Christian Thiel, Christoph Thiel

Business Continuity Management für KMU

Bei kleinen und mittelständischen Unternehmen (KMU) besteht erheblicher Nachholbedarf beim Business Continuity Management (BCM). Die existierenden Standards und Prüfvorschriften werden häufig als zu komplex und ihre Umsetzung als zu aufwändig und teuer empfunden. Der Beitrag stellt einen Leitfaden für KMU zur Implementierung eines BCM vor, der auf den Ergebnissen einer von der FHS St. Gallen durchgeführten Studie zur Erfassung von Good Practices basiert.

Einführung

Die Sicherheit von kleinen und mittelständischen Unternehmen (KMU) ist von entscheidender Bedeutung für die europäische Wirtschaft. Sie repräsentieren schließlich 99% aller Unternehmen in der EU mit ca. 65 Mio. Arbeitsplätzen. Daher ist es umso erschreckender, dass der Einsatz eines Business Continuity Managements in KMU keinesfalls üblich ist. Der Studie „Netz- und Informationssicherheit in Unternehmen 2009“ des Netzwerks Elektronischer Geschäftsverkehr zufolge werden lediglich in jedem fünften KMU IT-Notfallpläne erstellt [1]. In jedem vierten KMU fehlt eine standardisierte Vorgehensweise, um IT-Notfälle möglichst zügig abzuwenden. Das unabhängige Marktforschungsunternehmen Forrester Research stellt in seiner Studie „The State Of SMB IT Security: 2008 To 2009“ fest, dass 45 Prozent der US-amerikanischen und europäischen KMU kein BCM-Konzept ausweisen können.

Als wesentlicher Grund für den hohen Nachholbedarf der KMU im Bereich BCM wird von vielen Experten angeführt, dass die entsprechenden Standards zu komplex und ihre Implementierung für KMU nicht leistbar sei. Gestützt wird diese Annahme durch die Ergebnisse der Pilot-Studie „Assessing a simplified Information Security approach 2009“ der European Network and Information Security Agency (ENISA), die sehr wohl ein großes Bedürfnis der KMU nach vereinfachten Ansätzen des Sicherheits- und Risikomanagements nahelegen [2]. Diese Anforderung kann insbesondere auch für ein unternehmensspezifisches BCM unterstellt werden.

In diesem Beitrag wird ein Leitfaden für KMU zur Implementierung eines unternehmensspezifischen BCM vorgestellt. Im Sinne des von ENISA empfohlenen vereinfachten Ansatzes für KMU stellt er eine „one-size-fits-all“ Lösung, gerade für IT-Laien und kleine Organisationen mit relativ einfach zu verwaltenden Komponenten dar. Er basiert auf den Ergebnissen der Studie „Geplante Katastrophenabwehr, Krisen und Notfallmanagement bei KMU“, die im Auftrag eines der Autoren dieses Beitrags als wissenschaftliches Praxisprojekt von der FHS St. Gallen, Hochschule für Angewandte Wissenschaften, von Oktober bis Dezember 2009 in der deutschsprachigen Schweiz durchgeführt wurde [3]. Untersuchungsgegenstand dieser Studie ist Stand und Vorgehensweise von KMU bei der Umsetzung eines wirksamen unternehmensweiten BCM.

Dr. Christian Thiel

Dozent für Wirtschaftsinformatik, Institut für Informations- und Prozessmanagement
FHS St. Gallen, Hochschule für Angewandte Wissenschaften.
E-Mail: christian.thiel@fhsg.ch

Prof. Dr. Christoph Thiel

FH Düsseldorf – University of Applied Science
E-Mail:
christoph.thiel@fh-duesseldorf.de

1 Business Continuity Management

In einer global vernetzten Welt sind Unternehmen vom reibungslosen Funktionieren ihrer Infrastrukturen abhängig. Prozessstörungen oder gar ein Stillstand kritischer Prozesse stellen ein existenzbedrohendes Risiko dar. Krisenmanagement und Business Continuity Management gewinnen deshalb immer größere Bedeutung [4].

Der Begriff Business Continuity Management kann dabei definiert werden als „die Gesamtheit der Prozesse, Verfahrensweisen, Entscheidungen und Aktivitäten, welche sicherstellen, dass eine Unternehmung während eines längeren betrieblichen Unterbruchs trotzdem weiter funktionieren kann. Anders ausgedrückt: es müssen proaktive und reaktive Vorkehrungen getroffen werden, um zum einen Krisen oder Katastrophen möglichst zu vermeiden, und zum anderen, sollten diese dennoch auftreten, die schnellst mögliche Rückkehr zu business as usual zu gewährleisten.“ [5]. Danach ist BCM ein Querschnittsthema, das Schnittstellen zu zahlreichen anderen betrieblichen Steuerungsprozessen besitzt und deren Mitarbeit benötigt. Dazu gehören z. B. das Krisenmanagement, das Risikomanagement, die Informationssicherheit, das Qualitätsmanagement, das Sourcing-Management und das Compliance Management.

Insbesondere als Bestandteil des Risikomanagements unterliegt BCM einschlägigen rechtlichen Vorgaben, die sich nach Branche und Unternehmensgröße unterscheiden, sowie zusätzlich speziellen Standards. Hierzu zählen z. B. die Good Practice Guidelines des Business Continuity Institute [6]. Zentrale Kompetenzen für Praktiker sind in den (GB, USA) „Joint Stan-

dards" geregelt, die gemeinsam durch das Business Continuity Institute und das Disaster Recovery Institute herausgegeben werden. Die ISO/PAS 22399 beschreibt einen ganzheitlichen Managementprozess, der Bedrohungen und Schäden einer Organisation identifiziert und ein Rahmenwerk zur Minimierung der Auswirkungen bietet [7]. Sie basiert auf Best Practices aus fünf Nationen und enthält u. a. Teile des amerikanischen Standards NFPA 1600:2400 [8], des britischer Standards BS 25999-1:2006 [9], des australischen Standards HB 221:2004 [10], des israelischen Standards INS 24001:2007 [11], des japanischen Business Continuity Plan Drafting Guideline, Ministry of Economy, Trade and Industry of Japan 2005 und des Business Continuity Guideline, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005. Das deutsche Bundesamt für Sicherheit in der Informationstechnik hat den Standard BSI 100-4 „Notfallmanagement" als Ergänzung zum IT-Grundschutz bereitgestellt [12].

Neben allgemein gültigen Gesetzen wie dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) [13], dem Schweizerischen Obligationenrecht (vgl. Art. 663b OR, [14]), dem britischen Civil Contingencies Act [15] oder dem amerikanischen Sarbanes-Oxley-Act (SOX) [16] sind ggf. Anforderungen der Grundsätze ordnungsmäßiger Buchführung (GoBS) bei Einsatz von Informationstechnologie, Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce, Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren [17, 18, 19], die Veröffentlichungen des Basler Ausschusses hinsichtlich der Zweiten Basler Eigenkapitalverordnung (Basel II) und die Mindestanforderungen an das Risikomanagement (MaRisk) [20] relevant.

Selbst in Kenntnis der gesetzlichen Anforderungen stellt die Auswahl und noch mehr die Umsetzung eines der gebräuchlichen Standards für viele KMUs eine erhebliche Hürde dar. Dies liegt nicht nur an der Komplexität dieser Standards, die an der Lebenswirklichkeit der KMU häufig vorbeizielen, sondern auch an der (insbesondere sprachlich) ungeeigneten und nur für Experten verständlichen Darstellung auch einfacher Sachverhalte und Zusammenhänge.

Eine speziell für KMU geeignete Anleitung für die Einführung und den Betrieb eines BCM sollte daher im Umkehrschluss die tatsächlichen Rahmenbedingungen der KMU – wie z. B. geringe Personalressourcen, kein Expertenwissen im Risikomanagement etc. – berücksichtigen und Hilfestellung auch in einer für IT-Laien verständlichen Form bieten. Um diese Anforderungen zu realisieren wurde in einer Studie der FHS St. Gallen untersucht, wie sich KMU in der deutschsprachigen Schweiz auf unternehmensbedrohende Störungen in den Bereichen Infrastruktur/Logistik, Personal, externe Dienstleister und Technik vorbereiten. Es wurden Referenzunternehmen unter den befragten KMU identifiziert, denen es trotz der genannten Widrigkeiten gelingt, sich mit vertretbarem Aufwand vor den Auswirkungen solcher unternehmensbedrohenden Störungen zu schützen oder diese zumindest zu reduzieren. Die Analyse der Good Practices dieser Referenz-Unternehmen liefert einfach anwendbare Regeln, die KMU als Gestaltungsempfehlung für ein wirksames individuell zugeschnittenes BCM dienen können.

2 Studie

Die Studie setzt auf die Kombination zweier zunächst unabhängiger Erhebungsmethoden. In persönlichen Expertenbefragungen (zehn Berater, Revisoren, Versicherungen etc.) in Form eines Leitfadeninterviews wurden Informationen zu klar definierten Fragestellungen ermittelt. Das Interviewkonzept wirkt dabei in Hinblick auf den Ausschluss unergiebiger Themen als Steuerung, die den Befragten auf das interessierende Expertentum begrenzt (vgl. [21], S. 37).

Parallel wurden 59 KMU mit Hilfe eines standardisierten Fragebogens befragt, um kausale Zusammenhänge im Sinne von vergleichsweise stabilen, problemlos verallgemeinerbaren Relationen zwischen verschiedenen Variablen zu entdecken und zu quantifizieren. Die Kombination der genannten Erhebungsmethoden ermöglicht somit qualitative und quantitative Erhebungs- und Auswertungsschritte mit jeweils eigenen Datensätzen. Die daraus resultierenden Ergebnisse können nun wechselseitig aufeinander bezogen werden (vgl. [22], S. 300).

Im Fokus steht dabei die Frage, wie gut KMU auf unternehmensbedrohende Störungen bzw. Vorfälle vorbereitet sind. Es soll herausgefunden werden, welche BCM-Elemente in KMU zum Einsatz kommen und wie effektiv diese umgesetzt werden, damit hieraus allgemeine Empfehlungen abgeleitet werden können. Hierfür wird der Begriff des unternehmensweiten BCM bereits in der dimensionalen Analyse in die relevanten Dimensionen eingeteilt. Von Interesse sind dabei einerseits präventive Maßnahmen, die das Eintreten einer kritischen Störung vermeiden oder zumindest vermindern sollen, andererseits Maßnahmen zur Bewältigung einer eingetretenen Störung mit dem Ziel, die wichtigsten Geschäftsprozesse sowie anschließend den ganzen Betrieb so schnell wie möglich wiederherzustellen.

Prävention und auch Bewältigung sind latente Variablen unseres Messmodells, die sich jeweils in vier weitere betriebsrelevante Dimensionen unterteilen lassen: Infrastruktur/Logistik, Personal, Technik sowie externe Dienstleister. Diese Dimensionen spiegeln sich in den tieferen Gliederungsebenen des Interviewleitfadens und des Fragebogens wider.

In die Interviews und den Fragebogen eingeflochtene Kontrollfragen sichern die Konsistenz der Aussagen eines Umfrageteilnehmers (Experte oder KMU) ab. Aus Antworten auf Kontrollfragen kann im Fall eines erkennbaren Widerspruchs in der Beantwortung der Kernfragen geschlossen werden, ob sich dieser auf Unkenntnis des Themas oder auf falsch verstandene Fragen zurückführen lässt.

Für diesen Beitrag sind keine statistischen Rückschlüsse auf den Durchschnitt aller Schweizer KMU notwendig. Schließlich ist keine Momentaufnahme gesucht, sondern ein Benchmark, um von den Referenz-Unternehmen zu lernen. Daher wurde eine Indexierung der befragten KMU durchgeführt und die im Vergleich mit der Gesamtumfrage zehn bestplatzierten KMU als Referenz für eine Benchmarkanalyse gewählt. Bei diesen ist zudem ein klar positiver Zusammenhang zwischen eingesetzten Mitteln für BCM und dessen Wirksamkeit nachweisbar.

3 Aufbau des Leitfadens

Aus der Benchmarkanalyse der Referenz-Unternehmen leitet sich mit Hilfe von Methoden der quantitativen und qualitativen Sozialforschung der von den Autoren vorgeschlagene Leitfaden für Business Continuity Management für KMU ab. Mit diesem Leitfaden soll KMU geholfen werden, ein eventuell bereits bestehendes BCM im Unternehmen zu verbessern oder ein neu-

es BCM-Konzept zu erstellen. Dabei wurde versucht, ein schlankes Dokument zu liefern, das – wie die befragten Experten empfehlen – vor allem eine aktive Auseinandersetzung mit der Unternehmung (Prioritäten setzen) und mit dem Durchspielen von Notfallszenarien anregt. Im Folgenden skizzieren wir die Inhalte der einzelnen Kapitel des Leitfadens und beschreiben ihre jeweilige Herleitung:

Das Kapitel *Einleitung und Definition BCM* weist zunächst eindringlich darauf hin, dass der Leitfaden ein individuelles Konzept nicht ersetzen kann. Zudem wird dargelegt, dass ausreichend personelle und zeitliche Ressourcen sowie ein angemessenes Budget eingeplant werden müssen (vgl. [23], S. 113). Die Definition von BCM folgt den Definitionen des Business Continuity Institute [6] und den Formulierungen von [5].

Das Kapitel *Vorgehensweise zur Umsetzung eines BCM-Konzepts* orientiert sich am Management-Zyklus für BCM (vgl. [24, 9, 25]), und umfasst den Abschnitt *Empfohlene Grundsätze* sowie die den Phasen des Management-Zyklus entsprechenden Abschnitte *Vorbereitung, Maßnahmenplanung für Prävention bzw. Bewältigung*, *Eintritt eines Ereignisses* und *Nachbereitung* (vgl. Abb. 1). Die Inhalte dieser Abschnitte wiederum leiten sich aus den in der Benchmarkanalyse gewonnenen Erkenntnissen ab. Abb. 1 zeigt, dass BCM vor und nach einem Ereignis angewendet wird. So stellt die Nachbereitung bereits einen Teil der Vorbereitung dar. Die zentralen Punkte *Dokumentation/Einführung, Test/Schulung und Verbesserung/Aktualisierung* im BCM-Zyklus sind in allen vier Phasen gleichermaßen anzuwenden.

Der Abschnitt bzw. die Phase *Vorbereitung* lässt sich weiter unterteilen in die Punkte *SWOT-Analyse*, *Risikoanalyse* sowie *Business Impact Analyse* (BIA) und weitere Elementen in der Vorbereitungsphase. Zunächst gilt es eine Bestandsaufnahme in Form einer SWOT-Analyse vorzunehmen, wobei speziell die betroffenen Akteure identifiziert werden sollten. Weiterhin bietet die SWOT-Analyse die Basis zur Identifizierung kritischer Geschäftsprozesse. In einem zweiten Schritt ist eine sorgfältige Risikoanalyse durchzuführen, wie die Auswertung der Referenzunternehmen in der Benchmarkanalyse gezeigt hat.

Hierfür sind Beispiele von möglichen Risiken aufgelistet, die aus verschiedenen Quellen stammen [23, 26]. Die identifizierten Risiken gilt es in einer BIA auf ihre Auswirkungen hinsichtlich der kritischen Geschäftsprozesse zu untersuchen, was besonders von den Experten empfohlen und von den Referenzunternehmen mehrheitlich umgesetzt wird. Die daraus resultierenden Krisenherde werden klassifiziert und somit priorisiert (High-Risk-Szenario).

Anschließend wird die anzuwendende Strategie je Szenario bestimmt. Die maximale Ausfallzeit und Wiederherstellungsdauer sowie die notwendigen Ressourcen für einen Wiederanlauf sind die abschließenden Schritte der BIA. Die Bestimmung der Strategie führt zur Ausarbeitung von Maßnahmenkatalogen bzw. von Krisenplänen zur Reduktion von Ausfallrisiken. Für die Ausarbeitung verantwortlich ist zudem ein Krisenstab, den es auch in der Vorbereitungsphase zu definieren gilt. Alle Tätigkeiten inklusive Ergebnisse müssen Teil eines Krisenhandbuchs sein. Die Erläuterungen zur Erstellung eines Krisenhandbuchs stützen sich dabei auf die Schilderungen von Ditges, Höbel & Hofmann (vgl. [23], S. 107-113).

Die Klassifizierung der erkannten Ausfallszenarien ist der Ursprung für die Bestimmung der Schadensbekämpfungsstrategie. Der Abschnitt *Maßnahmenplanung für Prävention bzw. Bewältigung* unterscheidet dabei zwischen proaktiven sowie reaktiven Maßnahmen. Proaktive Maßnahmen dienen der Prävention von Unterbrüchen organisatorischer Abläufe, indem die Eintrittswahrscheinlichkeit des betroffenen Szenarios durch ursachenbezogene Maßnahmen reduziert wird. Reaktive Maßnahmen dienen der Behebung von kritischen Unterbrüchen in der Abwicklung von Geschäftsfällen, indem das Schadensausmaß durch auswirkungsbezogene Maßnahmen begrenzt wird (vgl. [27], S. 205).

Für jedes priorisierte Szenario können eigene Maßnahmenkataloge bzw. Krisenpläne erstellt werden, die Teil des gesamtunternehmerischen Krisenhandbuchs sind. Diese in den entsprechenden Plänen skizzierten Notfallmaßnahmen gilt es zu schulen, zu trainieren, zu testen sowie regelmäßig zu aktualisieren, wie insbesondere unsere Benchmarkanalyse bestätigt.

Das Kapitel *Eintritt eines Ereignisses* beschreibt den sinnvollen im Vorfeld geplanten Umgang mit existenzbedrohenden Schadensereignissen. Bei deren Eintritt muss der im Vorfeld definierte Krisenstab einberufen werden, dessen Anordnungen Priorität vor der Belangen der Normalorganisation haben. Für die Bewältigung der identifizierten Ausfallszenarien helfen die praktischen Handlungsanweisungen, die im Notfallplan bzw. Krisenplan festgehalten sind. Auf diese Weise lässt sich das Ausmaß eines Betriebsunterbruchs vermindern. Sollte der Normalzustand vor der Krise nicht mehr erreicht werden, gilt es, einen neuen Normalzustand zu bestimmen. Damit wird signalisiert, dass die Organisation trotz Veränderungen und Restrukturierungen auf dem Weg zurück zu einer produktiven Tätigkeit ist.

An diesem Punkt sollte schließlich auch das Ende einer Krise kommuniziert werden, um das Vertrauen der Mitarbeiter und der Kundschaft zum Unternehmen wieder herzustellen [25]. Alle Tätigkeiten zur Bewältigung einer Krise sollten in einem Krisenlog dokumentiert sein. Dies dient der rechtlichen Absicherung sowie der Aufarbeitung in der Nachbereitung (vgl. [23], S. 111).

Das Kapitel *Nachbereitung* erklärt, dass und wie die Erkenntnisse und Erfahrungen aus überstandenen Krisen der Verbesserung des Krisenplans dienen können. Schwachstellen im BCM-Konzept sollen aufgedeckt und optimiert sowie Strukturen und Prozesse für den Krisenfall festgelegt werden. Dabei wird darauf hingewiesen, dass die Optimierung bzw. Aktualisierung des BCM-Konzepts als kontinuierlicher Prozess zu verstehen ist und somit regelmäßig und nicht nur nach einer Krise durchgeführt wird. Der Kreis schließt sich dadurch, dass die Analyseergebnisse eines Schadensfalls als Basis für die erneute *Vorbereitung* genützt werden. Der Zyklus des BCM beginnt von Neuem.

4 Quickcheck

Im abschließenden Kapitel *Quickcheck* des Leitfadens werden alle wichtigen Schritte auf einer Seite zusammengefasst:

- Krisenstab definieren
- Krisenorganisation mit klaren Zuständigkeits-/Verantwortungszuweisungen
- Krisensprecher bestimmen
- Kontaktinformationen bzw. Kontaktliste
- kritische Bestandsaufnahme des Unternehmens mit SWOT-Analyse
- Risikoanalyse zur Identifizierung von Krisenherden
- BIA zur Bestimmung der Auswirkungen hinsichtlich der kritischen Geschäftsprozesse
- Identifikation wie lange das Unternehmen im Falle eines Ausfalles überleben kann
- Risiken klassifizieren

- Bestimmung der Strategie nach Geschäftsbereichen
  - Risiken akzeptieren – keine Veränderung vornehmen
  - Risiken akzeptieren, jedoch mit einer anderen Firma oder einem Business Continuity Partner eine gegenseitige Vereinbarung treffen, um die Hilfeleistung nach einem Vorfall sicherzustellen
  - Risiken möglichst reduzieren und Vorkehrungen zur Hilfeleistung nach einem Vorfall treffen
  - Risiken soweit reduzieren, bis keine externe Hilfestellung mehr erforderlich ist
  - Risiko vermeiden
  - Risiko auslagern bzw. versichern (Risiko transferieren)
- Präventionsmaßnahmen festlegen
  - Infrastruktur/Logistik (vor allem Brandschutz etc.)
  - Personal (4-Augenprizip etc.)
  - Externe Dienstleister (Zweitlieferanten)
  - Technik (Datensicherung, Datenspiegelung etc.)
- Bewältigungsmaßnahmen für High-Risk-Szenarien festlegen
  - Evakuierungspläne
  - Zweitstandortpläne
  - Zweitlieferantenpläne
  - IT-Disaster-Recovery-Pläne, etc
- Richtlinien und Checklisten aufgrund erstellter Krisenpläne
- Massnahmen schulen
- Pläne testen
- Pläne verbessern
- Pläne regelmässig aktualisieren (Empfohlen: 1x jährlich)

5 Zusammenfassung

Der Anstoß zur Entwicklung von Standards findet sich vielfach im internen Vorgehen von Unternehmungen, welches sich in der Praxis bewährt hat. In Diskussionen mit unterschiedlichsten Interessengruppen entstehen aus solchen Good Practices öffentlich zugängliche Empfehlungen. Diese werden durch die Überarbeitung von Fachexperten im Laufe der Zeit immer umfangreicher, das verwendete Vokabular immer fachspezifischer und für den Laien unverständlicher.

Vielfach muss der spätere Anwender diese Vorgaben wieder in eine für seine individuelle Situation passende und verständliche Sprache zurück übersetzen. Dieser Schritt ist für KMU nur schwer leistbar. Wir schlagen alternativ einen Leitfaden vor, der auf die Belange der KMU in Form und Formulierung eingeht, also einen wesentlichen Teil dieser Übersetzungsleistung vorwegnimmt. Dazu haben wir Good Practices und Experten-Knowhow in einer von der FHS St. Gallen durchgeführten Studie zusammengeführt [3]. Im vorliegenden Beitrag wurde der Aufbau dieses Leitfadens skizziert und inhaltliche Schwerpunkte begründet. Der eigentliche Leitfaden verwendet keine spezifischen Fachbegriffe oder komplexe Strukturen sondern überwiegend einfache Handlungsanweisungen und Checklisten. Wie die Referenz-Unternehmen unter den in der Studie analysierten KMU zeigen, kann dieser Leitfaden erfolgreich von kleineren Unternehmen ohne Hinzuziehen externer Berater und Experten umgesetzt werden.

Literatur

[1] Andreas Duscha: *Netz- und Informationssicherheit in Unternehmen 2009*. Studie des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk", 08.02.2010. http://www.ecc-handel.de/netz-_und_informationssicherheit_in_unternehmen_10467301.php

[2] European Network and Information Security Agency (ENISA): *Assessing a simplified Information Security approach*. 01.02.2009. http://www.enisa.europa.eu/act/rm/cr/infosec-smes/files/assessing-a-simplified-information-security-approach/at_download/fullReport

[3] Napoli, C., Holzmann, D., Triendl, T. Wieser, M.: *Geplante Katastrophenabwehr, Krisen und Notfallmanagement bei KMU*. Wissenschaftliches Praxisprojekt der FHS St. Gallen, 2009

[4] Richard Werner: *Business Continuity Management. Rüsten für den Krisenfall*. In ORGANISATOR, KMU-CONSULTING '07, 2007, S. 38-39

[5] Gantenbein, B., Morf, P.: *Business Continuity Management*. Theorie und Praxis am Beispiel einer Schweizer Privatbank. Publikation der Intercai (Schweiz) AG, 2006, http://www.intercai.ch/publikationen.cfm

[6] Business Continuity Institute: *Good Practise Guidelines, A Management Guide to Implementing Global Good Practice in Business Continuity Management*, Section 1 BCM Policy & Programme Management, 2008 http://www.thebcicertificate.org/pdf/GPG2008-2 Section 1 FINAL.pdf

[7] International Organization of Standardization (ISO): *ISO/PAS 22399:2007 Societal security – Guideline for incident preparedness and operational continuity management*, 2007

[8] National Fire Protection Association: *NFPA 1600 Standard on Disaster / Emergency Management and Business Continuity Programs*, 2007, http://www.nfpa.org/

[9] British Standards Institute: *BS 25999-1:2006 Business Continuity Management, Part 1: Code of practice, Part & 2: Specification*, www.thebci.org/standards.htm

[10] Standards Australia: *HB 221-2004 – Business Continuity Management Handbook*, originated as HB 221:2003, Second edition 2004.

[11] Standards Institution of Israel: *INS 24001:2007, Security and continuity management systems – Requirements and guidance for use*, 2007

[12] Bundesamt für Sicherheit in der Informationstechnik: *BSI Standard 100-4, Notfallmanagement*, 2008, https://www.bsi.bund.de/cae/servlet/contetblob/471454/publicationFile/30757/standard_1003.pdf

[13] *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)*, Bundesgesetzblatt, Deutschland, 1998, S. 786-794. http://www.bgblportal.de/BGBL/bgbl1f/b198024f.pdf

[14] Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht), Schweiz, vom 30. März 1911 (Stand am 1. Januar 2010) in der Systematischen Sammlung des Bundesrechts, http://www.admin.ch/ch/d/sr/220/index.html

[15] *Civil Contingencies Act 2004*, Großbritannien, 2004 http://www.statutelaw.gov.uk/cotent.aspx?activeTextDocId=915577

[16] The Sarbanes-Oxley Act of 2002, *Sarbanes-Oxley Act of 2002*, Pub. L. No. 107-204, 116 Stat. 745. Retrieved April 1, USA, 2009, http://www.sec.gov/about/laws/soa2002.pdf

[17] IDW RS FAIT 1 *Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie*. In: Die Wirtschaftsprüfung 21/2002, S. 1157 ff.

[18] IDW RS FAIT 2 *Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce*. In: Die Wirtschaftsprüfung 22/2003, S. 1258 ff

[19] IDW RS FAIT 3 *Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren*. In: Die Wirtschaftsprüfung 22/2006, S. 1465 ff

[20] Bundesanstalt für Finanzdienstleistungsaufsicht: *Mindestanforderungen an das Risikomanagement (BA), MaRisk*, Rundschreiben 15/2009 (BA), Geschäftszeichen: BA 54-FR 2210-2008/0001, Bonn / Frankfurt a.M., den 14.08.2009

[21] Mayer, H. O.: *Interview und schriftliche Befragung*. 4., überarbeitete und erweiterte Auflage, Oldenbourg Verlag, 2008.

[22] Kelle , U. & Erzberger, C.: *Qualitative und quantitative Methoden*. In: U. Flick, E.v.Kardoff & I. Steinke (Hrsg.), Qualitative Forschung. Ein Handbuch (S. 299-309). Rowohlt, Reinbek 2007

[23] Ditges, F., Höbel, P., Hofmann, T.: *Krisenkommunikation*. Uvk, 1. Auflage, 2008, S. 113

[24] Hohl, M. & Müller-Gauss, U.: *Schadensereignisse erfolgreich bewältigen*. In: KMU-Magazin Mai 2008.

[25] Asis International: *Business Continuity Guideline 2005*. http://www.asisonline.org/guidelines/guidelinesbc.pdf

[26] Swissbanking: *Empfehlungen für das Business Continuity Management (BCM). 2007* http://www.swissbanking.org/11107_d.pdf

[27] Von Campenhausen, C.: *Risikomanagement*. Orell Füssli Verlag, Zürich 2006