcen auch kurz- bis mittelfristig beschafft werden. Dem Revisionsteam scheint es dennoch wichtig, dass man sich über Risikoszenarien Gedanken macht, die zu einem längeren Unterbruch der Geschäftstätigkeiten führen könnten und welche Möglichkeiten in einem solchen Fall vorhanden wären.

Alle Organisationen haben das Krisenmanagement definiert. Das Revisionsteam hat davon mehrheitlich einen sehr guten Eindruck erhalten.

Beim ENSI und bei der FINMA kommt der Krisenstab hauptsächlich zum Einsatz, wenn von den unter Aufsicht stehenden Kunden eine Krisenlage verursacht wird (z.B. Panne in einem Atomkraftwerk oder Finanzkrise).

Bei den SBB und der Post gehört die Bewältigung von kleineren Ereignissen zum Tagesgeschäft. Für eskalierende Ereignisse verfügen beide Unternehmen auf Stufe Konzern über einen Krisenstab, sowie weitere in den einzelnen Geschäftsbereichen. Dabei ist genau geregelt, ab wann welche Krisenstäbe zum Einsatz kommen und welche Verantwortlichkeiten bzw. Kompetenzen diesen übertragen sind. Die notwendigen Alarmorganisationen sind umfassend geregelt.

Der Krisenstab des Konzerns SBB und derjenige beim ENSI sind generalstabsmässig organisiert, d.h. die Krisenräume sind bis ins letzte Detail vorbereitet, die Funktionsträger mit mehrfacher Stellvertretung ernannt und die Aufgaben inkl. Finanzkompetenz geregelt. Regelmässige Übungen finden statt, damit die Mitglieder dieser Stäbe über die notwendige Fitness im Umgang mit Krisenlagen verfügen.

Bei weiteren Organisationen sind ebenfalls Krisenräume definiert, in denen das notwendige Material gelagert wird. Im Tagesgeschäft werden diese Räume jedoch auch anderweitig genutzt. Bei einigen Organisationen bestehen mehrere Standorte, auf die jederzeit ausgewichen werden kann, womit sich weitergehende Planungen erübrigen.

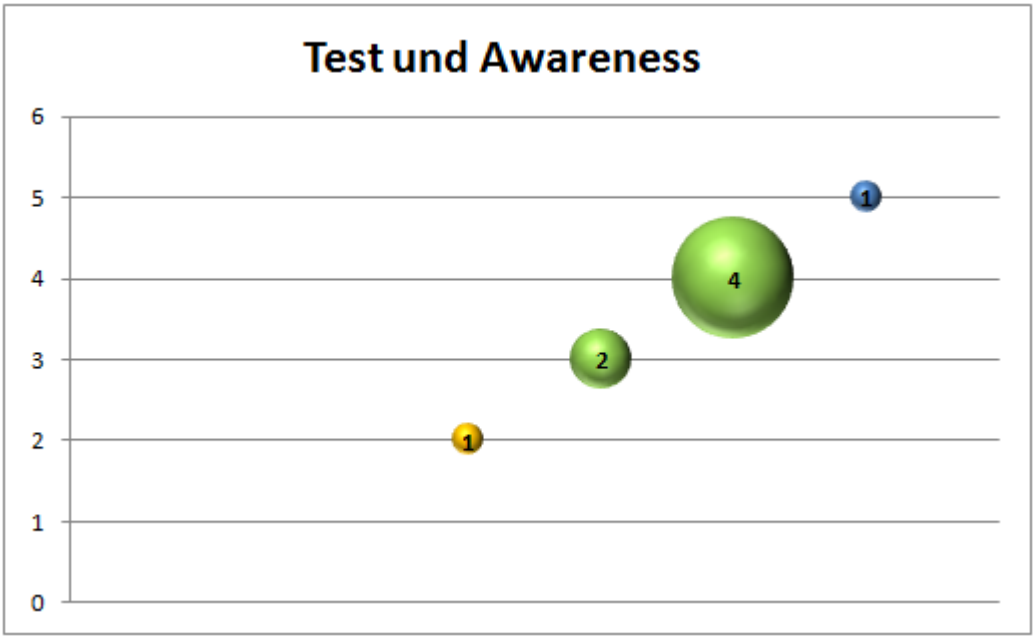
7 Test und Awareness

7.1 Anforderung

Eine BCM-Fähigkeit kann nur als verlässlich gelten, wenn sie geübt, gepflegt und überwacht wird. Übungen sollten aufgrund eines strukturierten Programmes erfolgen, welches mit einfachen Szenarien beginnt und in umfassenden Notfallübungen endet. Die stufengerechte Schulung aller am BCM beteiligten Mitarbeitenden gehört als kontinuierliche Aufgabe zu einer BCM-Kultur.

Nur wer regelmässig übt, was im BCP festgelegt ist, wird im Ernstfall die notwendige Fitness aufweisen, um eine Krise zeitgerecht zu überwinden.

7.2 Der Nutzen von Test und Awareness ist noch nicht überall erkannt worden



Übungen können auf unterschiedlichste Art und in allen Geschäftsbereichen durchgeführt werden (z.B. Dokumentenreviews, Gebäudeevakuierungen, Unterbrechung der Stromzufuhr, Risikoszenarien im Krisenstab durchgehen, usw.). Echttests finden auch immer wieder im Tagesbetrieb bei der Behebung von Störungen statt.

Die Mehrheit der Organisationen führt regelmässige Tests in verschiedenen Bereichen durch. Diese basieren teilweise auf Einzeldokumenten oder werden aufgrund einer Jahres- oder Mehrjahresplanung vorgenommen. Die SBB, Postfinance und Swiss Post Solutions gehen dabei systematisch und konsequent vor. Bei den anderen Organisationen fehlen entweder Testkonzepte/-planungen oder die Systematik.

Bei einem in der Praxis umgesetzten BCM sind die Mitarbeitenden soweit sensibilisiert bzw. ausgebildet, dass Unregelmässigkeiten automatisch und selbstverständlich gemeldet werden. Bei der Awareness gab es unterschiedliche Resultate, wobei in Produktionsbereichen (SBB, Post und auch generell IT) eine grössere Sensibilität herrscht. Die Awareness kann noch wesentlich verbessert werden.

8 Schlussbesprechung

Die Schlussbesprechung fand am 24. November 2010 mit Vertreterinnen und Vertretern von allen geprüften Organisationen bzw. Unternehmen statt. Da Empfehlungen in den einzelnen Teilberichten abgegeben worden sind, wird der Gesamtbericht nur noch zur Kenntnisnahme an die Geschäftsleitungen der geprüften Organisationen bzw. Unternehmen versandt. Die Schlussbesprechung wurde durchgeführt, damit sich alle Beteiligten zum Inhalt oder einzelnen Aussagen äussern konnten. Die Anwesenden haben den Bericht ohne Ergänzungen oder Korrekturen akzeptiert.

Allen Mitarbeiterinnen und Mitarbeitern sei für die gewährte Unterstützung und die angenehme Zusammenarbeit bestens gedankt. Dieser Dank geht insbesondere auch an die Mitarbeitenden der Internen Revision von SBB und Post, sowie die involvierten Drittfirmen im IT-Bereich der SBB.

Die Finanzdelegation der eidgenössischen Räte hat an der ordentlichen Sitzung im Februar 2011 vom Bericht Kenntnis genommen.

Anhang 1 : Erläuterungen zum Maturity Model

Die EFK hat sich bei der Beurteilung des Prozessreifegrades am nachfolgenden Maturity Model orientiert. Damit sollte erreicht werden, dass bei der Beurteilung der einzelnen Themen für alle geprüften Organisationen bzw. Geschäftsbereiche derselbe transparente Massstab angewendet wurde. Die Prozessreife liess sich dabei nicht immer auf einzelne Detailfragen herunter brechen; viel mehr musste sie im Gesamtzusammenhang betrachtet werden.

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

BCM	Business Continuity Management
BCP	Business Continuity Planning
BCS	Business Continuity Strategy
BIA	Business Impact Analysis
BS	British Standard, z.B. BS25999
COBIT	Control Objectives for Information and Related Technology (Herausgeber IT Governance Institute)
ENSI	Eidg. Nuklearsicherheitsinspektorat
FINMA	Eidg. Finanzmarktaufsicht
IGE	Institut für Geistiges Eigentum
ISMS	Information Security Management System (Standard ISO 27001)
ISO	International Organisation for Standardization
IT	Informations-Technologie
MM	Maturity Model
QM	Quality Management (Standard ISO 9001)
SBB	Schweizerische Bundesbahnen
SPS	Swiss Post Solutions (Geschäftsbereich des Konzerns Post)
Swissmedic	Schweizerisches Heilmittelinstitut
VE	Verwaltungseinheiten