6-2014

From Disaster Response Planning to e-Resilience: A Literature Review

Florian Maurer
Vorarlberg University of Applied Sciences, Austria, florian.maurer@fhv.at

Ulrike Lechner
Universität der Bundeswehr München, Germany, Ulrike.Lechner@unibw.de

27th Bled eConference

eEcosystems

June 1 - 5, 2014; Bled, Slovenia

From Disaster Response Planning to e-Resilience: A Literature Review

Florian Maurer

Vorarlberg University of Applied Sciences, Austria

florian.maurer@fhv.at

Ulrike Lechner

Universität der Bundeswehr München, Germany

ulrike.lechner@unibw.de

Abstract

Natural and man-made crises as well as IT-security issues foster the interest in robust and resilient business information systems. Information and Communication Technologies (ICT) are essential for successful e-business. If ICT technologies interrupt, the whole (e-) business continuity is threatened. ICT interruptions causing serious loss in organization's reputation, trust and revenues. This circumstance should increase manager's interest in the concepts of disaster recovery planning (DRP), business continuity management (BCM) and, the emerging imperative, resilience. This paper at hand presents the results of a database driven literature review on these concepts and its interrelation.

Keywords: ICT-security, disaster response planning, business continuity management, resilience

1 Introduction

Information and Communication Technologies (ICT) are considered as the most vulnerable components in delivering uninterrupted services. When disruptions affect ICT operations, whole (e-) business ecosystems suffer from the interruption and its cascading effects. Statistics undermine that once affected organizations have serious problems in future and many do not survive[1].

[1] e. g. 40 % of companies that were shut down by a disaster for three days failed within 36 months (Zheng et al., 2013); 93 % of the companies after five years after a major and unexpected system shutdown (Nelson, 2006); 80 % of businesses affected by a major incident close within 18 months. 90 % of businesses that loose data from a disaster are forced to shut down within two years (Tjoa et al., 2008).

This paper at hand presents the results of a literature review in the electronic database IEEExplore on disaster response planning (DRP), business continuity management (BCM) and resilience. It explores these concepts and the role of DRP and BCM in creating resilience. This literature review also reflects the perception of the concepts in technology-oriented literature.

The aim of this paper is to examine the origin and status quo of above mentioned concepts and to give an outline and extended view. Further aims are to highlight the overlapping and interrelations of these concepts.

The paper is organized as follows: In section 2 the research design is presented. Section 3 presents the literature review. Section 4 presents the findings and contains a brief conclusion.

2 Research Design

Used methodology for this paper is the literature review. Hart (2003) defines a literature review as the "selection of available documents […] on topic, which contain information, ideas, data and evidence written from a particular standpoint to fulfil certain aims or express certain views on the nature of the topic and how it is to be investigated, and the effective evaluation of these documents in relation to the research being proposed". The paper at hand uses quantitative and qualitative methods of the frequency and document analysis. These methods are appropriate to categorize the content and to structure the evaluation and interpretation of data. The literature review follows the structure proposed by Lamnek (1995), which is also visualized in Figure 2.

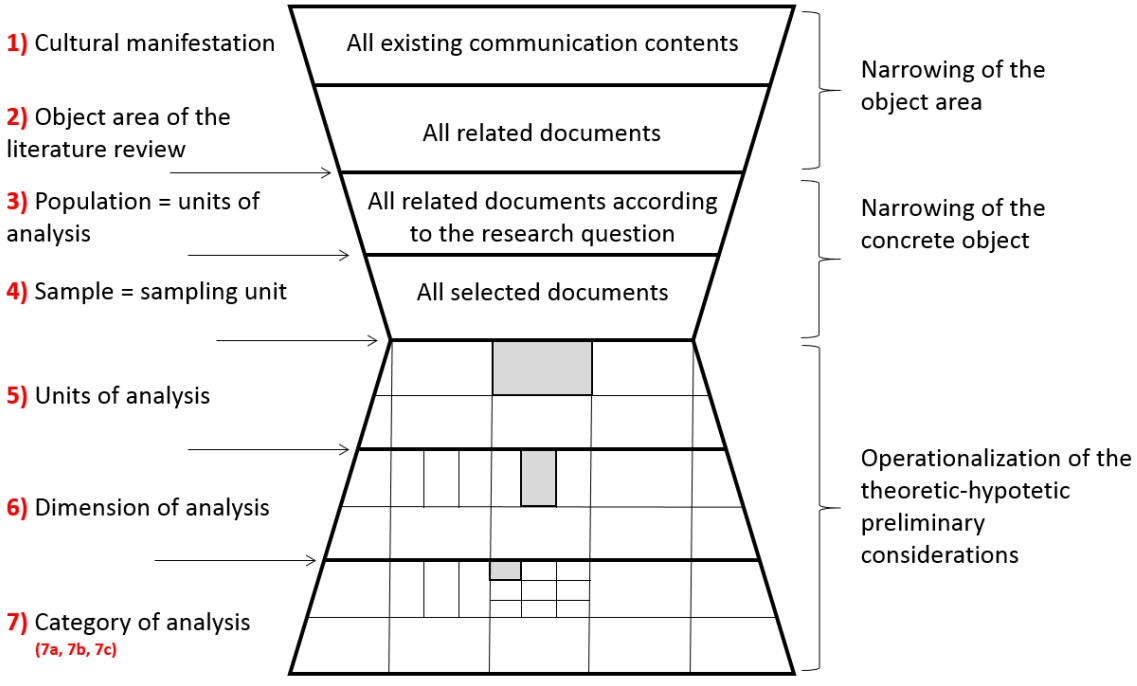

Figure 1: Schematic visualization of the approach of the literature review (Lamnek, 1995)

Cultural manifestation & object area of the literature review: The literature research bases on the electronic database IEEExplore (ieeexplore.ieee.org). This database offers

a good coverage of scholarly and practice-oriented publications and gives access to the latest research of the world's largest community of IT-technology professionals.

The literature search was conducted on the 15th of January 2014 and the 06th of March 2014 with full-text terms "Disaster Recovery Planning", "IT Disaster Recovery", "Business Continuity Planning" "Business Continuity Management" and "Business-Continuity-Management". The search was designed to include publications from year 2005 to 2013. The results of each search are listed in Table 1.

Data-base	Search Term	Re-ductions	Result	Useable + Wildcards	Not down-load-able	Non-Useable
IEEE Explore	Disaster Recovery Planning	Papers from 2005 - 2013	26	15	1	10
	IT Disaster Recovery		1	1		
	Business Continuity Planning		22	12	1	9
	Business Continuity Management		29	13	2	14
	Business-Continuity-Management		28	15		13
		Sum	106	56	4	46
		- doubles		-6		
		Total		50		

Table 1: Literature research statistics

Population & Sample: The database search resulted in a total of 106 papers. Four search results turned out because they were table of contents or not downloadable. Papers that the authors consider are papers with nine or more citations in google.scholar.com. The amount of nine marks the average of all citations of found papers. 67 papers had less than nine quotations. These 67 underwent an individual review for relevance. Nevertheless, 21 of these 67 papers got included. Thus, the sample consists of a total of 50 reviewed publications.

As the following tables show, six papers were submitted and presented at symposiums or workshops, 25 papers were submitted at conferences and 19 papers were published in journals.

Workshops	Year
Business-driven IT Management, 2008. BDIM 2008. 3rd IEEE/IFIP International Workshop on	2008
Electronic Commerce and Security, 2009. ISECS '09. Second International Symposium on	2009
Enterprise Distributed Object Computing Conference Workshops, 2009. EDOCW 2009. 13th	2009
Database and Expert Systems Applications (DEXA), 2011 22nd International Workshop on	2011
Software Reliability Engineering Workshops (ISSREW), 2012 IEEE 23rd International Symposium on	2012
Reliability and Maintainability Symposium (RAMS), 2013 Proceedings - Annual	2013

Table 2: Symposiums and workshops

Conferences	Year
Systems Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on	1999
Parallel and Distributed Computing, Applications and Technologies, 2005. PDCAT 2005. Sixth International Conference on	2005
Semantics, Knowledge and Grid, 2005. SKG '05. First International Conference on	2005
System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on	2006
Military Communications Conference, 2006. MILCOM 2006. IEEE	2006
International Professional Communication Conference, 2006 IEEE	2006
Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on	2007
Systems Conference, 2007 1st Annual IEEE	2007
Availability, Reliability and Security, 2008. ARES 08. Third International Conference on	2008
Rural Electric Power Conference, 2008 IEEE	2008
Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on	2008
Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on	2008
Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on	2009
Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference	2009
Security Technology (ICCST), 2010 IEEE International Carnahan Conference on	2010
Quality of Information and Communications Technology (QUATIC), 2010 Seventh International Conference on the	2010
Management and Service Science (MASS), 2010 International Conference on	2010
Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on	2010
Research and Innovation in Information Systems (ICRIIS), 2011 International Conference on	2011
GCC Conference and Exhibition (GCC), 2011 IEEE	2011
Availability, Reliability and Security (ARES), 2011 Sixth International Conference on	2011
Service Operations and Logistics, and Informatics (SOLI), 2012 IEEE International Conference on	2012
Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference on	2012
Technology Management for Emerging Technologies (PICMET), 2012 Proceedings of PICMET '12:	2012
Complex, Intelligent, and Software Intensive Systems (CISIS), 2013 Seventh International Conference on	2013

Table 3: Conferences

Amount	Journals	Year
	Engineering Management, IEEE Transactions on	1998
	Potentials, IEEE	2003
	Security & Privacy, IEEE	2004
	Dependable and Secure Computing, IEEE Transactions on	2005
	Manufacturing Engineer	2005
	Software, IEEE	2005
	IT Professional	2006
	Computer	2007
	Technology and Society Magazine, IEEE	2007
2 x	IT Professional	2008
	Systems Journal, IEEE	2009
	IT Professional	2009
	Security & Privacy, IEEE	2010
	Services Computing, IEEE Transactions on	2011
	IT Professional	2012
	Network and Service Management, IEEE Transactions on	2013
	Industry Applications Magazine, IEEE	2013
	Human-Machine Systems, IEEE Transactions on	2013

Table 4: Journals

Table 5 provides an overview, when the papers got published.

	All		Syposium / Workshops		Conferences		Journal Publications	
	Amount	Year	Amount	Year	Amount	Year	Amount	Year
	1 x	1998				1998	1 x	1998
	1 x	1999			1 x	1999		1999
	1 x	2003				2003	1 x	2003
	1 x	2004				2004	1 x	2004
	5 x	2005			2 x	2005	3 x	2005
	4 x	2006			3 x	2006	1 x	2006
	4 x	2007			2 x	2007	2 x	2007
	7 x	2008	1 x	2008	4 x	2008	2 x	2008
	6 x	2009	2 x	2009	2 x	2009	2 x	2009
	5 x	2010			4 x	2010	1 x	2010
	5 x	2011	1 x	2011	3 x	2011	1 x	2011
	5 x	2012	1 x	2012	3 x	2012	1 x	2012
	5 x	2013	1 x	2013	1 x	2013	3 x	2013
Total	50		6		25		19	

Table 5: Overview paper presentation / publication

Operationalization: After the scan- and skim-reading process of the samples, in total, 733 quotations ***(Category of analysis 3)*** got marked and clustered to 78 codes ***(Category of analysis 2)***. A quotation is an important rated text passage in a sample. A code is the aggregation of similar quotations found in different samples. The codes got clustered to 21 families ***(Category of analysis 1)***, which are the generic term of all quotations and the lowest level of analysis. Again, the families got clustered to eight super-families. Super-families symbolize the ***dimension of analysis*** and are comparable with a subset of the whole (unit). The super-families are summarized to five categories. These categories symbolize the ***units of analysis***. Table 6 visualizes the built categories and the amount of assigned super-families, families, codes and quotations.

	assigned ...			
Categories / Chapters	Super-families	Families	Codes	Quotations
= Units of Analysis	*= Dimension of Analysis*	*= Category of Analysis 1*	*= Category of Analysis 2*	*= Category of Analysis 3*
1) Introduction & definition DRP & BCM	2	10	52	590
2) BCM / DRP in theory & practice	1	2	11	149
3) Standards and related concepts	3	6	15	160
4) Resilience	1	1	6	162
5) Future Outlook	1	3	3	54

Table 6: Units of analysis *(and its clustering results)*

Figure 3 visualizes the clustering process. As this figure shows, it was possible to assign one quotation *(, code)* to "n" codes *(, families)*. "n" families *(, super-families)* were summarized in one super-family *(, category)*. Data management was handled with Microsoft Excel and Atlas.ti.

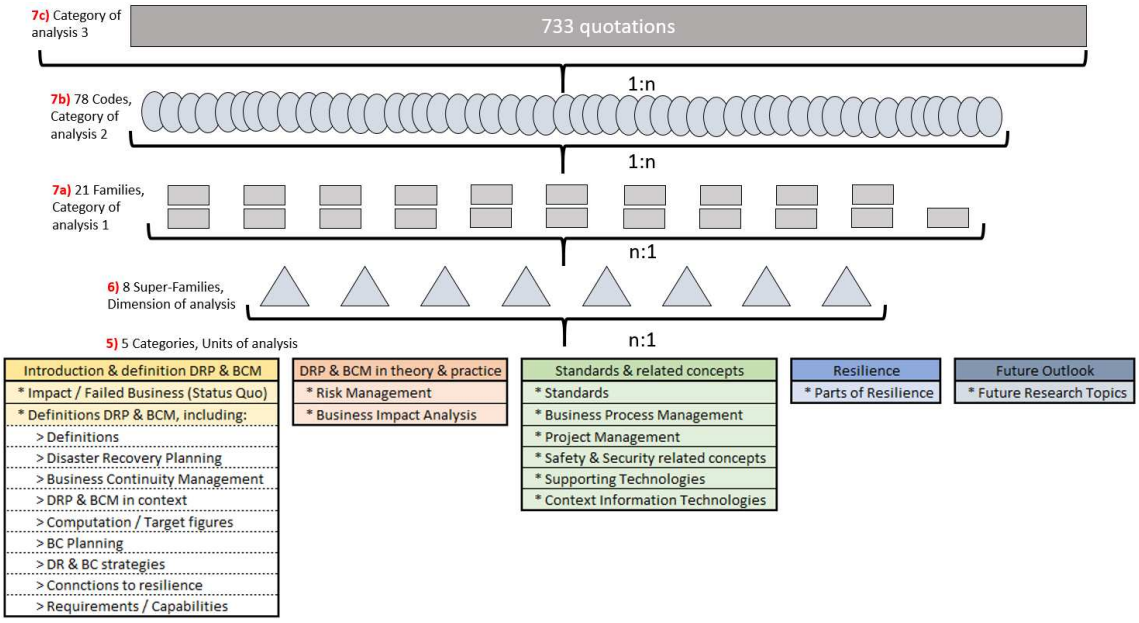

Figure 2: Clustering process

A first realization is that organizational security and continuity is well discussed in analysed literature. The concepts of DRP and BCM are well explored *(according to the quotations; see table 6)* and experience continuous and sustaining consideration *(according to table 5)*. Also, a larger amount of standards and related concepts could be identified. In comparison, the concept of resilience is underrepresented *(according to the quotations; see table 6)* and it seems to be an emerging approach in this field of research.

3 Literature Review

In the following chapters, the results of the categories "**Introduction & definition DRP & BCM**", "**DRP & BCM in theory & practice**" and "**Resilience**" get presented. Because of the limited results of the categories "**Standards & related concepts**" and "**Future Outlook**", their outputs are integrated in above chapters.

3.1 Disaster Response Planning & Business Continuity Management

This chapter is presented in five subchapters: the first subchapter is about the definition of DRP and BCM. The next chapters aim to present the various notions of DRP and BCM and the interrelation to resilience.

3.1.1 Introduction, Definition and Target Figures of DRP & BCM

Roberts (2006) and Fallara (2004) highlight that 86 % of IT- and business disruption are planned occurrences (e. g. by IT backups). ~13 % are caused by unplanned events (e. g human error, database corruption, etc.) and only less than 1 % is caused by "high impact low probability" (HILP) events. Alhazmi & Malaiya (2012), Winkler et al. (2010) and O'Callaghan & Mariappanadar (2008) state out that continuity planning is a vital requirement. Several authors as Nelson (2006), Tjoa et al. (2008), Lawler et al. (2007), Zheng et al. (2013) highlight that organizations which experience a disruption and do not have DRP and BCM in use eventually will fail. Also, they refer to the direct impacts

of disruptions on revenues, stock price, customer loyalty and satisfaction, business reputation and loss of market share as the reasons. Jorden (1999), Iyer & Sarkis (1998), Cousins (2007) and Dey (2011) summarize that DRP and BCM experience low commitment and most organizations have any or only little experience. These authors also argue, while some organizations realize that the lack of proper DRP and/or BCM can make them out of business at any time, others still try to protect themselves with business interruption services as e. g. insurances.

As Nelson (2006), Kolb (2008), Ncemane & Weeks (2012) and Draheim & Pirinen (2011) argue: Some consider the context of DRP and BCM as synonymous, others view DRP as more tightly focused on areas around IT systems. Nelson (2006), Winkler et al. (2010) and Tsai & Sang (2010) argue that nowadays information continuity equals business continuity. Therefore BCM must integrate IT security into its comprehensive planning process. Nelson (2006) highlights that organizations with BCM typically have a DRP either integrated or maintained as separate. Lawler et al. (2007), Ncemane & Weeks (2012), Draheim & Pirinen (2011), Shao (2005) and Wan & Chan (2008) define BCM as an umbrella concept, which encompassing a range of operational elements, including DRP. Wan & Chan (2008) and Elliott et al. (2010) highlight that BCM has its origin in DRP – but with an extended scope to the whole organization. Both concepts incorporate "acts of anticipating disruptions, ensuring prevention or less chance of occurrences and responding to any such incident in a planned and rehearsed manner so as to recover the losses and bring the business back into operation" (Shao, 2005). DRP and BCM can be considered as IT- and (e-) business continuity concepts with the following scope:

- DRP normally takes care of the continuity of ICT services and is mostly technical in nature (Dey, 2011). DRP focuses on restoring critical business processes and related ICT systems (Cha, Juo, Liu, & Chen, 2008). As Hoong & Marthandan (2011) note, DRP contains adequate details for technical recovery, but it takes less interest on people and communication issues.
- BCM does not address information technology outage as the only threat (Shao, 2005). BCM is about as many organizational threats and vulnerabilities as possible. BCM helps preparing the organization to handle them as well as possible (Draheim & Pirinen, 2011) in a way that prevents the organization from fulfilling its mission (Draheim & Pirinen, 2011). BCM defines how to establish alternative processes and information systems if critical parts cannot be restored within the scheduled deadline for recovery (Cha et al., 2008).

The following table summarizes operational targets of DRP and BCM.

Code	Definition	Literature
Fault, risk and disaster tolerance & criticality	Risk and disaster tolerance is a superset of fault tolerance; tolerance is the ability for a business to cope with the interruption. Criticality is related to the cost entailed for a process to be out for a period of time.	Fallara (2004), Lawler et al. (2007), Wan & Chan (2008) & criticality Fallara (2004)
Recovery time objective (RTO)	RTO is defined as the duration in which business functions is unavailable and must be restored (maximum time of permissible interrupt, time need / taken to restore; defines the "target time for resumption of product, service or activity delivery after an incident.	Alhazmi & Malaiya (2012), Hoong & Marthandan (2011), Wang et al. (2005), [12]
Recovery point objective (RPO)	RPO defines the limits / maximum amount of (data) loss an organization can sustain during an event.	Alhazmi & Malaiya (2012), Wang et al. (2005), Winkler et al. (2010)
Maximum tolerable period of disruption (MTPD) / Maximum Tolerable Downtime (MTD)	MTPD expresses the maximum acceptable downtime to guarantee the business continuity.	Zambon et al. (2007), Grimaila (2004), Rejeb et al. (2012), McDonald (2008), Dey (2011)
Availability	Is the ratio of time a system is functional to the total time availability and get computed by MTBF / (MTBF + MTTR)	Tsai & Sang (2010), [32]
Mean Time to Recovery (MTTR)	MTTR is the mean / average time to repair the failure and get back into business / service	Dey (2011), Tsai & Sang (2010), Costello (2012)

Table 7: Code, Definitions and Literature on Evaluation and Quantification of DRP and BCM

3.1.2 Planning for Continuity

According to Nelson (2006), a DR or BC plan documents various aspects of disaster preparations. A main task is to provide organization-wide policies and guidelines in case a disruption hit (Dey, 2011), (Wang et al., 2005), (Wang, Yin, Yuan, & Zhou, 2005) *(guaranteeing that incidents do not affect critical core processes and the availability of (IT) services (Wan & Chan, 2008), (Zambon et al., 2007))*. According to Grimaila (2004), further tasks of DR and BC planning include risk management, evaluation, incident and scenario planning, ethics, communication, security awareness education and training, etc. As Rejeb et al. (2012), Hoong & Marthandan (2011) and McDonald (2008) highlight, most BC plans are textual template documents and could be made up of many smaller plans. However, these documents need to have a good requirement definition (Roberts, 2006) and consist of:

- Owner structure (Costello, 2012)
- Formal BCM coordinators and BC team (Nelson, 2006), (Costello, 2012), (Xiang et al., 2008)
- Disaster management plan including incident and scenario plan (Jorden, 1999), (Dey, 2011), (Cha et al., 2008), (Hoong & Marthandan, 2011), (Wang, Zhou, et al., 2005), (Hayhoe, 2006)
- Prioritization of recovery objects (Costello, 2012) including backup and recovery procedures, system and work area recovery plan (Hoong & Marthandan, 2011), (Wan & Chan, 2008)
- Communication and corresponding plan (Hoong & Marthandan, 2011), (Wang, Zhou, et al., 2005), (Grimaila, 2004), (Costello, 2012)
- Specification of system and network infrastructure (Wan & Chan, 2008)
- Knowledge management practices (Nelson, 2006), (Hayhoe, 2006).

A vital requirement to continuity planning is the commitment of the strategic management level and the integration of DR & BC within the current operations (Roberts, 2006). DR & BC plans *(as result of DR & BC planning process)* do not mark the end of continuity efforts: As Nelson (2006), Dey (2011), Wan & Chan (2008) highlight, plans must be updated and tested frequently.

3.1.3 Continuity Strategies

The observed literature suggest following strategies to maintain IT- and (e-) business continuity:

- Strategic management commitment and adequate financial support (Hoong & Marthandan, 2011), (Nelson, 2006), (Tjoa et al., 2008), (Jorden, 1999), (McDonald, 2008)
- Investments in technology (Fallara, 2004), (Liu & Ormaner, 2009)
- Redundancy (Nelson, 2006), (Fallara, 2004), (Shao, 2005), (Hoong & Marthandan, 2011), (McDonald, 2008), (Alhazmi & Malaiya, 2013)
- Backup strategies (Nelson, 2006), (Fallara, 2004), (Alhazmi & Malaiya, 2012), (Tsai & Sang, 2010), (Hoong & Marthandan, 2011), (Wang, Zhou, et al., 2005), (Garlick, 2011)
- Active planning and testing (Fallara, 2004), (Alhazmi & Malaiya, 2012), (Hoong & Marthandan, 2011), (McDonald, 2008), (Gang, 2009)

  DRP and BCM must be executable, testable, scalable and maintainable (Alhazmi & Malaiya, 2012); include planning, scheduling, facilitation, communications, auditing and view documentation
- Flexibility and equipment replacement (Nelson, 2006), (Fallara, 2004), (Gang, 2009)

  e. g. by establishing of procedures and policies for coordinating continuity and restoration activities with external agencies (vendor agreements, equipment inventories, etc.)
- Optimization, incident management and scenario planning (O'Callaghan & Mariappanadar, 2008), (Hoong & Marthandan, 2011)
- Training and education (Liu & Ormaner, 2009)

  e. g. to create employee awareness of organizational security policies and practices
- Information sharing and communication (Zheng et al., 2013)

  e. g. to build a culture in which employees are willing and able to follow policies and practices

3.1.4 Continuity requirements and capabilities

Active and successful continuity planning requires a subset of organizational capabilities. Summarized, these capabilities are:

- Serious management commitment

  According to Nelson (2006), Tjoa et al. (2008), Jorden (1999), Hoong & Marthandan (2011) and McDonald (2008), to develop and maintain a common sense, the commitment of all business levels *(incl. the board of managers)* is necessary. Further requirements are an adequate management infrastructure (Nelson, 2006), (Hoong & Marthandan, 2011), formal coordinators (leaders,

leading team), documented and communicated roles and responsibilities (teams and awareness programs) as well as adequate financial support (Hoong & Marthandan, 2011).

- Continuity strategy

  DRP and BCM needs a clear strategy (incl. technology strategy (Nelson, 2006)) which has to be embedded in the organization's culture (Tjoa et al., 2011). It is important to integrate all employees from all operations (Roberts, 2006), (Fallara, 2004). Also business management practices, information resources, staff (life, safety and availability) and telecommunications (McDonald, 2008), (Dey, 2011) needs to be considered.

- Plan development and execution

  Existing plans needs to be audited, exercised, and re-worked regularly (Nelson, 2006), (Fallara, 2004), (Alhazmi & Malaiya, 2012), (Wang, Zhou, et al., 2005), (Gang, 2009).

- Training and counselling

  Managers and employees needs to be educated continously (Hoong & Marthandan, 2011), (Liu & Ormaner, 2009), (Gang, 2009).

- Periodic reporting

3.1.5 DRP's and BCM's interrelation with the concept of Resilience

As Madni & Jackson (2009) argue, resilience is a multi-faceted capability that encompasses avoiding, absorbing, adapting to, and recovering from disruptions. Nelson (2006), Tjoa et al. (2008) and Ncemane & Weeks (2012) identify DRP and BCM as cornerstones in the concept of resilience. For example, Nelson (2006) argues that DRP also represent a critical component of IT resilience. Tjoa et al. (2008) highlights that BCM is a prerequisite to strengthen the organization's resilience. They argue that BCM is a management process to improve resilience. Also the British Standard 25999 attributes BCM to build a framework for building resilience. Characteristics of resilience in context with DRP and BCM are:

- Flexibility *(continuous, flexible services)*: According to Nelson (2006), Garlick (2011) and Senda et al. (2013), resilience *(as well as BCM & DRP)* includes providing active services by ensuring the continued existence of critical data and systems, also after disastrous events.

- Redundancy: Hoong & Marthandan (2011) argue, resilience focus on critical assets which support key business processes, including building, equipment, technology, human resources and third party relationships.

- Risk Management: According to Garlick (2011) and Madni & Jackson (2009), *(equal to BCM and DRP)* resilience includes the reduction of exposure to cascading catastrophic events. Resilience is a proactive approach that looks for ways to enhance the ability of organizations to explicitly monitor risks.

3.2 Risk management (and BIA)

Object of examination were the concepts of "Risk Management" and "Business Impact Analysis" (BIA). As the literature review shows, these concepts are main-pillars of DRP and BCM. Risk management and BIA are sufficiently described in several national and international standards and guidelines. Due to this fact, the authors present a meaningful summary.

Tjoa et al. (2008) argue that risk management and BIA enable efficient and effective BCM as they deliver information about the impact of resources' disruption on business. Both are important components of BC planning (Dey, 2011). According to British Standard 25999 *(in Zambon et al. (2007))*, in the centre are the identification of activities and processes supporting the core services used by the organization, the identification of relationships and dependencies between activities and processes as well as the evaluation of the impact of a disruption to core services and processes. Risk management is the previous tasks of a successful BIA. According to Fallara (2004), risk management identifies the business processes, internal and external threats and vulnerabilities and classifies them by how critical they are to the overall business. Wang, Zhou, et al. (2005) quote, BIA basically analyses how a terminated resource affects other resources. BIA is to determine the impact for the organization a particular process has if it is out for a period of time.

Supporting standards and guidelines identified are BS25999, CIP, HB 221, IEEE P1700, ISO 13335, ISO 17799, ISO 22399, ISO 24762, ISO 27001, etc.

3.3 Resilience

Ncemane & Weeks (2012) see resilience as an umbrella concept which encompasses BCM and DRP. Tjoa et al. (2011) understand BCM as a management process to improve resilience in an organization.

3.3.1 Origin & Definition of Resilience

Senda et al. (2013) highlight, resilience is originally a term used and physics. It means the property of a material that enables it to resume its original position after being bent, stretched, or compressed. After the September 11th attacks resilience also became popular in social and business science. In 2004, the term became popular in psychology. The central idea is that failure is not necessarily a consequence of malfunction or poor design – it is a result of ongoing interactions and adaptions (Madni & Jackson, 2009). Westrum *(in Madni & Jackson (2009))* highlights that resilience is a term determined by at least two of the following: avoidance, survival, and recovery. The opposite of resilience is brittleness (Madni & Jackson, 2009).

3.3.2 Capabilities of resilient organizations

Resilience is a measure of the persistence of an organization and its ability to absorb change and disturbance (Ncemane & Weeks, 2012). Madni & Jackson (2009) distinguishes between two types of resilience: reaction and adaptation. Reaction implies *(for Madni & Jackson (2009))* immediate or short-term action while adaptation implies long-term learning. Adaption is underpinned by situational awareness and understanding key vulnerabilities. According to Ncemane & Weeks (2012) a resilient

framework is achieved, when the organization is able to bounce back. This includes the organizational abilities to …

- avoid, survive and recover from unpredicted disruptions (Ncemane & Weeks, 2012), (Madni & Jackson, 2009); *(resilience looks for ways to enhance the ability of organizations to explicitly monitor risks)*;
    - avoid: reduce the exposure to cascading catastrophic events (Garlick, 2011).
    - survive: provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation *(Sterbenz et al. in Madni & Jackson (2009))*; recover and stabilize following unexpected and unknown disrupt occurrences *(Oldfield in Ncemane & Weeks (2012))*.
    - recover: quickly return to normal operations; maintain effective operational level with minimal disruption to its performance (Ncemane & Weeks, 2012) if hit by a disruption.
- continue flexible and continuous services; ensuring the continued existence of critical data and systems (Garlick, 2011).
- circulate bad news and deal with the root causes quickly (Sheffi, 2005).

To be resilient means to maintain a strong sense of relationship, cooperation shared values, beliefs, and trust between employees, management, suppliers, partners and entities (Ncemane & Weeks, 2012). Strong leadership *(rather than management)* is essential which includes to interact with and empower its people, diversity in the workplace (Ncemane & Weeks, 2012), forward thinking and the development of survival instincts *(Sundstrom and Hollnagel in Ncemane & Weeks (2012))*. Well planned communication and change management *(agility to changed circumstances)* is essential to effectively adapt to turbulent changes. Resilience incorporates learning and knowledge sharing, adaption and experimentation (Ncemane & Weeks, 2012), (Madni & Jackson, 2009).

3.3.3 Resilience in context and its interrelation to safety, reliability & survivability

Resilience can be seen and argued from different viewpoints. Views are:

- Informatics: resilience is seen as the availability of computer systems which offer uninterrupted system access and services (Nelson, 2006). To maintain uninterrupted services, redundancy, data backup strategies, flexibility etc. need to be developed.
- Organization theory: resilience is achieved when the individuals and organizations continually adjust its performance to the prevailing conditions (Madni & Jackson, 2009).
- Supply chain management: resilience can be achieved either through redundancy or building in flexibility (Sheffi, 2005).

According to Madni & Jackson (2009) resilience is highly related to safety, reliability and survivability:

- Safety: ability of a system understanding how it can proactively ensure things stay under control (safety as a property, defined in terms of adherence to standards, policies, and error typology).
- Reliability: ability of a system to perform required functions under stated conditions.
- Survivability: ability to withstand attacks or countermeasures; ability to minimize the impact of a disruption achieved through (1) providing a minimal acceptable level of value delivery during and after a disruption or (2) the reduction of the likelihood or magnitude of disruption.

4 Findings & Conclusion

This paper presents a literature review on the perception of the concepts of DRP, BCM and resilience. A realization is that the database IEEE is a mainly (IT-) technical database. The findings are mainly technically nature and underlined with technical aspects. It is not a surprise that the concept of resilience is underrepresented. The concept of resilience include soft as e. g. the strong sense of *(internal and external)* relationships, shared values, cooperation, trust, etc.

The literature review shows, that DRP and BCM are concepts to establish, maintain and enhance ICT- and (e-) business continuity – also in face of organizational adversity. Both are related to security. While DRP is a specialized approach to ICT, BCM is related to the whole organization. BCM has its roots in DRP and includes ICT. On the one hand, DRP and BCM are seen as framework to develop resilience. On the other hand, resilience supports and enhances DRP and BCM. However, resilience extends the security views and adds safety, reliability and survivability. The concept of resilience is more interdisciplinary and is known, for example in the field of physics, psychology, emergency response, etc.

As some authors highlighted, once hit by a disruption, organizations have serious problems to keep business ongoing. As the literature review shows, reasons installing DRP, BCM and resilience are because of this internal and external, planned as well as unplanned risks and threats. With these concepts, managers try to avoid HILP events and improve the response options if a disruption hit.

4.1 Representation of DRP, BCM and resilience in literature

Table 6 shows that 590 quotations are in direct *(or indirect)* relation to the concepts of DRP and BCM. 168 *(or 28 %)* of these, found in 40 samples, are used for the literature review. According to the quotations, the concept of resilience is underrepresented in DRP and BCM. During the literature research, 162 quotations were coded *(see table 6)*. 41 *(or 25 %)* of these quotations were used for the literature review. The used quotations refer to a total of eight samples. These confirm the authors assumption that resilience in the field of DRP and BCM is an emerging topic.

Risk management and BIA are highly supported by several international standards. The most frequently mentioned standards are BS 25999, NIST SP-800, NFPA 1600 and ISO 22399. Although, 149 quotations were coded, only four authors were used for this subsection.

The following table visualizes a summary about the used samples, used quotations, average quotations and the authors above and below the average:

Section	Topic	Used Papers for the literature review	Used quotations	Average quotations	Authors above the average	Authors under the average
3.1	DRP & BCM	40	168	4,2	Nelson (2006), Hoong & Marthandan (2011), Fallara (2004), Dey (2011), Alhazmi & Malaiya (2012), Wang et al. (2005), McDonald (2008), Wan & Chan (2008)	Costello (2012), Tjoa et al. (2008), Winkler et al. (2010), Jorden (1999), Garlick (2011), Liu & Ormaner (2009), Grimaila (2004), Wang et al. (2005), Cha et al. (2008), Ncemane & Weeks (2012), Lawler et al. (2007), Madni & Jackson (2009), Tjoa et al. (2011), Zambon et al. (2007), Hayhoe (2006), Kolb (2008), O'Callaghan & Mariappanadar (2008), Senda et al. (2013), Alhazmi & Malaiya (2013), Xiang et al. (2008), Rejeb et al. (2012), Elliott et al. (2010), Cousins (2007), Iyer & Sarkis (1998), Zheng et al. (2013), Gang (2009), Shao (2005), Tsai & Sang (2010), Draheim & Pirinen (2011), Roberts (2006)
3.2	Risk Management & BIA	4	4	1,0	Used authors: Fallara (2004), Dey (2011), Wang et al. (2005), Zambon et al. (2007); Result not representative	
3.3	Resilience	8	41	5,1	Madni & Jackson (2009), Alhazmi & Malaiya (2012), Dey (2011)	Garlick (2011), Sheffi (2005), Nelson (2006), Tjoa et al. (2011), Senda et al. (2013)

Table 8: Summary of used samples and quotations

4.2 Relevance

The most influencing samples in DRP and BCM are Nelson (2006), Hoong & Marthandan (2011), Fallara (2004) and Dey (2011). In total, they include one third of all used quotation. In resilience, the most influencing samples are Madni & Jackson (2009), Alhazmi & Malaiya (2012) and Dey (2011). They include 83 % of all used quotations.

According to the used quotations, the most important multi-disciplinary samples are Nelson (2006), Alhazmi & Malaiya (2012), Dey (2011) and Madni & Jackson (2009). Alhazmi & Malaiya (2012) and Dey (2011) are above the average quotations in subsection DRP / BCM and subsection resilience. However, Nelson (2006) is above the average quotation in subsection DRP / BCM and Madni & Jackson (2009) is above the average in subsection resilience. In total, these four samples incorporate more than one third *(35 %)* of all used quotations in these sections.

The following table visualizes the amount of used quotation per sample. Also, the table shows, where and when the samples above the average per subsection got presented or published.

Quotation(s)	DRP & BCM	RM	Resilience	Presented at / Published in	Year
1	Zheng et al. (2013), Iyer & Sarkis (1998), Cousins (2007), Elliott et al. (2010), Rejeb et al. (2012), Xiang et al. (2008), Alhazmi & Malaiya (2013), Senda et al. (2013)	Fallara (2004), Dey (2011), Wang et al. (2005), Zambon et al. (2007)	Nelson (2006), Tjoa et al. (2011), Senda et al. (2013)		
2	O'Callaghan & Mariappanadar (2008), Kolb (2008), Zambon et al. (2007), Hayhoe (2006), Tjoa et al. (2011), Madni & Jackson (2009)		Garlick (2011), Sheffi (2005)		
3	Lawler et al. (2007), Ncemane & Weeks (2012), Cha et al. (2008), Wang et al. (2005), Grimaila (2004), Liu & Ormaner (2009), Garlick (2011)				
4	Jorden (1999), Roberts (2006), Draheim & Pirinen (2011), Tsai & Sang (2010), Shao (2005), Gang (2009)				
4,2	Average				
5	Winkler et al. (2010)			Quality of Information and Communications Technology (QUATIC), 2010 Seventh International Conference on the	2010
5,1			Average		
6	Tjoa et al. (2008)			Availability, Reliability and Security (ARES), 2011 Sixth International Conference on	2011
	Costello (2012)			IT Professional	2006

7	Wan & Chan (2008)			Business-driven IT Management, 2008. BDIM 2008. 3rd IEEE/IFIP International Workshop on	2008
	Wang et al. (2005)			Parallel and Distributed Computing, Applications and Technologies, 2005. PDCAT 2005. Sixth International Conference on	2005
	McDonald (2008)			Rural Electric Power Conference, 2008 IEEE	2008
	Alhazmi & Malaiya (2012)			Software Reliability Engineering Workshops (ISSREW), 2012 IEEE 23rd International Symposium on	2012
9	Dey (2011)			GCC Conference and Exhibition (GCC), 2011 IEEE	2011
10	Fallara (2004)			Potentials, IEEE	2003
11			Dey (2011)	GCC Conference and Exhibition (GCC), 2011 IEEE	2011
			Alhazmi & Malaiya (2012)	Software Reliability Engineering Workshops (ISSREW), 2012 IEEE 23rd International Symposium on	2012
12			Madni & Jackson (2009)	Systems Journal, IEEE	2009
16	Wang et al. (2005)			Research and Innovation in Information Systems (ICRIIS), 2011 International Conference on	2011
20	Nelson (2006)			System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on	2006

Table 9: Statistic of used quotation per sample

At this place, the authors point out that in the concept of resilience, several authors from different fields of research got cited *(e. g. Sterbenz et al.; Westrum (in Madni & Jackson (2009)), Oldfield; Sundstrom and Hollnagel (in Ncemane & Weeks (2012))*. This confirms again the authors' assumption, that the concept of resilience in DRP and BCM get adopted from other fields of research.

4.3 (Overlapping) Strategies and extended strategies

Top continuity strategies in the concept of DRP and BCM are backups, redundancies, management commitment and active planning and testing. The following table visualizes the strategies and its rating by quotations.

Strategy	Quotations	Samples
Backup	7	Nelson (2006), Fallara (2004), Alhazmi & Malaiya (2013), Tsai & Sang (2010), Hoong & Marthandan (2011), Wang et al. (2005), Garlick (2011)
Redundancy	6	Nelson (2006), Fallara (2004), Shao (2005), Hoong & Marthandan (2011), McDonald (2008), Alhazmi & Malaiya (2013)
Management Commitment	5	Nelson (2006), Tjoa et al. (2008), Jorden (1999), Hoong & Marthandan (2011)
Active planning & testing	5	Fallara (2004), Alhazmi & Malaiya (2013), Hoong & Marthandan (2011), McDonald (2008), Gang (2009)
Flexibility	3	Nelson (2006), Fallara (2004), Gang (2009)
Optimization, indcident management and scenario planning	3	Nelson (2006), Fallara (2008), Gang (2009)
Technology	2	Fallara (2004), Liu & Ormaner (2009)
Training & education	1	Liu & Ormaner (2009)
Information sharing	1	Zheng et al. (2013)

Table 10: DRP and BCM strategies

Training and education as well as information sharing, which are essentials in the concepts of resilience, are underrepresented in DRP and BCM. Overlapping strategies within the concept of resilience are flexibility and redundancy, as well as the use of risk management as anticipation and mitigation method.

References

Alhazmi, O. H., & Malaiya, Y. K. (2012). Assessing Disaster Recovery Alternatives: On-Site, Colocation or Cloud. In *2012 IEEE 23rd International Symposium on*

Software Reliability Engineering Workshops (ISSREW) (pp. 19–20). doi:10.1109/ISSREW.2012.20

Alhazmi, O. H., & Malaiya, Y. K. (2013). Evaluating disaster recovery plans using the cloud. In *Reliability and Maintainability Symposium (RAMS), 2013 Proceedings - Annual* (pp. 1–6). doi:10.1109/RAMS.2013.6517700

Cha, S.-C., Juo, P.-W., Liu, L.-T., & Chen, W.-N. (2008). RiskPatrol: A risk management system considering the integration risk management with business continuity processes. In *IEEE International Conference on Intelligence and Security Informatics, 2008. ISI 2008* (pp. 110–115). doi:10.1109/ISI.2008.4565039

Costello, T. (2012). Business Continuity: Beyond Disaster Recovery. *IT Professional*, *14*(5), 64–64. doi:10.1109/MITP.2012.92

Cousins, T. J. (2007). Devising Post-Disaster Continuity Plans that Meet Actual Recovery Needs. *IEEE Technology and Society Magazine*, *26*(3), 13–23. doi:10.1109/MTS.2007.906672

Dey, M. (2011). Business Continuity Planning (BCP) methodology #x2014; Essential for every business. In *2011 IEEE GCC Conference and Exhibition (GCC)* (pp. 229–232). doi:10.1109/IEEEGCC.2011.5752503

Draheim, D., & Pirinen, R. (2011). Towards Exploiting Social Software for Business Continuity Management. In *2011 22nd International Workshop on Database and Expert Systems Applications (DEXA)* (pp. 279–283). doi:10.1109/DEXA.2011.81

Elliott, D., Swartz, E., & Herbane, B. (2010). *Business Continuity Management, Second Edition: A Crisis Management Approach*. Routledge.

Fallara, P. (2004). Disaster recovery planning. *IEEE Potentials*, *22*(5), 42–44. doi:10.1109/MP.2004.1301248

Gang, C. (2009). BCM Mechanism Based on Infinite-horizon Growth Model in E-commerce. In *Second International Symposium on Electronic Commerce and Security, 2009. ISECS '09* (Vol. 1, pp. 435–438). doi:10.1109/ISECS.2009.239

Garlick, G. (2011). Improving Resilience with Community Cloud Computing. In *2011 Sixth International Conference on Availability, Reliability and Security (ARES)* (pp. 650–655). doi:10.1109/ARES.2011.100

Grimaila, M. R. (2004). Maximizing business information security's educational value. *IEEE Security Privacy*, *2*(1), 56–60. doi:10.1109/MSECP.2004.1264855

Hart, C. (2003). *Doing a literature review: releasing the social sciene research imagination*. London [etc.]: Sage.

Hayhoe, G. F. (2006). Managing in a Post-9/11, Post-Katrina World: An Introduction to Disaster-recovery Planning for Technical Communicators. In *2006 IEEE International Professional Communication Conference* (pp. 34–36). doi:10.1109/IPCC.2006.320367

Hoong, L. L., & Marthandan, G. (2011). Factors influencing the success of the disaster recovery planning process: A conceptual paper. In *2011 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1–6). doi:10.1109/ICRIIS.2011.6125683

Iyer, R. K., & Sarkis, J. (1998). Disaster recovery planning in an automated manufacturing environment. *IEEE Transactions on Engineering Management*, *45*(2), 163–175. doi:10.1109/17.669763

Jorden, E. (1999). Project prioritization and selection: the disaster scenario. In *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences, 1999. HICSS-32* (Vol. Track7, p. 7 pp.–). doi:10.1109/HICSS.1999.772779

Kolb, T. W. (2008). The Ingredients of Successful IT Management and Governance. *IT Professional*, *10*(4), 54–55. doi:10.1109/MITP.2008.93

Lamnek, S. (1995). *Qualitative Sozialforschung*. Weinheim: Beltz, Psychologie-Verl.-Union.

Lawler, C. M., Szygenda, S. A., & Thornton, M. A. (2007). Techniques for Disaster Tolerant Information Technology Systems. In *2007 1st Annual IEEE Systems Conference* (pp. 1–6). doi:10.1109/SYSTEMS.2007.374693

Liu, S., & Ormaner, J. (2009). From Ancient Fortress to Modern Cyberdefense. *IT Professional*, *11*(3), 22–29. doi:10.1109/MITP.2009.48

Madni, A. M., & Jackson, S. (2009). Towards a Conceptual Framework for Resilience Engineering. *IEEE Systems Journal*, *3*(2), 181–191. doi:10.1109/JSYST.2009.2017397

McDonald, R. (2008). New considerations for security compliance, reliability and business continuity. In *2008 IEEE Rural Electric Power Conference* (pp. B1–B1–7). doi:10.1109/REPCON.2008.4520132

Ncemane, S. N., & Weeks, R. V. (2012). Organisational Resilience in the South African services sector. In *Technology Management for Emerging Technologies (PICMET), 2012 Proceedings of PICMET '12:* (pp. 3206–3214).

Nelson, K. (2006). Examining Factors Associated with IT Disaster Preparedness. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS '06* (Vol. 8, p. 205b–205b). doi:10.1109/HICSS.2006.166

O'Callaghan, K., & Mariappanadar, S. (2008). Restoring Service after an Unplanned IT Outage. *IT Professional*, *10*(3), 40–45. doi:10.1109/MITP.2008.56

Rejeb, O., Bastide, R., Lamine, E., Marmier, F., & Pingaud, H. (2012). A model driven engineering approach for business continuity management in e-Health systems. In *2012 6th IEEE International Conference on Digital Ecosystems Technologies (DEST)* (pp. 1–7). doi:10.1109/DEST.2012.6227931

Roberts, W. C. (2006). Business Continuity Planning for Disasters is Just Good Planning. In *IEEE Military Communications Conference, 2006. MILCOM 2006* (pp. 1–5). doi:10.1109/MILCOM.2006.302086

Senda, S., Nguyen, K., & Yamada, S. (2013). Requirements for Resilient Information and Communication Technology. In *2013 Seventh International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)* (pp. 418–423). doi:10.1109/CISIS.2013.76

Shao, B. B. M. (2005). Optimal redundancy allocation for information technology disaster recovery in the network economy. *IEEE Transactions on Dependable and Secure Computing*, *2*(3), 262–267. doi:10.1109/TDSC.2005.38

Sheffi, Y. (2005). Preparing for the big one [supply chain management]. *Manufacturing Engineer*, *84*(5), 12–15. doi:10.1049/me:20050503

Tjoa, S., Jakoubi, S., Goluch, G., Kitzler, G., Goluch, S., & Quirchmayr, G. (2011). A Formal Approach Enabling Risk-Aware Business Process Modeling and Simulation. *IEEE Transactions on Services Computing*, *4*(2), 153–166. doi:10.1109/TSC.2010.17

Tjoa, S., Jakoubi, S., & Quirchmayr, G. (2008). Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modeling and Simulation Methodology. In *Third International Conference on Availability, Reliability and Security, 2008. ARES 08* (pp. 179–186). doi:10.1109/ARES.2008.206

Tsai, D.-R., & Sang, H.-A. (2010). Constructing a risk dependency-based availability model. In *2010 IEEE International Carnahan Conference on Security Technology (ICCST)* (pp. 218–220). doi:10.1109/CCST.2010.5678723

Wan, S. H. C., & Chan, Y.-H. (2008). Adoption of business continuity planning processes in IT service management. In *3rd IEEE/IFIP International Workshop on Business-driven IT Management, 2008. BDIM 2008* (pp. 21–30). doi:10.1109/BDIM.2008.4540071

Wang, K., Yin, Z., Yuan, F., & Zhou, L. (2005). A Mathematical Approach to Disaster Recovery Planning. In *First International Conference on Semantics, Knowledge and Grid, 2005. SKG '05* (pp. 46–46). doi:10.1109/SKG.2005.16

Wang, K., Zhou, L., Cai, Z., & Li, Z. (2005). A Disaster Recovery System Model in an E-government System. In *Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005. PDCAT 2005* (pp. 247–250). doi:10.1109/PDCAT.2005.6

Winkler, U., Fritzsche, M., Gilani, W., & Marshall, A. (2010). A Model-Driven Framework for Process-Centric Business Continuity Management. In *Quality of Information and Communications Technology (QUATIC), 2010 Seventh International Conference on the* (pp. 248–252). doi:10.1109/QUATIC.2010.46

Xiang, W., Wang, Y., & Zhang, Z. (2008). The Research on Business Continuity Planning of E-government Based on Information Security Risk Management. In *IEEE International Conference on Networking, Sensing and Control, 2008. ICNSC 2008* (pp. 446–450). doi:10.1109/ICNSC.2008.4525258

Zambon, E., Bolzoni, D., Etalle, S., & Salvato, M. (2007). A Model Supporting Business Continuity Auditing and Planning in Information Systems. In *Second International Conference on Internet Monitoring and Protection, 2007. ICIMP 2007* (pp. 33–33). doi:10.1109/ICIMP.2007.4

Zheng, L., Shen, C., Tang, L., Zeng, C., Li, T., Luis, S., & Chen, S.-C. (2013). Data Mining Meets the Needs of Disaster Information Management. *IEEE Transactions on Human-Machine Systems*, *43*(5), 451–464. doi:10.1109/THMS.2013.2281762