Resilient Organisations in the Cloud

By,

Lizeth Andrea Herrera Suescún

(Andrea Herrera)

A thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy in Information Systems,

The University of Auckland, 2016

Abstract

Cloud computing is a service-based computing resources sourcing model that is changing the way in which companies deploy and operate information and communication technologies (ICT). This sourcing model is reshaping the ICT services supply chain by creating a more dynamic environment with various levels of service needed and a broader range of providers offering alternative value propositions making it larger and more complex. This leads to a higher risk of disruption and brings additional organisational resilience challenges. Organisational resilience defined herein as the ability of organisations to survive and also thrive when exposed to disruptive incidents.

This thesis adopts a qualitative research design to investigate how ICT resilience activities can best be coordinated across a cloud supply chain. Based on existing supply chain resilience theories and considering specific characteristics of cloud supply chains, it proposes and empirically validates a conceptual model as a tool for guiding efforts to maintain and improve resilience in cloud supply chains. The model is based on existing supply chain management and supply chain resilience theories and identifies a set of coordination mechanism that positively impact ICT resilience processes within this chain. The empirical findings suggest the value of the model in terms of structuring the organisational resilience conversation across cloud supply chains.

Acknowledgements

First and foremost I would like to thank my supervisor Dr. Lech Janczewski. I appreciate all his contributions of time, ideas, and funding to make my Ph.D. experience productive and stimulating. Also, I would like thank my co-supervisor, Dr. Fernando Beltrán, for guiding me on this journey particularly at the very beginning. Attending conferences is an important part of an academic career and without my supervisors, I would not have been able to attend conferences in New Zealand, South Korea, Portugal, South Africa and Hawaii. During some of these conferences I met awesome people who have become great friends and colleagues.

I would also like to thank the entire faculty and staff of the ISOM department for providing all the motivational, financial and operational support required during this great learning experience, Jo I have no words except thank you!! David I wish we had had the chance to work a bit more together… Well never is too late, right? To my peers, especially Parastoo and Koti, all my gratitude. My time at the University of Auckland was very enjoyable in large part due to the people that became part of my life, Dana, the lab without you never would have been such a fun place … you inspired me in so many ways; you will be forever in my heart.

To my very close friends outside the business school, I am so grateful for the time we spent together… especially during our memorable trips. Pallis, Judith, Aleja & James, Dana and Dario if I write here how much you guys mean to me it would probably take as many pages as my thesis so I better just say thank you! To Connie & Wess, my adoptive parents! I am so lucky, I have got the best parents on this little blue planet and on top of that I got blessed with the best adoptive parents, all my love for you both! Sonia & Fernando thank you for your constant support and encouragement. You all are the best and you made New Zealand my home far away from home!

To my friends in other latitudes Nadya, Sebastián, Cami, Joha, Nenita, Marce, Marce Acosta, Yami, Adri, Jose, OLGV… Pinzón! You guys were always ready to support me when needed, without our uncountable skype chats, this journey would not have been possible. Jos, love inspires you and gives you hope… hartelijk bedankt, kus!!

Last but not least, I would like to thank my family, who has always supported me in all my pursuits, for all their love, advice, and encouragement, GRACIAS!!! Papá, Mamá, hermanito, peques (Sebastián, Pipe & Nata), Ne, Marcela, and tía Nena millones de gracias los amo profundamente! Thanks for being always there by my side. I love you guys!

THE UNIVERSITY OF AUCKLAND
SCHOOL OF GRADUATE STUDIES

Co-Authorship Form

Graduate Centre
ClockTower – East Wing
22 Princes Street, Auckland
Phone: +64 9 373 7599 ext 81321
Fax: +64 9 373 7610
Email: postgraduate@auckland.ac.nz
www.postgrad.auckland.ac.nz

This form is to accompany the submission of any PhD that contains research reported in published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work. Chapter 4: "Modelling Organizational Resilience in the Cloud" (2013). PACIS 2013 Proceedings. Paper 275. http://aisel.aisnet.org/pacis2013/275	
Nature of contribution by PhD candidate	As first author, Andrea Herrera has taken the lead in writing this article with editing done by the co-author.
Extent of contribution by PhD candidate (%)	90%

CO-AUTHORS

Name	Nature of Contribution
Lech Janczewski	10% Editing

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate’s contribution to this work, and the nature of the contribution of each of the co-authors; and
- in cases where the PhD candidate was the lead author of the work that the candidate wrote the text.

Name	Signature	Date
Lech Janczewski		30/10/2015

THE UNIVERSITY OF AUCKLAND
SCHOOL OF GRADUATE STUDIES

Co-Authorship Form

Graduate Centre
ClockTower – East Wing
22 Princes Street, Auckland
Phone: +64 9 373 7599 ext 81321
Fax: +64 9 373 7610
Email: postgraduate@auckland.ac.nz
www.postgrad.auckland.ac.nz

This form is to accompany the submission of any PhD that contains research reported in published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work.

Chapter 5: "Issues in the Study of Organisational Resilience in Cloud Computing Environments"

Procedia Technology - Volume 16, 2014, Pages 32–41. doi:10.1016/j.protcy.2014.10.065

Nature of contribution by PhD candidate	As first author, Andrea Herrera has taken the lead in writing this article with editing done by the co-author.
Extent of contribution by PhD candidate (%)	90%

CO-AUTHORS

Name	Nature of Contribution
Lech Janczewski	10% Editing

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate’s contribution to this work, and the nature of the contribution of each of the co-authors; and
- in cases where the PhD candidate was the lead author of the work that the candidate wrote the text.

Name	Signature	Date
Lech Janczewski		30/10/2015

THE UNIVERSITY OF AUCKLAND
SCHOOL OF GRADUATE STUDIES

Co-Authorship Form

Graduate Centre
ClockTower – East Wing
22 Princes Street, Auckland
Phone: +64 9 373 7599 ext 81321
Fax: +64 9 373 7610
Email: postgraduate@auckland.ac.nz
www.postgrad.auckland.ac.nz

This form is to accompany the submission of any PhD that contains research reported in published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work.

Chapter 6: "Resilient Organisations in the Cloud" (2014). ACIS 2014 Proceedings. Paper 229

http://hdl.handle.net/10292/8028

Nature of contribution by PhD candidate	As first author, Andrea Herrera has taken the lead in writing this article with editing done by the co-author.
Extent of contribution by PhD candidate (%)	85%

CO-AUTHORS

Name	Nature of Contribution
Fernando Beltran	10% Editing
Lech Janczewski	5% Editing

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- in cases where the PhD candidate was the lead author of the work that the candidate wrote the text.

Name	Signature	Date
Fernando Beltran	Fern Beltran	06/11/2015
Lech Janczewski		30/10/2015

THE UNIVERSITY OF AUCKLAND
SCHOOL OF GRADUATE STUDIES

Co-Authorship Form

Graduate Centre
ClockTower – East Wing
22 Princes Street, Auckland
Phone: +64 9 373 7599 ext 81321
Fax: +64 9 373 7610
Email: postgraduate@auckland.ac.nz
www.postgrad.auckland.ac.nz

This form is to accompany the submission of any PhD that contains research reported in published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work.

Chapter 7: "Cloud Resilience: A Supply Chain Coordination Approach" (2015). ISSA 2015 Proceedings. Paper 91. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7335076

Nature of contribution by PhD candidate	As first author, Andrea Herrera has taken the lead in writing this article with editing done by the co-author.
Extent of contribution by PhD candidate (%)	90%

CO-AUTHORS

Name	Nature of Contribution
Lech Janczewski	10% Editing

Certification by Co-Authors

The undersigned hereby certify that:

- ❖ the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- ❖ in cases where the PhD candidate was the lead author of the work that the candidate wrote the text.

Name	Signature	Date
Lech Janczewski		30/10/2015

THE UNIVERSITY OF AUCKLAND
SCHOOL OF GRADUATE STUDIES

Co-Authorship Form

Graduate Centre
ClockTower – East Wing
22 Princes Street, Auckland
Phone: +64 9 373 7599 ext 81321
Fax: +64 9 373 7610
Email: postgraduate@auckland.ac.nz
www.postgrad.auckland.ac.nz

This form is to accompany the submission of any PhD that contains research reported in published or unpublished co-authored work. **Please include one copy of this form for each co-authored work**. Completed forms should be included in all copies of your thesis submitted for examination and library deposit (including digital deposit), following your thesis Acknowledgements.

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work.

Chapter 8: Cloud Supply Chain Resilience Model: Development and Validation (2016). HICSS 2016

Proceedings. Paper 1122.

Nature of contribution by PhD candidate	As first author, Andrea Herrera has taken the lead in writing this article with editing done by the co-author.
Extent of contribution by PhD candidate (%)	90%

CO-AUTHORS

Name	Nature of Contribution
Lech Janczewski	10% Editing

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- in cases where the PhD candidate was the lead author of the work that the candidate wrote the text.

Name	Signature	Date
Lech Janczewski		30/10/2015

Table of Contents

List of Figures

List of Tables

List of Original Articles

This thesis consists of four chapters that introduce the research problem and discuss the main findings of this research, and five original articles. The original publications are listed below along with a description of the author’s contribution.

Article I

> Herrera, Andrea and Janczewski, Lech. (2013). *Modelling Organisational Resilience in the Cloud*. PACIS 2013 Proceedings. Paper 275.
> http://aisel.aisnet.org/pacis2013/275

Abstract: Cloud computing (CC) is a promising information and communication technologies (ICT) services delivery model that has already had a significant impact on Government agencies, small and medium enterprises and large organisations. Even though its adoption is moving from the early stage to mainstream, many organisations are still afraid that their resilience might deteriorate because of the additional levels of abstraction that CC introduces. This additional complexity makes the assessment of ICT operational resilience more difficult and no consensus exists of such analysis. Following a multi-method approach, this research proposal first extends prior research in the field, looking at new possible categories of resilience-oriented requirements when working in CC environments. Based on the results, this research will propose a conceptual model that helps organisations to maintain and improve Organisational Resilience (OR) when working in CC environments, from the ICT operational perspective. Particularly, as a lack of coordination has been identified as one of the main problems when facing disruptive incidents, using coordination theory, this research will identify the fundamental coordination processes involved in the proposed model. The results of this research should be of interest to academic researchers and practitioners.

Keywords: Cloud computing, ICT resilience, conceptual modelling, coordination theory

As first author, Andrea Herrera has taken the lead in writing this article with editing done by the co-author.

Article II

Herrera, Andrea and Janczewski, Lech. (2014). *Issues in the Study of Organisational Resilience in Cloud Computing Environments*. Procedia Technology, 16(0), 32-41.
doi: http://dx.doi.org/10.1016/j.protcy.2014.10.065

Abstract: Cloud computing is a promising ICT service delivery model that has already had a significant impact on government agencies, SMEs and large organisations. Even though its current adoption is moving away from the early stage to the mainstream, many organisations are still uncertain given the additional levels of abstraction that cloud environments introduce. Particularly, this additional complexity represents a hurdle in the assessment of ICT readiness for organisational resilience, and no consensus exists yet for its analysis. Based on a literature review of cloud computing reference architectures, and organisational resilience and business continuity frameworks, this paper suggests a framework to guide research into this field from an operational perspective.

Keywords: ICT services resilience; cloud computing environments; research framework; organisational resilience

As first author, Andrea Herrera has taken the lead in writing this article with editing done by the co-author.

Article III

Herrera, Andrea; Beltrán, Fernando and Janczewski, Lech. (2014). *Resilient Organisations in the Cloud*. ACIS 2014 Proceedings. Paper 229.
http://hdl.handle.net/10292/8028

Abstract: Cloud computing is a way of delivering computing resources that promises numerous benefits, however, organisations worry about its extra levels of abstraction. This additional complexity represents a hurdle in the assessment of information and communication technologies (ICT) resilience and no consensus exists yet for its analysis. Therefore, CC failures and their effects in organisational resilience (OR) need to be understood. Here, OR is defined as the ability of organisations to survive and also thrive when exposed to disruptive incidents. Aiming to find out what the requirements are for setting up and running an effective ICT operational resilience management system in cloud computing environments (CCE), a conceptual model that helps organisations to maintain and improve OR when working within CCE is being developed. This paper addresses the research design of this investigation focusing on the foundations and challenges of the conceptual model.

Keywords: Cloud computing environments, coordination theory, ICT resilience, organisational resilience

As first author, Andrea Herrera has taken the lead in writing this article with editing done by the co-authors.

Article IV

Herrera, Andrea and Janczewski, Lech. (2015). *Cloud Supply Chain Resilience: A Coordination Approach*. ISSA 2015 Proceedings. Paper 91. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7335076

Abstract: Cloud computing is a service-based computing resources sourcing model that is changing the way in which companies deploy and operate information and communication technologies (ICT). This model introduces several advantages compared with traditional environments along with typical outsourcing benefits reshaping the ICT services supply chain by creating a more dynamic ICT environment plus a broader variety of service offerings. This leads to higher risk of disruption and brings additional challenges for organisational resilience, defined herein as the ability of organisations to survive and also to thrive when exposed to disruptive incidents. This paper draws on supply chain theory and supply chain resilience concepts in order to identify a set of coordination mechanisms that positively impact ICT operational resilience processes within cloud supply chains and packages them into a conceptual model.

Keywords: Cloud computing environments; Organisational resilience; ICT operational resilience; Cloud supply chain resilience; Coordination mechanisms

As first author, Andrea Herrera has taken the lead in writing this article with editing done by the co-author.

Article V

Herrera, Andrea and Janczewski, Lech. (2016). *Cloud Supply Chain Resilience Model: Development and Validation*. HICSS 2016 Proceedings. Paper 1122. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7427674

Abstract: Cloud computing is reshaping the information and communication technology (ICT) supply chain and creating a more dynamic ICT environment. However, this transformation is accompanied by a greater risk of disruption and brings new organisational resilience (OR) challenges. Focusing on OR in relation to the cloud supply chain (CSC), this paper adopts a two-stage qualitative research design to investigate how ICT resilience activities can best be coordinated across a CSC. It proposes and empirically validates a conceptual model as a tool for guiding efforts to maintain and improve resilience in CSCs. The model is based on existing supply chain management and supply chain resilience theories and considers specific characteristics of the CSC in order to identify coordination mechanisms that positively impact ICT resilience processes within it. Empirical validation with New Zealand companies established the value of the model in terms of structuring the OR conversation across the CSC.

Keywords: Cloud supply chain resilience; Organisational resilience; ICT operational resilience; Coordination mechanisms

As first author, Andrea Herrera has taken the lead in writing this article with editing done by the co-author.

1 Introduction

Cloud computing is a service-based computing resources sourcing model that is changing the way in which companies deploy and operate information and communication technologies (ICT). Based on its potential, industry analysts have predicted a complete transformation of the computing industry. Gartner (2013), for example, expects cloud computing market to reach US$ 250 billion by 2017. The International Data Corporation (IDC) meanwhile anticipates that more than 65% of organisations will commit to hybrid cloud computing technologies before 2016 (International Data Corporation, 2014), and Forrester Research predicts that in 2016 an accelerated consolidation around three or four primary providers at the infrastructure service level will force current providers to refocus their services on niche markets (Bartoletti et al., 2016). As part of this transformation a radical reconfiguration of the ICT services supply chain is expected, with various levels of service needed and a range of providers offering alternative value propositions (Willcocks, Venters, & Whitley, 2013b), making it larger and more complex with globally dispersed components (Lindner et al., 2010).

This diverse and dynamic scenario of cloud services and a community of suppliers has raised a number of issues and more and more researchers and practitioners are investigating both the technical and business issues involved (Willcocks, Venters, & Whitley, 2013a; Yang & Tate, 2012). Effective management in the ICT services supply chain is an especially challenging task, given the threat of unexpected disruptions. Researchers and industry organisations (Armbrust et al., 2010; Cloud Security Alliance, 2011; Dekker, 2012) have therefore described cloud computing as a double-edged sword:

> On the one hand, large cloud providers can deploy state-of-the-art security and resilience measures and spread the associated costs across the customers. On the other hand, if an outage occurs the consequences could be big, affecting a lot of data, many organisations and a large number of citizens at once (Dekker, 2012, p. iii).

In other words, the special nature of a cloud supply chain creates resilience but it also increases dependencies that can cause cascading failures, and therefore there is a need to strengthen organisations' ability to not only survive but also thrive when exposed to cloud supply chain disruptive events (Arean, 2013; IBM Global Technology Services, 2014; International Data Corporation, 2014).

Such an ability is referred to in the literature as organisational resilience, which has been defined as “the ability of an organization to anticipate, prepare for, and respond and adapt to everything from minor everyday events to acute shocks and chronic or incremental changes” (British Standards Institute, 2014, p. 1). This concept recognises that organisations interact with other organisations and that therefore it is essential to build resilience in partnership with others (Morisse & Prigge, 2014), particularly when some of their processes have moved outside of their traditional boundaries, as is the case with cloud services. Despite the critical role that ICT play in organisations, and the need for novel concepts for guiding organisational resilience efforts when using new ICT sourcing models such as cloud computing (Caralli, Allen, Curtis, White, & Young, 2010b; Maurer & Lechner, 2014; Morisse & Prigge, 2014), the information systems research community’s interest in exploring how to enhance organisational resilience from an ICT operational perspective has been intermittent (Butler & Gray, 2006; Morisse & Prigge, 2014).

1.1 Motivation

Business organisations play a key role in delivering essential services that our society relies on, therefore, disruptions to their operation can have significant and widespread impacts globally. Boin and Lagadec (2000) point out that “crises are becoming more complex in nature, they are increasingly transboundary and interconnected; in a way, crises have become endemic features of modern society” (p. 185). On top of that, the number of high-risk events, both natural and man-made, has steadily increased worldwide in the past 35 years (United Nations, 2015), resulting in the need for organisations to become much more proactive in the management of their responses to such events (Bevere, Enz, Menhlhorn, & Tamura, 2012). The demand for organisations to exhibit high reliability in the face of adversity – in other words, organisational resilience – has therefore increased (McManus, Seville, Brunsdon, & Vargo, 2007).

The term *resilience* comes from the Latin word *resilire* (to leap or spring back). It refers to the ability of systems to absorb changes and persist; or the degree to which a system is capable of self-organisation (Carpenter, Walker, Anderies, & Abel, 2001; Holling, 1973; Klein, Nicholls, & Thomalla, 2003; The Resilience Alliance, 2012). Thus, being resilient to disruptive events implies focusing on capabilities and mechanisms that enable systems to successfully cope with and learn from the unexpected (Sutcliffe & Vogus, 2003). The concept of resilience has also permeated the field of management. Organisational resilience emerged in literature in the 1990s as an explanation for the ability of organisations to both survive and thrive when exposed to external shocks such as natural disasters, terrorist attacks and uncertain environments (Wilson, 2010). Specifically, resilience is identified as one of the characteristics responsible for the mindfulness that keeps high-reliability organisations working well when facing unexpected situations (Weick, Sutcliffe, & Obstfeld, 1999; Weick & Sutcliffe, 2001) and it has been identified as a key concept driving preparedness in the disaster management and crisis management literature (Kendra & Wachtendorf, 2003; Paton & Johnston, 2001; Tierney, 2003). Organisational resilience not only has been seen from the traditional approach of designing organisations that are less vulnerable to damage from hazard events but also as the ability and speed of organisations to evolve and adapt successfully to unforeseen and disruptive changing environments (Dalziell & McManus, 2004; Stephenson, 2010). From this approach organisational resilience enables organisations to gain a competitive edge by identifying gaps and taking advantage of opportunities; to be more agile and innovative by learning from trends; to reduce costs and increasing efficiency by avoiding potential pitfalls and to preserve and improve their reputation by being seen as diligent and robust (British Standards Institute, 2014).

According to van der Vegt, Essens, Wahlström, and George (2015), there are three critical sources for an organisation to become more resilient: their employees' adaptive behaviour and embeddedness in the organisation's network; their organisational structure and decision-making mechanisms; and their relationship with other organisations and environment. For the last, the authors highlight the "urgent need to find new ways of dealing with and overcoming inevitable supply chain disruptions and uncertainty" (p. 12) and the importance of coordination within and across organisations in order to effectively deal with this type of disruption. With this in mind and given the radical reconfiguration of the ICT services supply chain due to the massive adoption of the cloud computing model, this research investigates how sourcing ICT services from a cloud supply chain affects ICT resilience activities in an organisation. Accordingly, the research problem and the research objective are defined as follows:

> *Research Problem: There is a need to strengthen the ability of organisations to not only survive but also thrive when exposed to disruptive incidents within a cloud supply chain.*
>
> *Research Objective: To provide a conceptual tool for guiding efforts to maintain and improve resilience in cloud supply chains.*

Both, the research problem and the research objective, are the result of an evolutionary research process that is presented in detailed in Chapter 3 and in order to achieve this, the scope of this research is focused on the coordination mechanisms that positively impact ICT resilience activities within a cloud supply chain.

1.2 Scope

This study is bounded by the cloud supply chains and organisational resilience domains. This section first outlines cloud computing as an ICT services sourcing model and describes cloud supply chains. It then defines organisational resilience from the ICT perspective and briefly discusses the role of dependency as a key concept driving the integration of these two domains in this research.

Cloud computing is a service-based computing resources sourcing model. Many definitions exist but there is broad acceptance of the one provided by the US National Institute for Standards and Technology (NIST). In the NIST definition Mell and Grance (2011) characterise cloud computing as a “model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (p. 3). In this type of ICT services sourcing environment three main actors have been recognised (Behrendt et al., 2011; Liu et al., 2011):

- Consumers: organisations that have a relationship with, and consume a single or composite service delivered from a particular cloud provider.
- Providers: organisations responsible for making a service available to interested parties and might be directly in contact with cloud consumers.
- Brokers: entities that combine or enrich a cloud service to create a composite cloud service; they are a specific type of providers that are responsible for designing, creating, packaging, and deploying cloud services for consumer consumption.

The arrangement described above is typical of a supply chain insofar as cloud consumers obtain their services from providers who in turn depend on other providers to provide that service. Thus, a disruption to one service in a cloud supply chain immediately disrupts the interdependent services, resulting in a disruption to the overall service delivered to the cloud consumer, which could impact business services and potentially lead to organisational damage (Oppenheimer, Ganapathi, & Patterson, 2003). In fact, Lindner et al. (2010) first formally defined a cloud supply chain as “two or more parties linked by the provision of cloud services, related information and funds” (p. 3). As mentioned above, cloud computing environments are of interest to information systems researchers for both their business and technical aspects (Willcocks et al., 2013a; Yang & Tate, 2012). Until recently, however, very few information systems scholars have explored the cloud computing phenomenon as a supply chain (Fischer & Turner, 2009; ISACA, 2012; Lindner, McDonald, Conway, & Curry, 2011).

Butler and Gray (2006) argue that because ICT environments such as cloud supply chains have become more complex, highly distributed and fragile, "practitioners need conceptual tools to help them mindfully, so they can support the efforts of other to survive and thrive in complex, dynamic environments" (p. 221). This study answers that call by exploring how sourcing ICT services from a cloud supply chain impacts resilience activities in an organisation.

Organisational resilience is the other domain within the scope of this study. A widely accepted definition of organisational resilience is that it refers to "the ability of an organization to anticipate, prepare for, and respond and adapt to everything from minor everyday events to acute shocks and chronic or incremental changes" (British Standards Institute, 2014, p. 1). Organisational resilience is therefore an organisation's proficiency to not only survive but also thrive in the face of uncertainty. According to the organisational resilience literature there are two types of resilience (Dalziell & McManus, 2004). The first is engineering resilience, which involves "maximising the efficiency of systems and processes to return and maintain the system at its desired state relatively easy and rapidly" (p. 8). The second type is ecological resilience, which involves "designing flexible systems and processes that continue to function in the face of large disturbances, even though this may not maximise efficiency" (p. 8). Both types are enhanced by coordinating various operational disciplines that an organisation might already be applying, including but not limited to the following list (British Standards Institute, 2014; Cockram, 2012):

- Risk management
- Business continuity management
- Crisis and communication management
- Security management
- ICT continuity or ICT operational resilience
- Health, safety and environmental management
- Financial control

This study is positioned within the ICT operational resilience discipline. ICT operational resilience is considered an organisation's ability to improve the mission assurance of their high-value business services by preventing, detecting, responding and recovering from ICT services incidents (British Standards Institute, 2011; Caralli et al., 2010b). Managing ICT services requires a wide set of skills and competencies and usually a single organisation does not control all the activities involved in providing these types of services. Instead, these activities may be performed by external entities. The level of external dependency varies according to the specific ICT service sourcing model and these models are typically distinguished by the "location of supplier staff, the type of contract used to govern the relationship, and market differences" (Kern, Willcocks, & Lacity, 2002, p. 114). For instance, insourcing is a sourcing model where internal resources are used under internal management while cloud computing is a pay-as-you-go model where supplier-owned resources are consumed on-demand by costumers over a broad network. Ongoing management of those dependencies and relationships is critical in establishing, managing and improving ICT operational resilience (Caralli, Allen, Curtis, White, & Young, 2010a), particularly, when some processes have moved outside traditional organisational boundaries, as is the case with cloud services. Consequently, it is essential to build organisational resilience not only within organisations, but also across their supply chains. Despite this, however, a recent literature review on the topic by Morisse and Prigge (2014) shows that ICT operational resilience-related concepts have drawn limited attention from the information systems research community and most of the related concepts are studied for single organisations. In this study, theoretical concepts from the supply chain field are borrowed in order to understand how ICT operational resilience activities can be best coordinated across the cloud supply chain in order to make the supply chain more resilient.

The next section describes the research approach and introduces the research design.

1.3 Research Approach

The purpose of this section is to present the qualitative research approach used in this multi-paper thesis. First the philosophical stance taken is outlined and then a brief description of the methods used is given, including the data collection techniques and the data analysis approach.

All research is based on some underlying assumptions about what constitutes valid research and which research methods are most appropriate. According to Myers (2009), there are three main philosophical perspectives: positivist, critical, and interpretive. Positivist studies assume that reality is objectively given and can be described by measurable properties which are independent of the researcher. Positivist studies tend to test theory in an attempt to increase the predictive understanding of phenomena (Orlikowski & Baroudi, 1991). Critical researchers meanwhile assume that social reality is historically constituted and the "main task of critical research is seen as being one of social critique, whereby the restrictive and alienating conditions of the status quo are brought to light" (Myers, 2009, p. 42). Finally, interpretive studies assume that reality is accessed through social constructions and generally attempt to understand phenomena through the meanings that people assign to them (Myers, 2009). The philosophical stance of this study is interpretive. Interpretive research methods in information systems are "aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context" (Walsham, 1993, pp. 4-5).

This research looks at ICT operational resilience activities across cloud supply chains and proceeded through a number of phases (Mingers, 2001). These phases involve different activities and problems for the researcher and some research methods are more useful in some phases than in others. Accordingly, a multi-method approach was adopted following the four major phases proposed by Mingers (2001): appreciation, analysis, assessment, and action. The first phase includes methods that allow the involvement of the researcher in the situation through relevant actors and a prior literature review. Phase two includes methods to select strategies and propose an explanation of the phenomenon in terms of possible mechanisms or structures and how to improve specific weaknesses. This is followed by the third phase, which involves methods to help the researcher in interpreting the results, and their implications. The final phase involves reporting on the research findings and theoretical or practical implications (Mingers, 2001). A multi-method approach provides a nexus of diverse research fields and different research methods with the aim of gaining a richer understanding of the phenomenon under study.

Two main data-collection techniques were used in this study: semi-structured interviews that involved the use of pre-formulated questions but without strict adherence to them (McCracken, 1988); and tabletop exercises in order to analyse an emergency situation in an informal and stress-free environment (British Standards Institute, 2011; Chen, Sharman, Rao, & Upadhyaya, 2008; U.S. Department of Homeland Security, 2011). The analysis and interpretation of the data mainly involved the use of thematic analysis. This form of narrative analysis focuses in the content of the interview-generated narratives and uses prior theoretical concepts to identify and validate themes (Czarniawska, 1998; Riessman, 2008).

The next chapter and articles I, III and V provide more detailed information about the research design used in this study.

1.4 Thesis Structure

Figure 1.1 illustrates the structure of this thesis. After this introductory chapter, Chapter 2 conducts a review of the literature relating to organisational resilience and cloud supply chains. This is presented in addition to the literature reviews included in the original articles in order to provide a basic understanding of organisational resilience in cloud computing environments from an ICT perspective. This chapter also discusses the role of dependency, a key concept driving this study, and the supply chain management and supply chain resilience theories adopted by this research in order to develop the proposed conceptual model.

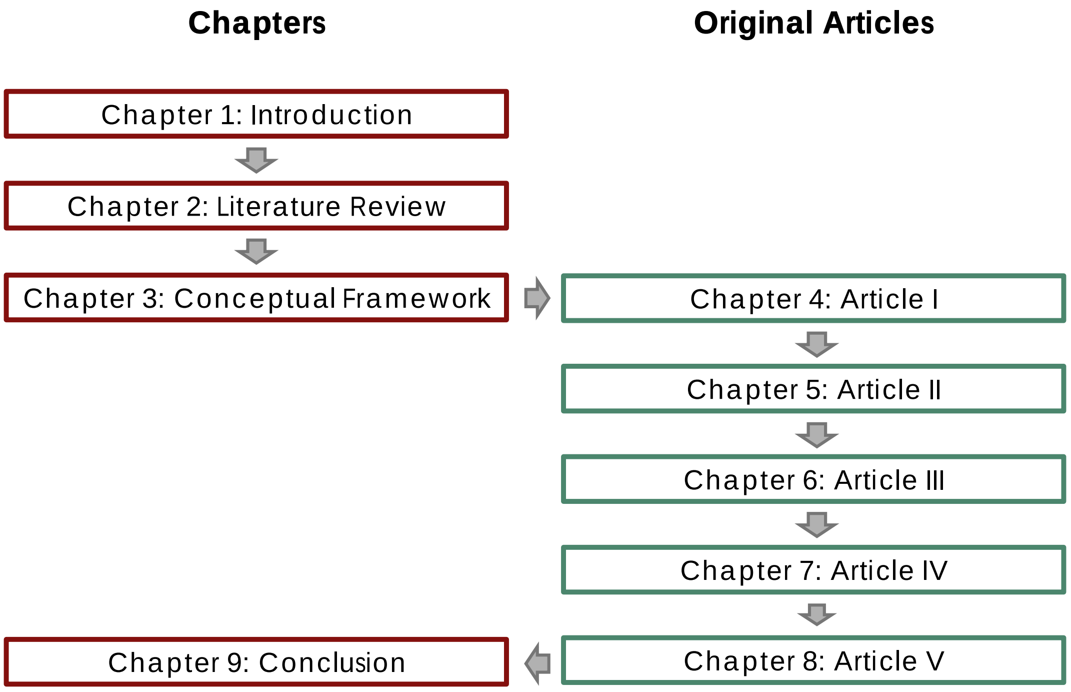


Figure 1.1: Structure of this Thesis

Chapter 3 presents an overview of the conceptual framework of this research and explains in detail how the different papers are conceptually linked and how they connect to the research questions. The theoretical approaches used in this study are also described.

Chapters 4–8 consist of the five original articles. Chapters 4 serves as an initial exploration of the organisational resilience topic in the cloud computing context by identifying the specific research problem and justifying the value of a solution. Chapter 5 develops a multi-level research framework which addresses major issues when studying organisational resilience in cloud computing environments from an ICT perspective. The framework is constructed from a literature review of cloud computing reference architectures and incorporates aspects of organisational resilience and business continuity frameworks.

Chapter 6 presents the foundations of the proposed conceptual model, the main challenges it faces, and its high-level representation. Chapter 7 further develops the model by adopting a supply chain approach and identifies the key role that coordination mechanisms play across cloud supply chain members. Chapter 8 is an empirical study that validates the proposed conceptual model's ability to capture past experience and its perceived usefulness as a tool for guiding efforts to maintain and improve resilience in cloud supply chains.

Finally, Chapter 9 summarises the findings of the research and provides an overview of the study and its main contributions to research as well as its practical implications. This Chapter closes by presenting the limitations of this study and making some suggestions for future research.

2 Literature Review

The objective of this chapter is to review the relevant literature in relation to the three main concepts guiding this research. Each of the individual articles in this thesis contains its own literature review section. Therefore the purpose of Chapter 2 is to provide a baseline understanding of organisational resilience in cloud supply chains. The literature review sections in each of the articles draws on or extends the literature presented in this Chapter. The Chapter starts by defining cloud computing as an ICT sourcing model and outlining cloud supply chains. Next, organisational resilience in the ICT operational context is discussed and the theoretical lens used in this research presented. Finally, the role of coordination mechanisms as activities that must be carried out in order to manage problems that arise from dependencies is described.

2.1 Cloud Supply Chain

Governments, organisations, and consumers are increasingly reliant on ICT products and services, and thus on the supply chains that deliver them. Over the past few years, cloud computing as an emerging ICT services sourcing model has reshaped the services-based computing resources supply chain making it larger both geographically and in the number of supply elements involved (Cadzow et al., 2015; Lindner et al., 2010). Researchers have explored the supply chain concept in the ICT services arena specifically for traditional software implementation supply chains, service-based delivery model supply chains such as application-as-a-service and, most recently, in the cloud computing context. Lindner et al. (2010, p. 3) first formally defined a cloud supply chain as “two or more parties linked by the provision of cloud services, related information and funds”. From this definition two main actors can be identified as having essential roles: cloud consumers and cloud providers. However, cloud services can be too complex for consumers to manage and increasingly consumers are requesting services from cloud brokers, instead of contacting providers directly (Behrendt et al., 2011; Lindner et al., 2010; Liu et al., 2011). This means that there are in fact three main actors, as shown in Figure 2.1:

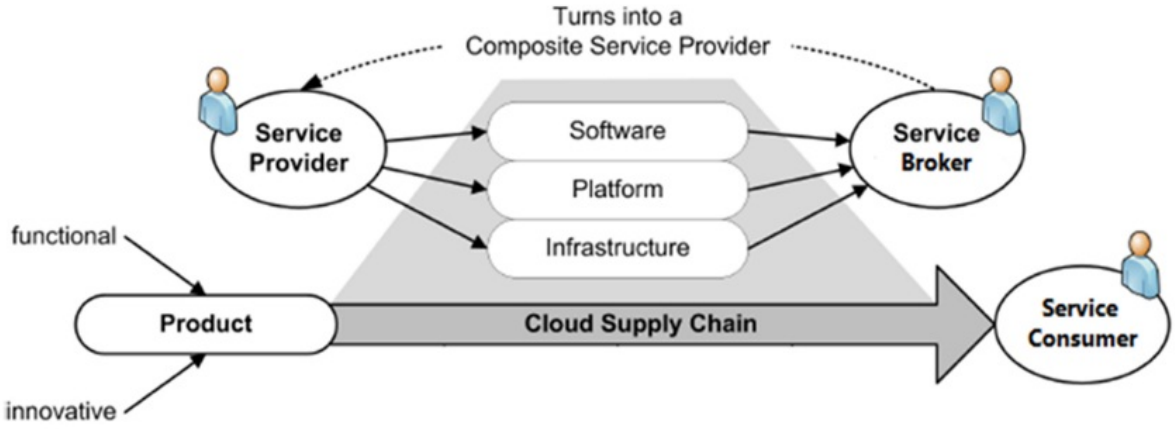


Figure 2.1: Cloud Supply Chain Definition (Lindner et al., 2010, p. 4)

- Cloud consumers are organisations that have a relationship with, and consume a single or composite service delivered from a particular cloud provider.
- Cloud providers are organisations responsible for making a service available to interested parties and might be directly in contact with cloud consumers.
- Cloud brokers are entities that combine or enrich a cloud service to create a composite cloud service; they are a specific type of provider that are responsible for designing, creating, packaging, and deploying cloud services for consumer consumption.

These three major participants interact in a highly dynamic environment. Cloud computing, as defined in the previous chapter, is a “model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance, 2011, p. 3). This ICT services sourcing model has three fundamental components: essential characteristics, service delivery models, and deployment models (Mell & Grance, 2011):

1. Essential characteristics:

    - On-demand self-service refers to the consumers’ capability to provision computing resources as needed without requiring service provider human interaction.
    - Broad network access refers to the availability of computing resources over the network via standard mechanisms that support heterogeneous client platforms.

- Resource pooling refers to the autonomous dynamic multi-consumer sharing of computing resources.
- Rapid elasticity refers to the seemingly unlimited dynamic and immediate provisioning of computing resources that scales (up or down) to the consumers demand.
- Measured service refers to the transparent provisioning, metering, and accounting of an abstraction of computing resources in accordance with a service level agreement.

These characteristics by themselves and the highly dynamic environment that results from them represent the key novelties of cloud computing compared to other ICT service-based sourcing models (Weinhardt et al., 2009; Zhang, Cheng, & Boutaba, 2010).

2. There are three service delivery models: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS):

- IaaS providers supply ICT infrastructure resources such as processing, storage, memory, and other fundamental computing resources as services for consumers to deploy their own software. Cloud providers under this layer manage the physical infrastructure and provide virtualised infrastructure while consumers are given complete ownership of the virtual image, which can configure according to their requirements.
- PaaS providers enable consumers to deploy onto the cloud infrastructure consumer-created or consumer-acquired applications by delivering programming environments, layered interfaces, and other development tools as services. Cloud providers under this layer host the hardware and software on its own infrastructure and consumers manage the deployed applications.
- SaaS providers supply a wide range of applications from productivity applications to enterprise applications that are accessible from various devices through a thin client interface. Consumers do not manage the underlying cloud infrastructure nor the individual application capabilities.

These different service offerings affect an organisation’s control over its computing resources and therefore what can be done by each of the three major participating actors. Regardless of this fact, all three actors collaboratively design, build, deploy, and operate the system (Liu et al., 2011). More importantly, all parties share the responsibilities in providing it with adequate protections.

3. There are four deployment models describing how these services can be shared:

    - Private cloud infrastructure: operates exclusively for a sole organisation.
    - Community cloud infrastructure: collectively supports organisations that have a shared affinity, concerns, or purpose.
    - Public cloud infrastructure: commercially available to the general public or a large industry group.
    - Hybrid cloud infrastructure: comprises two or more clouds (private, community, or public) and is bound together by standardised technology that enables data and application portability.

    The main difference among these deployment models relates to how exclusive the computing resources are made to a cloud consumer and these variations have potential implications as well (Liu et al., 2011). Unpredictable tenants co-existing with each other with different requirements is certainly a concern in a public cloud, however, these boundaries can be analysed in terms of the resource-pooling essential characteristic.

An ICT sourcing model with such characteristics promises to deliver numerous benefits for organisations including increased agility, shorter time to market, reduced cost, and renewed focus on the core business (Kern, Lacity, & Willcocks, 2002; Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). Attracted by these benefits, organisations are increasingly becoming party to this type of ICT services supply chain (Gartner, 2012; International Data Corporation, 2013; Ried & Kisker, 2011). However, effective management in this type of supply chain is a challenging task, especially with the threat of unexpected disruptions. Researchers and industry organisations (Armbrust et al., 2010; Cloud Security Alliance, 2011; Dekker, 2012) have therefore described cloud computing as a double-edged sword: “on the one hand, large cloud providers can deploy state-of-the-art security and resilience measures and spread the associated costs across the customers. On the other hand, if an outage occurs the consequences could be big, affecting a lot of data, many organisations and a large number of citizens at once” (Dekker, 2012, p. iii). Table 2.1 summarises the most significant cloud outages in the last two years (Kobialka, 2014; Tsidulko, 2014; Tsidulko, 2015).

Incident	Users affected	Outage time
10/08/2015:Amazon central cloud computing platform suffered major outage	Customers of Elastic Compute Cloud (EC2) and Simple Storage Service (S3)	Roughly 4 hours
20/05/2015: Several Apple services stopped working	40% of the world's 500 million iCloud users	Around 9 hours
16/03/2015: Microsoft Azure storage services outage affects users worldwide	Customers in the Central U.S of Microsoft IaaS and PaaS offerings	Roughly 11 hours
18-19/02/2015: Google Compute Engine was not reachable	Customers in multiple zones of Google's IaaS	Around 3 hours (most instances running again in 40 minutes)
14/10/2014: Google Drive slows down	More than 190 million users	Around 4 hours
10/06/2014: Hackers target Evernote	More than 100 million users	At least 10 hours
27/05/2014: Joyent's East Coast data centre fails	Customers in the East Coast zone as all compute nodes were rebooted	Between 20 and 150 minutes
16/05/2014: Internap suffers a data centre outage	About 20 customers including Livestream and StackExchange	Around 6 hours
14-15/05/2014: Adobe Creative Cloud is unavailable	Almost 4 million paid subscribers	Around 24 hours
24/03/2014: Basecamp gets attacked	About 9 million users	Roughly 2 hours
24/01/2014: Gmail gets interrupted	More than 500 million users	Less than an hour
10/01/2014: Dropbox goes down	More than 300 million people use Dropbox to share and store files	Around 3 hours

Table 2.1: Summary of Major Cloud Services Outages 2014-2015

These incidents clearly show that there is nothing inherent in a cloud supply chain that makes a cloud service 100% reliable and also highlight how important it is for an organisation to be prepared in order to survive and prosper from these outages. From the resilience perspective all three fundamental components of cloud computing raise organisational resilience concerns. However, service models and deployment models are strongly linked to a specific cloud supply chain structure. In order to explore cloud computing as an ICT sourcing model this research focuses specifically on how the essential characteristics of cloud computing services and their highly dynamic supply chains impact ICT operational resilience in an organisation.

2.2 Cloud Supply Chain Operational Resilience

As defined in the previous chapter, organisational resilience refers to "the ability of an organization to anticipate, prepare for, and respond and adapt to everything from minor everyday events to acute shocks and chronic or incremental changes" (British Standards Institute, 2014, p. 1). Consequently, the primary goal of organisational resilience is to increase the magnitude of consequences that organisations could withstand when facing disruptive events by controlling their behaviour and response during times of disruption. In other words, organisational resilience is an organisation's ability to achieve its mission consistently, especially in times of stress.

In order to make that possible, organisational resilience management "defines processes and related practices that an organization uses to design, develop, implement, and control the strategies to protect and sustain high-value services, related business processes, and associated assets" (Caralli et al., 2010b, p. 19). ICT services have become a critical enabler of many of these organisational high-value services and therefore developing, managing and adjusting ICT operational resilience processes plays a critical role in improving organisational resilience. ICT readiness for organisational resilience is defined as the ability "to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services" (British Standards Institute, 2011, p. vi). Frameworks from both industry and academia can be found in the literature describing processes to identify and specify aspects for improving an organisation's ICT operational resilience readiness in support of broader organisational resilience management. Of these, the "BS ISO/IEC 27031 Information Technology – Security Techniques – Guidelines for ICT Readiness for Business Continuity" (British Standards Institute, 2011), and the "Resilience Management Model" (Caralli et al., 2010b) encompass all types of events that could have an impact on ICT infrastructure and systems. These frameworks introduce key foundational concepts for the establishment of ICT operational resilience management activities.

According to these frameworks, an organisation needs to first identify their organisational drivers, such as their strategic objectives, risk appetite and internal/external operational constraints. These organisational drivers together with the services that are critical to the success of the organisation's mission, known as high-value services, will establish their high-level organisational resilience requirements. Therefore, an organisation's high-value services are the focus of the operational resilience management activities. There may be a number of ICT services that are considered to be critical for the provision of those high-value services, and these are known as high-value ICT services. For each ICT high-value service the current resilience capability should be reviewed from a preventive perspective to assess risks of service outages, and opportunities should also be sought to improve ICT service resilience. As a result, comprehensive management of ICT operational resilience includes both developmental and operational activities across the three stages of the organisational resilience lifecycle (Labaka, Hernantes, Rich, & Sarriegi, 2013; Standards Australia/Standards New Zealand, 2010; Witty & Morency, 2014): prevent and predict; stabilise, continue critical services, recover and manage consequences; and improvement activities:

- Preventive activities employ strategies designed to minimise a high-value service's exposure to sources of disruption by implementing proactive mechanisms that can make potentially disruptive events less frequent or severe. These activities are focused on preventing and predicting the realisation of operational risk to a high-value service.
- Continuity activities include stabilising, continuing critical functions and recovering activities. They employ strategies designed to activate contingent mechanisms once disruptive incidents commence and to keep high-value services operating as close to normal as possible during disruptive incidents. Additional strategies are aimed at returning to routine operations and a full recovery as soon as possible.
- Improvement activities employ strategies designed to achieve continual improvement by adapting and/or adopting new strategies of both previous types.

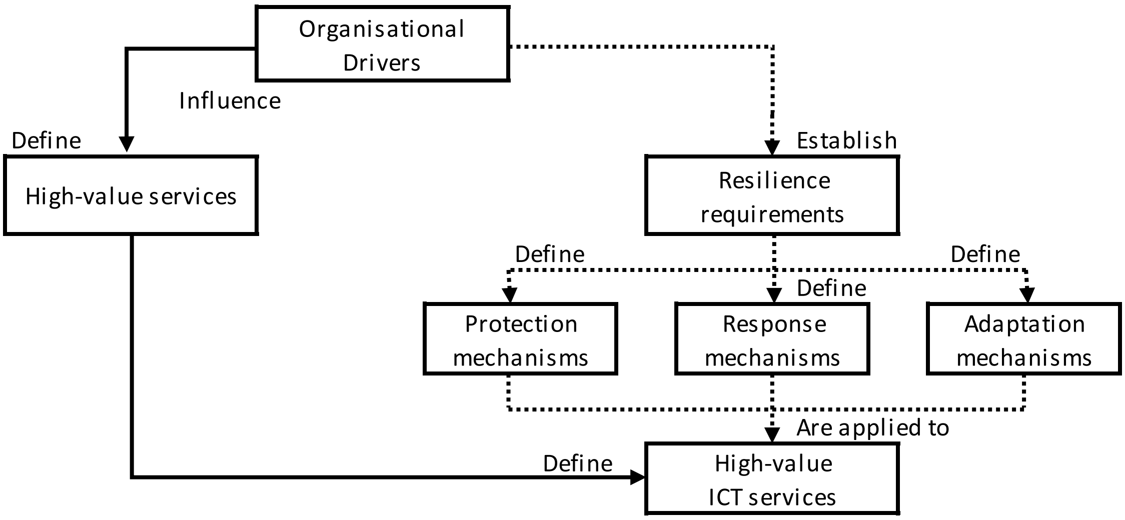


Figure 2.2: ICT Operational Resilience Foundational Concepts

In short, all resilience requirements must support the accomplishment of organisational drivers and therefore all three types of activities must be applied to the ICT services that are considered to be critical for the high-value services in order to align with the organisation needs. Figure 2.2 illustrates these foundational concepts of ICT operational resilience.

As already stated, organisations are increasingly depending on partnerships to achieve their mission. New sourcing models have emerged (Kern, Lacity, et al., 2002) and a varied range of processes have moved outside traditional organisational boundaries with the aim of increasing productivity and reducing costs. ICT products and services supply chains are not an exception to this phenomenon (Cadzow et al., 2015). In a cloud sourcing model, high-value ICT services are provided by a chain of external partners. When cloud consumers cede control over some of their ICT processes to their cloud provider, they need to rethink how to build their ICT operational resilience across their networks. However, a review of the information systems literature revealed that while disruptions and methods to maintain ICT supply chains running have received little attention (Morisse & Prigge, 2014), the need for novel concepts for ICT operational resilience management when using ICT sourcing models such as cloud computing has been recognized (Caralli et al., 2010b; Maurer & Lechner, 2014; Morisse & Prigge, 2014). From the management perspective, some resilience-related issues of cloud environments have been studied such as incident management (Cao & Zhan, 2011; Grobauer & Schreck, 2010); risk management (Dutta, Peng, & Choudhary, 2013; Kaliski Jr & Pauley, 2010; Martens & Teuteberg, 2011; Saripalli & Walters, 2010; Troshani & Wickramasinghe, 2011); high availability strategies (Shropshire, 2015); real-time monitoring (Shim & Lim, 2013; Spring, 2011a, 2011b); and the mechanisms that organisations are using to enhance organisational resilience among interorganisational ICT relationships (Järveläinen, 2012).

While the information systems research community's interest in this topic has been intermittent, an increased focus on disruptions in the supply chain literature over the last decade has led to the theorising of disruption management and its relation to supply chain resilience (Christopher & Peck, 2004; Kleindorfer & Saad, 2005; Pettit, Fiksel, & Croxton, 2010; Ponomarov & Holcomb, 2009; Sheffi, 2005; Soni, Jain, & Kumar, 2014). Supply chain resilience has been defined as "the adaptive capability of the supply chain to prepare for unexpected events, respond to disruptions, and recover from them" (Ponomarov & Holcomb, 2009, p. 131). A range of terms have been used to describe the elements that facilitate the attainment of resilience in a supply chain (Christopher & Peck, 2004; Kleindorfer & Saad, 2005; Pettit et al., 2010; Ponomarov & Holcomb, 2009; Sheffi, 2005; Soni et al., 2014). Specifically, Christopher and Peck (2004) define four principles that underpin resilience in a supply chain:

- Supply chain (re-)engineering: typically supply chains have been designed to optimise costs and customer service but are rarely designed to increase resilience. In this sense, the authors suggest that resilience should be "designed-in" to minimise, when possible, a supply chain's exposure to sources of disruption. This principle is enhanced by having a good understanding of the supply chain network, analysing multi-sourcing supplier environments and/or single supplier environments with multiple sites, and applying re-engineering practices to continuously improve resilience. Other authors have recognised the following factors as resilience enablers: knowing the supply chain structure (Soni et al., 2014); allowing for flexible and redundant strategies (Sheffi, 2005; Soni et al., 2014); and organisational learning (Pettit et al., 2010; Ponomarov & Holcomb, 2009; Sheffi, 2005; Soni et al., 2014). Thus, this principle focuses on understanding the supply chain structure, designing alternatives to meet expected levels of resilience, and leveraging knowledge in order to become more resilient.
- Supply chain collaboration: all the studies reviewed agree that a high level of collaboration across a supply chain makes that chain significantly more resilient. The challenge is to create conditions for sharing information and working collaboratively. Christopher and Peck (2004) affirm that even though there is no history of such sharing, organisations within a supply chain are moving to adopt closer relationships with each other, and point out the potential of supply chain event management in this regard. The focus of this principle then

is to develop a common language and to provide effective communication channels in order to keep supply chain members' efforts aligned.

- Creating a supply chain risk management culture: supply chain risks represent the most serious threat to supply chain resilience, therefore Christopher and Peck (2004) affirm that the only way to build supply chain resilience is by creating a risk management culture within supply chain members. Risk sharing requires continuous risk analysis, assessment and report. Even though all the reviewed studies recognise the role of risk management in achieving supply chain resilience, only two explicitly agree on this principle (Pettit et al., 2010; Soni et al., 2014). Thus, this principle focuses on identifying and analysing vulnerabilities by collecting information about risk-control activities across the chain, assessing their effectiveness and ensuring their enforcement.
- Agility: according to Christopher (2004), "one of the most powerful ways of achieving resilience in the supply chain is to create networks which are capable of more rapid response to changed conditions" (p. 19). This principle refers to both the individual members within the supply chain and the supply chain itself. Two key components have been identified: visibility and velocity. Visibility highlights the importance of knowing the conditions and the standard practices within the supply chain while velocity relates to constantly monitoring how rapidly the supply chain can react to changes. Of the studies reviewed for this research, the only one that does not refer explicitly to this principle is Ponomarov and Holcomb (2009). The focus of this principle then is to establish a clear understanding of the environment and the necessary mechanisms to monitor it in order to identify and respond to changed conditions.

This research applied the above theoretical concepts relating to supply chain resilience to the specific features and challenges of cloud supply chains in order to explore how ICT resilience activities can best be coordinated to make this supply chain more resilient. The final key concept driving this investigation is the notion of dependency, and the next section demonstrates how the theoretical foundations of this concept advanced in the literature can also be applied to cloud supply chain resilience.

2.3 Coordination Literature

Dependencies constrain how tasks can be performed and problems that arise from dependencies are referred to in the literature as coordination problems. In fact, Malone and Crowston (1994) define coordination as managing dependencies. Coordination has long been considered important for managing dependencies within organisations to achieve desired outcomes and the literature is replete with findings about effective mechanisms for coordinating these dependencies (Argote, 1982; Galbraith, 1973; March & Simon, 1958; Mintzberg, 1980; Thompson, 1967; Van de Ven, Delbecq, & Koenig Jr, 1976). Malone and Crowston (1994) and Crowston and Osborn (2003) propose coordination theory as a framework for analysing complex processes in terms of actors performing interdependent activities. This theory identifies two types of activities within a process: “activities that directly contribute to the output of the process” (Simatupang, Victoria Sandroto, & Hari Lubis, 2004, p. 257) and coordination mechanisms, which are additional activities that must be carried out in order to manage dependencies among the first type of activities.

Coordination mechanisms are actions taken for accomplishing a goal that is constituted of interdependent tasks taken by multiple actors (Jarzabkowski, Lê, & Feldman, 2012). These mechanisms may be specific, such as “incident detection and reporting procedures” or general, such as organisational policies (Crowston, 1994). In their review of the literature, Okhuysen and Bechky (2009) recognise that despite the variation due to different approaches and focal interests, the main role of coordination mechanisms is to integrate parties working collectively on interdependent organisational activities in order to achieve collective organisational goals. Prior literature exhibits a clear interest in specifying the standards, rules, schedules and procedures that comprise coordination mechanisms (Okhuysen & Bechky, 2009; Sabherwal, 2003; van Fenema, Pentland, & Kumar, 2004), however, researchers have long noted that these mechanisms are not stable entities and the following essential features have been identified:

- It has been recognised that coordination mechanisms are not a single way to organise but rather have to adapt to the interdependent work of actors (Jarzabkowski et al., 2012). In other words, coordination in organisations is an ongoing accomplishment and consequently coordination mechanisms need to be flexible and dynamic enough to cope with uncertainty and complexity (Malone et al., 1999). Faraj and Xiao (2006) accordingly define coordination as “a temporally unfolding and contextualized process of input regulation and articulation to realize a collective performance” (p. 1157).
- Coordination mechanisms also have to adapt to non-routine conditions. When a disruptive event occurs, it creates obstacles for parties to accomplish their task and it is important to distinguish between circumstances in order to decide on the appropriate coordination mechanisms to adopt. All organisations face times of pressure and it would be “naïve to

assume that the enactment of coordination practices will remain the same under different operating conditions" (Houtman, Kotlarsky, & Van den Hooff, 2014, p. 2).

- Researchers have also suggested that in order to meet new demands for flexibility and uncertainty organisations have shifted the nature and location of their task boundaries. In this context, Kellogg, Orlikowski, and Yates (2006) studied how members of organisations perform coordination work in conditions where operations are fast-changing; goods and services are intangible and informational; authority is distributed; and accountability is uncertain. The authors conclude that in cross-boundary coordination, the construction of shared knowledge and the use of various boundary-spanning mechanisms such as routines, languages, repositories and models play essential roles.

In addition, even though most of the research studying coordination issues and coordination mechanisms has been focused on how or why coordination occurs within a single organisation, coordination with external organisations has become increasingly important for achieving desired performance outcomes. This topic has received growing attention in the management literature as a result of the increased degree of organisations' vertical disintegration, particularly on a cross-border basis, in order to remain competitive (Gilson, Sabel, & Scott, 2009) and that growing interest is also shown in the information systems literature (Gittell & Weiss, 2004; Gosain, Malhotra, & El Sawy, 2004; Legner & Schemm, 2008; Nurmi, 2009; Tan & Sia, 2006). Researchers have also recognised that as a result of this dynamic environment traditional mechanisms are often "insufficient for coordinating the resulting interdependencies among organisations, thus requiring more explicit attention to the design of mechanisms for managing inter-organizational relationships" (Gittell & Weiss, 2004, p. 127).

A cloud supply chain requires extensive coordination to connect all the elements of a service across its different members in order to deliver it consistently to the customer, especially in times of disruption. The above literature review reveals that in order to address the unique characteristics of cloud services and their impact on organisational resilience more research on specific coordination mechanisms that enhance the four supply chain principles of (re-) engineering, collaboration, risk management culture and agility, is required. In order to analyse the ways in which coordination is accomplished and how coordination mechanisms adapt to non-routine conditions in this type of supply chain, distinctions between the three stages of the organisational resilience lifecycle – preventive, continuity and improvement – need to be made. Accordingly, this study builds on previous supply chain resilience work focusing on how ICT operational resilience activities can best be coordinated across the cloud supply chain in order to make this supply chain become more resilient.

The previous chapter has provided a literature review of the three main concepts guiding this research. As this thesis consists of five original articles, the next section presents the conceptual framework connecting all five articles together.

3 Conceptual Framework

This chapter describes the conceptual framework of the research reported in this thesis and presents the research questions. According to Miles and Huberman (1994), a conceptual framework "explains, either graphically or in narrative form, the main things to be studied—the key factors, constructs or variables—and the presumed relationships between them" (p. 18). In other words, a conceptual framework is "the researcher's representation of the conceptual structure brought to the research process" (Carroll & Swatman, 2000, p. 237), therefore, the conceptual framework presented here provides an overview of how the five original publications that are part of this thesis are linked and how they fit into the "bigger picture" of the research problem.

Figure 3.1 diagrammatically represents the conceptual framework used in this study. Reflecting the process approach (Mingers, 2001) described in Chapter I, the framework consists of three main stages: Exploration, Analysis, and Validation. The figure also shows the data collection approach for each stage. The Exploration stage identifies the specific research problem and involves understanding the particular phenomenon which is under investigation within the research problem context. This stage also defines the main expected outcome of the research: a conceptual model that can be used as a tool for guiding efforts to maintain and improve organisational resilience within cloud environments. The Analysis stage identifies essential aspects of the conceptual model in order to define a sound baseline, and refines this baseline based on experts' opinions. It then further develops the model. The final stage, Validation, involves an empirical test of the proposed model.

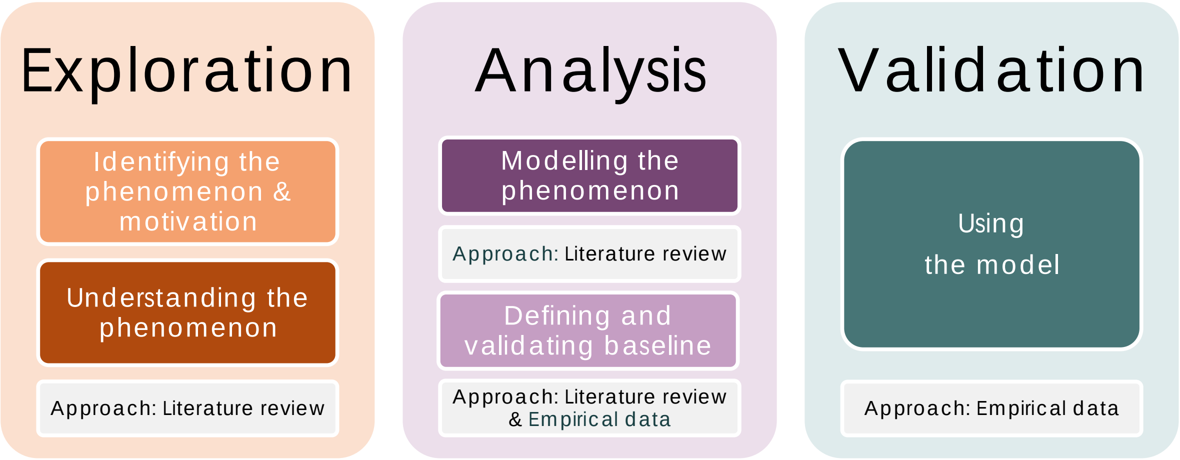

Exploration
Identifying the phenomenon & motivation
Understanding the phenomenon
Approach: Literature review
Analysis
Modelling the phenomenon
Approach: Literature review
Defining and validating baseline
Approach: Literature review & Empirical data
Validation
Using the model
Approach: Empirical data

Figure 3.1: Conceptual Framework

This research takes a sequential cumulative approach, with each stage building on the previous stages' insights and findings including feedback from the research community. The associated findings were reported to relevant audiences through five publications and the feedback gathered from the reviewers' comments was incorporated in the subsequent stage of the research. In the following sections the framework is deconstructed to explain each of its components.

3.1 Stage 1: Exploration

This research began with the objective of understanding how the introduction of cloud computing environments as an ICT services sourcing model impacts business continuity activities in an organisation. In this early stage, only one assumption was made: that despite all the hype about cloud computing environments, this type of sourcing model is not infallible. In other words, even the most reputable cloud services can malfunction ("go down") and therefore it is crucial that organisations providing and consuming cloud services are prepared for system failures. This objective and associated assumption reflect the explicit interest of the researcher in exploring the topic of business continuity in cloud computing environments from an ICT readiness perspective.

The Exploration stage was divided into two parts in order to define the research problem and specific phenomenon of interest, and gain an understanding of the latter. The following subsections describe the main activities of this stage.

3.1.1 Identifying the phenomenon and motivation

The aim of the Exploration stage was to explore and understand the current research landscape concerning the topic of business continuity preparedness in cloud computing environments, and to some extent validate its relevance as a research topic. Business continuity management encompasses incident preparedness, disaster recovery planning, and emergency response management (International Organization for Standardization, 2012). It has been defined as a "holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience" (International Organization for Standardization, 2012, p. 2). In accordance with this definition, building organisational resilience in cloud computing environments became the focus of this research and the motivation driving the initial exploration of this topic was to identify how the adoption of cloud computing as an ICT services sourcing model affects the ability of an organisation to survive and thrive when exposed to cloud services disruptive incidents.

To gain an understanding of the topic, a literature review approach was chosen that concentrated on two specific subjects: cloud computing as an ICT services sourcing model; and organisational resilience, particularly in the ICT context. In the former, several academic and practitioner association publications were identified from targeted searches and analysed, with a focus on those describing the fundamental components and benefits of cloud computing as well as the barriers to its adoption. In the latter, academic publications and several industry standards were reviewed. This analysis revealed that while the need for organisations to exhibit high reliability in the face of adversity has increased and the key role of ICT resilience is well recognised, disruptions and mechanisms to keep businesses running in ICT-based interorganisational environments – such as cloud computing – have not been greatly studied. However, the need for novel concepts in this topic has been recognised (Caralli et al., 2010b; Maurer & Lechner, 2014; Morisse & Prigge, 2014). These findings supported the research topic and led to the research problem being defined as:

> *Research Problem: There is a need to strengthen the ability of organisations to not only survive but also thrive when exposed to disruptive incidents within a cloud environment.*

During this stage, the researcher became aware of the importance of building organisational resilience in partnership with others, particularly when some processes have moved outside of the traditional organisational boundaries as is the case with cloud services. At this point the notion of dependency arose as a key concept. Problems that result from dependency are referred in the literature as coordination problems; in fact, Malone and Crowston (1994) define coordination as managing dependencies. Malone and Crowston (1994) and Crowston and Osborn (2003) propose coordination theory as a framework for analysing complex processes in terms of actors performing interdependent activities. In this research, the coordination concept was used as a “sensitising device” which allows the researchers to view the research problem in a particular way (Klein & Myers, 1999). This concept was used both to guide the initial research design and as part of the iterative process of data collection and analysis (Walsham, 1995).

This initial exploration of the state of the problem and the importance of its solution led to the defining of the main objective of this research:

> *Research Objective: To provide a conceptual tool for guiding efforts to maintain and improve resilience within a cloud environment.*

Additional findings and insights concerning this stage are presented in Article I.

3.1.2 Understanding the phenomenon

The next part of the Exploration stage was to set the boundaries for, and scope of, the rest of this research. Initially, an exploratory empirical study was proposed in order to identify the main issues that organisations consuming cloud services face when handling disruptive incidents and the types of mechanisms being used by these organisations to prepare, respond and learn from these events. However, after a preliminary assessment of the research design described in Article I, a different approach was chosen. Before exploring how organisations are changing their ICT resilience activities as a result of adopting cloud computing as an ICT services sourcing model, a conceptual understanding of the phenomenon was needed as there has been little research in this area.

Previous research has established sets of organisational resilience requirements and specific operational processes in the ICT context. However, most of the information systems literature applies ICT organisational resilience concepts to a single organisation only (Morisse & Prigge, 2014) and assumes that ICT services are mainly provided in-house. Cloud services have some important characteristics that make them quite different to in-house ICT services. It is therefore apparent that further understanding of how the elements involved in a cloud computing environment impact the existing ICT resilience processes, was needed. To address this need, Article II presents a research framework designed to provide a roadmap for researchers exploring the area of ICT resilience in cloud computing environments.

To gain the necessary conceptual understanding of the phenomenon a literature review approach was chosen. From this review a cloud baseline architecture founded on three dimensions – principles, actors, and architecture building blocks – was compiled (Behrendt et al., 2011; Cisco Systems, 2011; Cloud Security Alliance, 2013; Khasnabish et al., 2013; Liu et al., 2011; Liu, Zhang, Hu, & He, 2012; Oracle Corporation, 2012). Then a set of specifications divided on the stages of the organisational resilience lifecycle– preventive, continuity, and improvement – was derived from the most popular organisational resilience standards and models (American National Standards Institute, 2009; International Organization for Standardization, 2012; National Fire Protection Association, 2004; Standards

Australia/Standards New Zealand, 2010) and a set of 26 ICT process areas (Caralli et al., 2010b) was compiled. This led to the development of the first research question:

> *Research Question 1: How do the main reference architecture characteristics of cloud computing environments affect the ICT operational resilience requirements?*

The key contribution of this stage was the development of a multi-level research framework to identify major differences in studying ICT operational resilience between cloud computing environments and in-house environments. This framework captures key issues from the macro level of cloud computing's architectural building blocks to the micro level of organisational resilience capabilities. At the macro level it aims to bridge current ICT resilience processes and high-level cloud service components and at the micro level it is designed to analyse linkages among resilience process areas in order to identify dependencies that should be considered when conducting a comprehensive study of a specific process area. The research framework was published as Article II.

3.2 Stage 2: Analysis

After gaining a conceptual understanding of the research areas under investigation, the researcher realised that the proposed conceptual model needed to address a set of specific issues presented in the research framework. Accordingly, this stage was divided into two parts: definition and validation of a sound baseline for the model; and development of the model. This led to the development of the second research question:

> *Research Question 2: How should the existing processes and mechanisms be adjusted? What new processes and mechanism should be created?*

The following subsections describe the main activities of this stage.

3.2.1 Defining baseline

Having defined the development of a conceptual model as the main outcome of this research, the researcher set about defining a sound baseline as the starting point of its development. In line with the definition of Wand and Weber (2002) a conceptual model as "a representation of selected phenomena in some domain" (p. 363), the proposed conceptual model is a representation of how ICT operational resilience activities in an organisation are impacted by consuming cloud services. Based on the research framework and on an extensive relevant literature review, three essential elements were identified as part of the model's baseline: four foundations on which the model is developed; specific organisational resilience challenges that the model addresses; and its high-level representation. This analysis resulted in the definition of the baseline that was published as Article III. Particularly, the four foundations on which the baseline is set up are presented below:

- F1: Designing flexible processes to not only maintain and return to the desired state but also to continue to function in the face of disturbance (Dalziell & McManus, 2004).
- F2: Analysing how cloud characteristics affect the three distinct sets of organisational resilience activities: preventive, continuity and improvement (British Standards Institute, 2014).
- F3: Managing dependencies as all parties share responsibility in providing the environment with adequate protections (Herrera & Janczewski, 2014).
- F4: Determining the coordination mechanisms for ICT resilience processes highly impacted by cloud adoption (Caralli et al., 2010b; Herrera & Janczewski, 2014).

Finally, given the importance of this baseline for the research and due to the limited academic literature on the topic, the researcher considered that at this early stage experts' opinions would be of significant value (Linstone & Turoff, 2002) and a preliminary assessment by a group of domain experts was designed. Primary data from semi-structured interviews with 10 experts with an average of 10+ years of experience in organisational resilience and ICT service management were collected in order to validate this baseline focusing on the model's foundations. The interview questions were composed (see Appendix 1 for the Interview Protocol) and participants were recruited from among members of special interest groups such as the New Zealand Information Security Forum, the IT Disaster Recovery and Service Continuity Professionals group, and the Cloud Security Alliance and selected based on their expertise in both the organisational resilience and the ICT domains. Each interview lasted approximately 45–60 minutes, was audio recorded and followed guidelines by McCracken (1988). An overview of the study was given at the start of each interview and then the interviewee was asked open-ended questions from an organisational resilience perspective that were structured around three main categories: (1) the main changes introduced by consuming cloud services; (2) the main challenges of managing dependencies in a cloud environment; and (3) the main mechanisms used to coordinate efforts among all involved parties.

The main findings and insights of this assessment are presented in the first section of Article V, “Initial Conceptualisation Validation”. Overall, three foundations were accepted but a key concern regarding F4 was raised, which led to a change in the focus from organisational resilience activities in themselves to how members of a cloud supply chain can coordinate their activities to increase resilience. The analysis of the interviews showed that the problem under study is perceived and framed in practice from a supply chain perspective. Almost all the interviewees stated that it would be more beneficial to analyse how organisational resilience activities can best be coordinated across cloud supply chains rather than identifying new activities or changes in specific activities derived from sourcing ICT services from a cloud (F4). This analysis was added to the feedback gathered from Article III and resulted in a supply chain approach being adopted to further develop the model.

In addition to the baseline itself, the most important outcome of the first part of this stage was the critical reflection on the adopted approach and the evolution of the theoretical perspective of this research accordingly.

3.2.2 Modelling the phenomenon

After the critical reflection in the previous step and before further development of the model, an additional literature review was conducted in order to reframe the research problem using a supply chain approach. Accordingly, the research problem and the main objective were reworded as:

> *Research Problem: There is a need to strengthen the ability of organisations to not only survive but also thrive when exposed to disruptive incidents within a cloud supply chain.*

> *Research Objective: To provide a conceptual tool for guiding efforts to maintain and improve resilience in cloud supply chains.*

And the second research question became:

> *Research Question 2: How can ICT resilience activities best be coordinated across the cloud supply chain in order to make this supply chain become more resilient?*

As mentioned earlier, this research developed cumulatively with each stage being informed by the findings and analysis of the previous ones. Building on the insights from earlier stages of the research and findings from previous research on supply chain resilience (Christopher &

Peck, 2004; Kleindorfer & Saad, 2005; Pettit et al., 2010; Ponomarov & Holcomb, 2009; Sheffi, 2005; Soni et al., 2014) and supply chain coordination mechanisms (Simatupang et al., 2004; Xu & Beamon, 2006), a set of coordination mechanisms that positively impacts ICT operational resilience processes across cloud supply chains was identified. These categories of mechanisms were packaged into the conceptual model. This model represents the key contribution of this research and is the first step towards gaining a conceptual understanding of the studied phenomenon. The model and additional findings and insights of this stage have been published as Article IV.

3.3 Stage 3: Validation

The final logical step was to empirically validate the model and this was the purpose of the third stage of the conceptual framework. An empirical analysis of coordination mechanisms in cloud supply chains was outlined and this led to the development of the third and fourth research questions:

> *Research Question 3: Is the model able to capture the richness of a real cloud incident?*
>
> *Research Question 4: Is the model perceived as a useful tool for guiding efforts in maintaining and improving cloud supply chain resilience?*

For this study, the unit of analysis was a cloud incident across the three stages of the resilience life cycle: preventive, continuity, and improvement (British Standards Institute, 2014). Major players in different cloud supply chains in the New Zealand cloud services market were contacted and data from six incidents were collected using two methods. Interviewees were senior employees, at least two from each firm where possible, with ICT backgrounds and experience in incident response. First, data about the incident were collected through semi-structured interviews (see Appendix 2 for the Interview Protocol). All the incidents were documented in terms of the model and the relevant literature was used as a secondary source for the analysis. All the incident interpretations were presented, discussed, and refined when necessary (see Appendix 3 for Incident Summary Sheets). Then simple tabletop exercises (U.S. Department of Homeland Security, 2011) based on the studied scenarios were conducted in order to identify additional mechanisms that could positively impact their cloud supply chain resilience (see Appendix 3 for Incident Summary Sheets). The analysis and discussion of the findings of this study have been published as Article V.

The next section explains how the five publications fit into the conceptual framework.

3.4 How the Publications Fit within the Conceptual Framework

In the preceding sections the conceptual framework applied to this research was presented. It is also necessary to discuss how each of the original articles published as part of this thesis fit within the conceptual framework. This is shown in Figure 3.2 below.

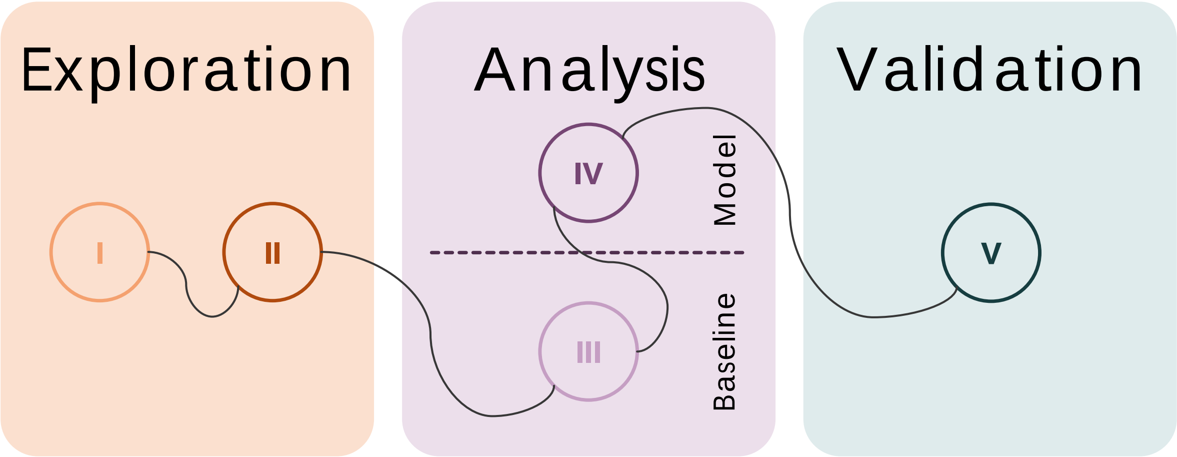


Figure 3.2: Conceptual Framework showing how the Original Publications are connected

Article I, “Modelling Organizational Resilience in the Cloud”, was published in the proceedings of the 2013 Pacific Asia Conference on Information Systems (PACIS 2013) and explores the state of the research problem and the importance of its solution; it also defined a preliminary research approach. Article II, “Issues in the Study of Organisational Resilience in Cloud Computing Environments”, was published in the proceedings of the 2014 Conference on ENTERprise Information Systems (CENTERIS 2014) and conceptualises ICT operational resilience in cloud computing environments. Article III, “Resilient Organisations in the Cloud”, was published in the proceedings of the 2014 Australasian Conference on Information Systems (ACIS 2014) and addresses the research design of this investigation, focusing on the foundations and challenges of the conceptual model. Article IV, “Cloud Supply Chain Resilience: A Coordination Approach” was published in the proceedings of the 2015 International Information Security South Africa Conference (ISSA 2015) and identifies a set of coordination mechanisms that positively impact ICT operational resilience processes within cloud supply chains and packages them into a conceptual model. Finally, Article V, “Cloud Supply Chain Resilience Model: Development and Validation”, was published in the proceedings of the 2016 Hawaii International Conference on System Sciences (HICSS 2016) and empirically validates the model with New Zealand companies, thereby establishing its value. Chapters 4 to 8 are exact copies of these five original articles; only figure numbers and table numbers have been modified in order to be consistent with the structure of this document.

Crucially, these articles also show how the theoretical perspective of this research evolved over time in the process of discovering an effective solution to the research problem. They also demonstrate the importance of reporting and disseminating the research results to both practitioner-oriented and scholar-oriented audiences in order to continuously validate the research's relevance and rigor. Figure 3.3 illustrates how the articles align with the conceptual framework and lists their contributions.

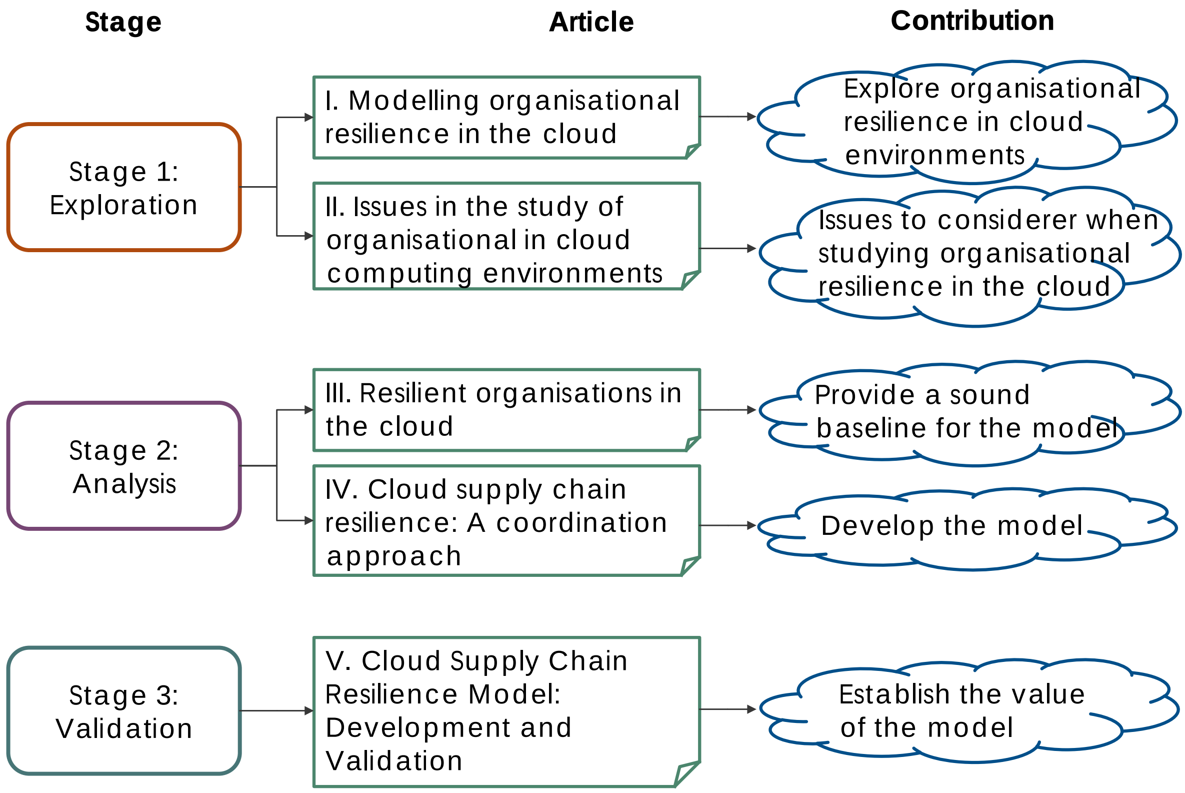

Stage
Article
Contribution
Stage 1: Exploration
I. Modelling organisational resilience in the cloud
Explore organisational resilience in cloud environments
II. Issues in the study of organisational in cloud computing environments
Issues to considerer when studying organisational resilience in the cloud
Stage 2: Analysis
III. Resilient organisations in the cloud
Provide a sound baseline for the model
IV. Cloud supply chain resilience: A coordination approach
Develop the model
Stage 3: Validation
V. Cloud Supply Chain Resilience Model: Development and Validation
Establish the value of the model

Figure 3.3: Stages, Articles and their Contributions

What follows are the published articles that together address the discussed research problem.

4 Modelling Organisational Resilience in the Cloud

Cloud computing (CC) is a promising information and communication technologies (ICT) services delivery model that has already had a significant impact on Government agencies, small and medium enterprises and large organisations. Even though its adoption is moving from the early stage to mainstream, many organisations are still afraid that their resilience might deteriorate because of the additional levels of abstraction that CC introduces. This additional complexity makes the assessment of ICT operational resilience more difficult and no consensus exists of such analysis. Following a multi-method approach, this research proposal first extends prior research in the field, looking at new possible categories of resilience-oriented requirements when working in CC environments. Based on the results, this research will propose a conceptual model that helps organisations to maintain and improve Organisational Resilience (OR) when working in CC environments, from the ICT operational perspective. Particularly, as a lack of coordination has been identified as one of the main problems when facing disruptive incidents, using coordination theory, this research will identify the fundamental coordination processes involved in the proposed model. The results of this research should be of interest to academic researchers and practitioners.

4.1 Introduction

Cloud computing is a new paradigm that promises uncountable benefits for organisations including agility, reduced time to market, reduced cost and renewed focus on the core business. According to IDC[1], regardless of their specific motivation, organisations are increasingly turning to this type of service; in fact, it has been predicted that by 2016, US $1 of every US $5 will be spent on cloud-based software and infrastructure (Mahowald & Sullivan, 2012). However, like every new trend, CC also has risks and concerns that are being identified in order to use it effectively and safely. An increasing number of researchers and practitioners worldwide are developing new knowledge about CC in a wide range of applications from the business perspective to more technical issues (Yang & Tate, 2012). In the former, researchers have been working specifically on economic impact, costs, reasons for its adoption, and growth trends (Centre for Economics and Business Research ltd, 2011; Iansiti & Richards, 2011; Marston et al., 2011; Saya, Pee, & Kankanhalli, 2010). In the latter, issues regarding portability,

[1] International Data Corporation is a market research specialized in information technology.

interoperability and security have been studied (Buyya, Ranjan, & Calheiros, 2010; Catteddu & Hogben, 2009; Chen, Paxson, & Katz, 2010; Cloud Security Alliance, 2010).

Somewhere in the intersection between these technical and business concerns, many researchers and renowned international organisations and associations have identified *Availability / Business Continuity* as one of the main obstacles to and opportunities for the growth of CC (Armbrust et al., 2010; Badger, Grance, Patt-Corner, & Voas, 2012; Catteddu & Hogben, 2009; Cloud Security Alliance, 2011; Hancock & Hutley, 2012). Business continuity and disaster recovery plans become even more important in cloud environments because cloud outages and cloud security compromises are some of the many additional issues that can lead to an operational disruption. Thus, if things go wrong, a joint effort between the cloud provider and the organisation that requires high levels of coordination, is needed in order to avoid unacceptable downtimes (Toomer, 2011).

According to the International Organization for Standardization (ISO), Business Continuity Management (BCM) is an "holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which *provides a framework for building organizational resilience* (…)" (2012, p. 2). Then, the final objective of BCM is to build Organisational Resilience (OR). In fact, this concept has gained considerable attention in the last few years, mainly because organisations are the engine of economic growth and sustainable development and disruptions can have significant and widespread impacts globally (Boin & Lagadec, 2000). On top of that, the annual number of both natural and man-made disasters has increased significantly during the past 20 years. As a consequence, the need for organisations to exhibit high reliability in the face of adversity has increased and in order to build and improve OR a deep understanding of the information and communication technologies (ICT) environment is essential. These two factors, the massive adoption of CC as a model for performing ICT functions and the growing relevance of the OR concept, have highlighted the need to strengthen the ability of organisations to respond to disruptive incidents when working in cloud environments.

Based on these facts, this research aims, firstly, to understand how the adoption of CC impacts the ability of an organisation to continue to function in the face of disruption, in order to identify new categories of resilience-oriented requirements when working in CC environments. Secondly, using these results and the analysis of the CC reference architecture (Liu et al., 2011) the main purpose of this research is to propose a conceptual model that helps organisations to maintain and improve OR when working in CC environments, from the ICT operational perspective. In addition, as lack of coordination has been identified as one of the main problems when facing disruptive incidents (Hossain & Kuti, 2010) using coordination theory (Malone & Crowston, 1994), this research will identify the fundamental coordination processes involved in the proposed model. The assessment of these two artefacts will be performed through the experts' opinions approach, and walkthrough and tabletop exercises. Finally, the proposed artefacts will be used to analyse one of the current ICT resilience standards in order to identifying possible gaps and make some suggestions to respond to the new CC requirements. It is expected that the designed artefacts will integrate the foundational and practical requirements of ICT operational resilience in CC environments and could be used for planning and decision making to anticipate, prevent, prepare for, and respond to ICT disruptive incidents.

4.2 Literature Review and Research Questions

In seeking to understand the impact of CC adoption in OR, firstly this section gives a brief description of CC and its main characteristics. Secondly, it presents a broad overview related to the resilience concept focusing on OR and how coordination among individuals, ICT services and organisations is an essential process especially when responding to disruptive incidents. Thirdly, it gives an overview of some well cited studies conducted in the OR field, specifically in the ICT domain and lastly, it presents the primary research questions for this research.

4.2.1 Cloud computing as an ICT performing functions model

CC is a type of computing services sourcing model. There are many definitions but there is broad acceptance of the one provided by the US National Institute for Standards and Technology (NIST). NIST defines it as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011, p. 2). This definition requires computing services to be accessible across private or public networks and also implies that computing resources are pooled, reusable and rapidly reconfigured. Therefore, five essential characteristics are derived: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. In practice CC describes three predominant and related service models (Hancock & Hutley, 2012):

- SaaS - Software as a Service or paying access to software as web-accessed services instead of installing it on the premises.
- PaaS - Platform as a Service or developing and hosting tailor made software in cloud environments (platforms) that provide all required tools, languages, databases and resources.
- IaaS - Infrastructure as a Service or paying access to a computer processing power and storage.

In addition, there are four deployment models for these cloud service offerings: public, private, community and hybrid. The main characteristics of each of them and their main benefits are summarised in Table 4.2.

Cloud type	**Definitions** (Liu et al., 2011, pp. 10-12)	**Benefits** (Armbrust et al., 2010; Hancock & Hutley, 2012; Intelligence and National Security Alliance, 2012)
Public	"It is one in which the cloud infrastructure and computing resources are made available to the general public over a public network"	* Ability to rapidly scale the allocation of computing resources to match fluctuations in business demand * Utility-based pricing. Users only pay for resources actually used * Potentially large economies of scale
Private	"It gives a single cloud consumer's organization the exclusive access to and usage of the infrastructure and computational resources"	* Considered the most secure option but with reduced potential for economies of scale and productivity gains
Community	"It serves a group of cloud consumers which have shared concerns such as mission objectives, security, privacy, and compliance policy (…) It is considered the half way between private and public clouds"	* Reduced economies of scale traded-off for increased security
Hybrid	"It is a composition of two or more clouds that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability"	* Allows for multiple deployment methods to meet specific business/agency needs

Table 4.2: Cloud Deployment Models – Characteristics and Benefits

Despite the benefits there are several constraints that need to be overcome (Armbrust et al., 2010; Hancock & Hutley, 2012; Intelligence and National Security Alliance, 2012). The natural barriers to full adoption include, but are not limited to:

- Speed/latency issues and reliance on telecommunications services providers.
- Compatibility of an organisation's internal processes with cloud offerings.
- Location of data and related security and data sovereignty issues.
- Business continuity/disaster recovery and integration.
- Limited knowledge of product offering and lack of familiarity of business with opportunities.

Business continuity and disaster recovery plans become even more important in CC environments because cloud outages and cloud security compromises are some of the many additional issues that can lead to an operational disruption.

4.2.2 Organisation resilience and coordination processes

Resilience may be viewed as a property or quality that enables a system (individual, organisation or community) to adapt and recover from a disturbance. Notwithstanding the many definitions in the literature, researchers recognise two general types: engineering resilience and ecological resilience (Holling, 2010); the main difference being that the former focuses on efficiency while the latter focuses on persistence. In the field of management, OR emerged in literature in the 1990s as an explanation for the ability of organisations to survive and also thrive when exposed to external shocks such as natural disasters, terrorist attacks and uncertain environments (Wilson, 2010). The concept has been applied to crisis and disasters management; and high-reliability organisations (HROs) (Coutu, 2002; Dalziell & McManus, 2004; Kendra & Wachtendorf, 2003; Paton & Johnston, 2001; Stephenson, 2010; Tierney, 2003; Weick & Sutcliffe, 2001; Weick, Sutcliffe, & Obstfeld, 2008; Woods & Wreathall, 2008). Particularly, Dalziell and McManus (2004) have identified that from this perspective, the main implications of each of the two recognised types of resilience are:

- Engineering resilience implies "maximising the efficiency of systems and process to return and maintain the system at its desired state" (p. 8).
- Ecological resilience implies "designing flexible systems and processes that continue to function in the face of disturbances" (p. 8).

Moreover, organisations increasingly depend on partnerships to achieve their mission (Caralli et al., 2010b). External partners provide essential skills and functions as in the case of CC, where organisations that are consuming CC services are ceding control of some of their business processes to their CC provider. Therefore, organisations are forced to rethink how to assess and build their OR and, especially under suddenly altered conditions of operation, when the coordination process among individuals, ICT services, and other organisations is particularly complex and not well-understood (Comfort & Kapucu, 2006). In fact, Hossain and Kuti (2010) highlight that many of the underlying problems during a disruptive incident response are the result of a poor coordination process. In addition, coordination has been studied in both stable working relationships (Malone & Crowston, 1994) and disruptive incidents response (Comfort & Kapucu, 2006; Hossain & Kuti, 2010). In the former, the main processes analysed include managing shared resources, producer/consumer relationships, simultaneity constraints, and task/subtask dependencies while in the latter, a social networking and a complex adaptive systems perspective have been explored for overcoming coordination problems in emergency response networks.

Based on the abovementioned findings, this study also seeks to extend the scope of prior research by looking at the main changes in the partnership coordination processes when handling disruptive incidents and by adopting an ecological resilience approach in order to focus on designing flexible coordination processes between organisations consuming cloud services and their cloud providers.

4.2.3 Organisational resilience in ICT

In the context of ICT, resilience has been studied mainly from two different perspectives. The first perspective is essentially technical and is often used as a synonym of robustness or fault tolerance. Thus, failures are unavoidable and a resilient system is capable of operating in perturbed mode (Bursztein & Goubault-Larrecq, 2007; Hawes & Reed, 2006; Najjar & Gaudiot, 1990). The second perspective is organisational, being the main interest of this research, and has been studied mainly to understand: how computing systems impact organisational performance, how to assess alternative methods and how to establish essential components. A brief summary of research addressing these topics is presented in Table 4.3.

Topic	Authors
How the strengthen of information systems (individual and systems level) is translated into reliable organisational performance	(Butler & Gray, 2006; Riolli & Savicki, 2003; Shao, 2005)
Impact of information technology and managerial pro-activeness in building net-enabled organisational resilience	(Oh & Teo, 2006)
Comparison of different contingency plans or resilience scenarios, trade-offs and decisions	(Post & Diltz, 1986; Van de Walle & Rutkowski, 2006; Zobel, 2011; Zobel & Khansa, 2012)
Establishment of the essential components of disaster recovery methods	(Cumbie, 2007) (Mousavi, Marjanovic, & Hallikainen, 2012)
Resilience Management Model (RMM) that seeks to manage of ICT operational resilience across three disciplines: security management, BCM and ICT operations management.	(Caralli et al., 2010b)

Table 4.3: ICT Organisational Resilience-related Research

However, few academics and practitioner associations have published specific research on how the adoption of CC impacts the ICT operational resilience and, in general, how to maintain and improve OR when working in cloud environments. Some of these are briefly outlined below:

- Kounev et al. (2012) define resilience as the "system's ability to continue providing available, responsive and reliable services under external perturbations such as security attacks, accidents, unexpected load spikes or fault-loads" (p. 67). The author's consider resilience as part of dependability and provide an overview of the research challenges and opportunities in providing dependability and resilience in cloud environments mainly from the self-adaptive and power management perspectives.
- Undheim, Chilwan, and Heegaard (2011) focus on the availability attribute of a cloud service level agreement (SLA). They develop a simplified cloud system model and identify two possible dimensions for differentiating cloud application as well as proposing some improvements to the cloud's SLAs.
- The Cloud Security Alliance (2011) has been working in the Cloud Controls Matrix, a security controls framework for cloud providers and consumers in assessing the overall security risk of a cloud provider. The domain called "Resiliency" addresses aspects like BCM policy, Impact Analysis, BCM testing and some specific mechanism for particular failures.

This shows that research in ICT operational resilience in CC environments is relatively unexplored and a recent academic literature review shows that many, if not all, avenues are open for future research in this topic (Hoberg, Wollersheim, & Krcmar, 2012).

4.2.4 Research Questions

CC has already had a significant impact on Government agencies, small and medium enterprises and large organisations (Iansiti & Richards, 2011). According to the IDC, ICT cloud services are moving from the early stage of adoption to the mainstream adoption (Gens, 2010), however, organisations are still afraid that their resilience might deteriorate because the additional levels of abstraction that CC introduces making the assessment of ICT operational resilience more difficult (Da Rold, Heiser, & Morency, 2011) and no consensus yet exists on the form or content of such analysis. Based on this, it is the interest of this study to find out what the requirements are for setting up and managing an effective ICT operational resilience management system in CC environments and four research questions around this issue have been identified:

- RQ1: which are the controls and coordination mechanisms that organisations, working on cloud environments, currently use to handle disruptive incidents? An exploratory study will be conducted in order to identify new categories of resilience-oriented requirements when working in CC environments.
- RQ2: how do the main reference architecture characteristics of CC affect the ICT operational resilience requirements? What new requirements emerge? This part of the study will look at the reference architecture components of CC and mapping them with the current ICT resilience management requirements in order to identify possible gaps.

As a result of this first part, this research will propose a conceptual model that helps organisations to maintain and improve OR when working in CC environments, from the ICT operational perspective, focusing on the coordination processes involved in the model. Following, in order to improve the effectiveness of the ICT resilience programs in organisations working in cloud environments an answer to the two final questions of this study needs to be found. Therefore, the proposed artefacts will be used to analyse one of the current ICT resilience standards in order to identify possible gaps and contribute suggestions to respond to the new CC requirements and thereby providing answers to the two final questions.

- RQ3: what should be amended in the current ICT resilience / BCM standards to fulfil these new needs?
- RQ4: in order to support these standards, how should the current controls/processes be adjusted? What new controls/processes should be created?

4.3 Research Design

In the field of information systems many research methodologies have been used, depending on the topic and the philosophical position of the researchers (Burstein & Gregor, 1999). The specific topic that this research is addressing has two main scientific interests. On one hand, it aims to understand how the adoption of CC impacts the OR requirements in order to identify and classify categories of mechanisms that are being used by organisations consuming CC services. This part of the research pursues fundamentally a knowledge-producing objective. On the other hand, it also aims to propose a model that helps organisations that are turning to CC services to maintain and improve their OR from the ICT operational perspective, which is fundamentally a knowledge-using objective. Therefore, the dual nature of the addressed problem is clearly recognisable and this research aims to solve a practical problem while contributing to the body of knowledge. In addition, given the social-technical nature of the problem: "joint effort between the cloud provider and the organisation that requires high levels of coordination in order to avoid unacceptable downtimes", primarily an interpretive approach is employed.

In addition, a number of studies have found that a multiple research methodology should be used to discover different dimensions of the research problem, particularly when the problem deals with real-world complexities, in order to achieve richer results (Adams & Courtney, 2004; Mingers, 2001; Nunamaker, Chen, & Purdin, 1991). Based on the above, this research adopts the multi-methodological approach proposed by Mingers (2001) that follows four major phases: appreciation, analysis, assessment and action as shown in the Figure 4.1.

Specifically, this research in progress proposal is structured as follows:

- The appreciation phase will organise the exploratory study and aims to identify new categories of resilience-oriented requirements when working in CC environments. Collection of real-world data through semi-structured interviews will help to identify and classify the specific mechanisms that are being used by organisations consuming CC services.

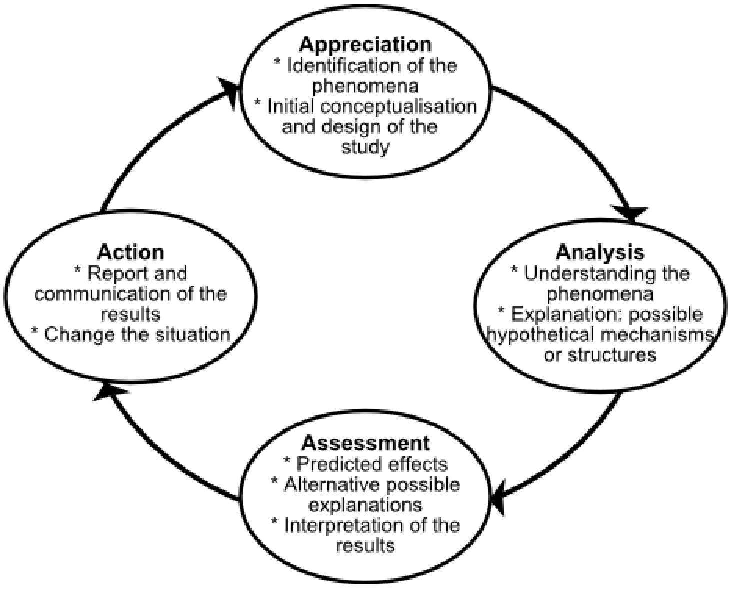

Appreciation
* Identification of the phenomena
* Initial conceptualisation and design of the study
Analysis
* Understanding the phenomena
* Explanation: possible hypothetical mechanisms or structures
Assessment
* Predicted effects
* Alternative possible explanations
* Interpretation of the results
Action
* Report and communication of the results
* Change the situation

Figure 4.1: Research as a Process: a Multi-method Approach to IS Research, based on (Mingers, 2001)

- The phase of analysis, using the results from the previous phase and focusing on the reference architecture of CC (Liu et al., 2011), will propose a conceptual model that helps organisations to maintain and improve OR when working in CC environments from the ICT operational perspective. In addition, as lack of coordination has been identified as one of the main problems when facing disruptive incidents, this model will include the fundamental coordination processes for overcoming managing dependencies problems between the organisation that is consuming cloud services and their CC provider.
- The assessment phase will test the two designed artefacts through three different approaches: first, based on a structuralist approach the elements of the model and the connections among them will be assessed. Secondly, following an experts' opinions approach the two artefacts will be presented to determine the quality of their foundation in order to obtain academic judgments as an additional input to refine it. Finally, in order to demonstrate the validity of the artefacts through different types of tests, like walkthrough and tabletop exercises, that are domain specific to the main research topic, ICT resilience.
- In the final action phase the proposed artefacts will be used to analyse one of the current ICT resilience standards in order to identifying possible gaps and make some suggestions to respond to the new CC requirements.

In addition, other authors have proposed conceptual frameworks for understanding, executing and evaluating IS research when using multiple paradigms. For instance, the framework proposed by Hevner, March, Park, and Ram (2004) is particularly helpful for this study because it addresses the "interplay among business strategy, IT strategy, organizational infrastructure, and IS infrastructure" (p. 78) while balancing the practical and theoretical contributions. In conclusion, this study is employing mainly an interpretive approach adopting a tailored multi-method framework.

4.4 Expected Contributions

The main contributions of this study will be the proposed conceptual model and the fundamental coordination processes involved in the model. It is expected that the designed artefacts will integrate the foundational and practical requirements of ICT operational resilience in CC environments and be used for planning and decision making to anticipate, prevent, prepare for, and respond to ICT disruptive incidents. Thus, the results of this research should be of interest to academic researchers and practitioners.

In addition, given the explained context and the problem addressed, this research tangentially contributes to:

- Establishing a common terminology in ICT resilience that could be used for both academics and practitioners to facilitate its understanding and/or its operationalization. Particularly, from the CC services market perspective, the current lack of common terminology in ICT operational resilience is a specific problem that makes it more difficult to assess the trustworthiness of CC providers as mentioned previously.
- Identifying and classifying new requirements in the ICT resilience subject for cloud environments that could guide future research. Also, this classification could be used as an educational material to improve resilience awareness in organisations working in cloud environments.
- Identifying controls and mechanisms that organisations could use to minimise potential impacts of ICT services disruptions particularly useful for cloud environments. Even though current ICT resilience standards provide guidelines that can be used by organisations to achieve this objective, new specific requirements for cloud environments could demand some changes.
- Reducing CC adoption barriers, working on and learning from one of the identified challenges. This research supports the boosting of cloud computing and its positive impacts and helps with increasing resilience against the risks that ICT can bring to organisations (World Economic Forum & INSEAD, 2012).

- Enabling reliable services, organisations using CC can expand their markets and governments can make their services more efficient while decreasing ICT expenses but not their reliability (European Commision, 2012).

Acknowledgments

A special thank you goes to Dr. Fernando Beltrán and Dr. David Sundaram for their valuable comments and sharing their knowledge.

4.5 References

Adams, L. A., & Courtney, J. F. (2004, 5-8 Jan. 2004). Achieving relevance in IS research via the DAGS framework. Paper presented at the HICSS, 2004. Proceedings of the 37th Annual Hawaii International Conference on System Sciences.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Gunho L., Patterson D., Rabkin A., Stoica I. & Zaharia, M. (2010). A view of cloud computing. Commununications of the ACM, 53(4), 50-58. doi: 10.1145/1721654.1721672.

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). SP 800-146: Cloud computing synopsis and recommendations.

Boin, A., & Lagadec, P. (2000). Preparing for the future: critical challenges in crisis. Management. Journal of Contingencies and Crisis Management, 8(4), 185-191. doi: 10.1111/1468-5973.00138.

Burstein, F., & Gregor, S. (1999). The systems development or engineering approach to research in information systems: an action research perspective. Proceedings of the 10th Australasian Conference on Information Systems.

Bursztein, E., & Goubault-Larrecq, J. (2007). A logical framework for evaluating network resilience against faults and attacks. Advances in Computer Science–ASIAN 2007. Computer and Network Security, 212-227.

Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. MIS Quarterly, 30(2), 211-224.

Buyya, R., Ranjan, R., & Calheiros, R. (2010). InterCloud: utility-oriented federation of cloud computing environments for scaling of application services. In C.-H. Hsu, L. Yang, J. Park & S.-S. Yeo (Eds.), Algorithms and architectures for parallel processing (Vol. 6081, pp. 13-31): Springer Berlin / Heidelberg.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). CERT® Resilience management model v1.0: improving operational resilience processes (S. E. Institute, Trans.): Carnegie Mellon.

Catteddu, D., & Hogben, G. (2009). Cloud computing: benefits, risks and recommendations for information security: European Network and Information Security Agency.

Centre for Economics and Business Research ltd. (2011). The cloud dividend: part two - the economic benefits of cloud computing to business and the wider EMEA economy (Comparative analysis of the impact on aggregated industry sectors). London: Cebr.

Chen, Y., Paxson, V., & Katz, R. H. (2010). What's new about cloud computing security?: University of California at Berkeley - Electrical Engineering and Computer Sciences.

Cloud Security Alliance. (2010). Top threats to cloud computing, version 1.0.

Cloud Security Alliance. (2011). Security guidance for critical areas of focus in cloud computing V3.0.

Comfort, L. K., & Kapucu, N. (2006). Inter-organizational coordination in extreme events: The World Trade Center attacks, September 11, 2001. Natural Hazards, 39(2), 309-327.

Coutu, D. L. (2002). How resilience works. Harvard Business Review, 80(5), 46-56.

Cumbie, B. (2007). The essential components of disaster recovery methods: a delphi study among small businesses. Paper presented at the AMCIS 2007 Proceedings. Paper 115.

Da Rold, C., Heiser, J., & Morency, J. P. (2011). The realities of cloud services downtime: what you must know and do.

Dalziell, E., & McManus, S. (2004). Resilience, vulnerability and adaptive capacity: implications for system performance. Paper presented at the International Forum for Engineering Decision Making.

European Commision. (2012). Unleashing the potential of cloud computing in europe. Brussels: Retrieved from http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf.

Gens, F. (2010). IDC IT cloud services survey, 2Q10.

Hancock, I., & Hutley, N. (2012). Modelling the economic impact of cloud computing: KPMG and Australian Information Industry Association (AIIA).

Hawes, C., & Reed, C. (2006). Theoretical steps towards modelling resilience in complex systems. Computational Science and Its Applications-ICCSA 2006, 644-653.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly., 28(1), 75-105.

Hoberg, P., Wollersheim, J., & Krcmar, H. (2012). The business perspective on cloud computing - a literature review of research on cloud computing. Paper presented at the AMCIS 2012 Proceedings. Paper 5.

Holling, C. S. (2010). Engineering resilience versus ecological resilience. In L. H. Gunderson, C. R. Allen & C. S. Holling (Eds.), Foundations of ecological resilience Washington : Island Press, c2010.

Hossain, L., & Kuti, M. (2010). Disaster response preparedness coordination through social networks. Disasters, 34(3), 755-786.

Iansiti, M., & Richards, G. L. (2011). Economic impact of cloud computing white paper. Working papers series. Retrieved from http://ssrn.com.ezproxy.auckland.ac.nz/abstract=1875893.

Intelligence and National Security Alliance. (2012). Cloud computing: risk, benefits, and mission enhancement for the intelligence community: Intelligence and National Security Alliance - INSA, Cloud Computing task force.

International Organization for Standardization. (2012). 22301: Societal security - Business continuity management systems - Requirements terms and definitions. Switzerland.

Kendra, J. M., & Wachtendorf, T. (2003). Elements of resilience after the world trade center disaster: reconstituting New York City's Emergency Operations Centre. Disasters, 27(1), 37-53.

Kounev, S., Reinecke, P., Brosig, F., Bradley, J., Joshi, K., Babka, V., Stefanek, A. & Gilmore, S. (2012). Providing dependability and resilience in the cloud: challenges and opportunities. In K. Wolter (Ed.), Resilience assessment and evaluation of computing systems: Berlin ; London : Springer, 2012.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). SP 500-292: NIST Cloud computing reference architecture. Gaithersburg, MD: US National Institute of Standards and Technology (NIST) - Information Technology Laboratory.

Mahowald, R. P., & Sullivan, C. G. (2012). Worldwide SaaS and cloud software 2012–2016 Forecast and 2011 Vendor Shares: International Data Corporation.

Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. ACM Comput. Surv., 26(1), 87-119. doi: 10.1145/174666.174668.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. Decision Support Systems, 51(1), 176-189. doi: http://dx.doi.org/10.1016/j.dss.2010.12.006.

Mell, P., & Grance, T. (2011). The NIST Definition of cloud computing special publication (SP) 800-145. Gaithersburg, MD: US National Institute of Standards and Technology (NIST).

Mingers, J. (2001). Combining IS research methods: towards a pluralist methodology. Information systems research, 12(3), 240-259.

Mousavi, P., Marjanovic, O., & Hallikainen, P. (2012). Disaster recovery – The process management perspective. Paper presented at the PACIS 2012 Proceedings. Paper 67.

Najjar, W., & Gaudiot, J. L. (1990). Network resilience: a measure of network fault tolerance. IEEE Transactions on Computers, 39(2), 174-181.

Nunamaker, J., Chen, M., & Purdin, T. D. M. (1991). Systems development in information systems research. Journal of Management Information Systems, 7(3), 89-106.

Oh, L. B., & Teo, H. H. (2006). The impacts of information technology and managerial proactiveness in building net-enabled organizational resilience. The Transfer and Diffusion of Information Technology for Organizational Resilience, 33-50.

Paton, D., & Johnston, D. (2001). Disasters and communities: vulnerability, resilience and preparedness. Disaster Prevention and Management, 10(4), 270-277.

Post, G. V., & Diltz, J. D. (1986). A stochastic dominance approach to risk analysis of computer systems. MIS Quarterly, 10(4), 363-375.

Riolli, L., & Savicki, V. (2003). Information system organizational resilience. Omega, 31(3), 227-233.

Saya, S., Pee, L. G., & Kankanhalli, A. (2010). The impact of institutional influences on perceived technological characteristics and real options in cloud computing adoption. Paper presented at the International Conference On Information Systems (ICIS).

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

Stephenson, A. V. (2010). Benchmarking the resilience of organisations. (Doctoral thesis), University of Canterbury, Christchurch.

Tierney, K. J. (2003). Conceptualizing and measuring organizational and community resilience: lessons from the emergency response following the September 11, 2001 attack on the World Trade Center.

Toomer, L. G. D. (2011). FISMA compliance and cloud computing. Paper presented at the Proceedings of the 2011 Information Security Curriculum Development Conference, Kennesaw, Georgia.

Undheim, A., Chilwan, A., & Heegaard, P. (2011). Differentiated availability in cloud computing SLAs. Paper presented at the 2011 12th IEEE/ACM International Conference on Grid Computing (GRID).

Van de Walle, B., & Rutkowski, A.-F. (2006). A fuzzy decision support system for IT service continuity threat assessment. Decision Support Systems, 42(3), 1931-1943. doi: 10.1016/j.dss.2006.05.002.

Weick, K. E., & Sutcliffe, K. M. (2001). Managing the Unexpected: Assuring high performance in an age of complexity. 2001. University of Michigan Business School Management Series.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: processes of collective mindfulness. Crisis management, 3, 81-123.

Wilson, R. L. (2010). Organizational resilience models applied to companies in bankruptcy. (Doctor of Management), University of Maryland University College, United States - Maryland.

Woods, D. D., & Wreathall, J. (2008). Stress-strain plots as a basis for assessing system resilience. Resilience Engineering: Remaining Sensitive to the Possibility of Failure, 143-158.

World Economic Forum, & INSEAD. (2012). The global information technology report 2012: Living in a Hyperconnected World.

Yang, H., & Tate, M. (2012). A descriptive literature review and classification of cloud computing research. Communications of the Association for Information Systems, 31(1), 2.

Zobel, C. W. (2011). Representing perceived tradeoffs in defining disaster resilience. Decision Support Systems, 50(2), 394-403. doi: 10.1016/j.dss.2010.10.001.

Zobel, C. W., & Khansa, L. (2012). Quantifying cyberinfrastructure resilience against multi-event attacks. Decision Sciences, 43(4), 687-710. doi: 10.1111/j.1540-5915.2012.00364.x.

5 Issues in the Study of Organisational Resilience in Cloud Computing Environments

Cloud Computing is a promising ICT service delivery model that has already had a significant impact on government agencies, SMEs and large organisations. Even though its current adoption is moving away from the early stage to the mainstream, many organisations are still uncertain given the additional levels of abstraction that cloud environments introduce. Particularly, this additional complexity represents a hurdle in the assessment of ICT readiness for organisational resilience, and no consensus exists yet for its analysis. Based on a literature review of cloud computing reference architectures, and organisational resilience and business continuity frameworks, this paper suggests a framework to guide research into this field from an operational perspective.

5.1 Introduction

Cloud computing (CC) is a new way of delivering computing resources. For some, it is the most important revolution in recent times in the field of ICT, while for others, it is only another step towards utility computing. Regardless of how notable this model is, it promises numerous benefits and organisations are increasingly turning to these services. International Data Corporation's (IDC) forecasts that by 2016, US $1 of every US $5 will be spent on CC (Mahowald & Sullivan, 2012). However, cloud environments have also raised various concerns and an increasing number of researchers are developing knowledge about CC from technical to business issues (Yang & Tate, 2012). In the former, issues regarding portability, interoperability and security have been studied (Buyya et al., 2010; Chen et al., 2010). In the latter, researchers have been working specifically on economic impact, costs, reasons for adoption and growth trends (Marston et al., 2011). A topic that incorporates issues from both perspectives, known as availability in CC environments, has been identified as one of the main obstacles to and opportunities for the growth of CC (Armbrust et al., 2010; Cloud Security Alliance, 2011). Therefore, CC failures and their effects in organisational resilience (OR) needs to be understood.

This necessity is also as a result of the considerable attention that the OR concept has gained in the last few years (Gibson & Tarrant, 2010) and consequently the increased demand for organisations to exhibit high reliability in the face of adversity. These two factors have highlighted the need to strengthen the ability of organisations to respond to disruptive incidents when working in cloud environments. This paper presents a research framework which addresses key issues when studying OR in CC environments, from an ICT's operational perspective. The framework is constructed from a literature review of CC characteristics derived from well-known reference architectures, and a compilation of OR specifications also derived from the most popular OR / Business Continuity (BC) standards and models.

This paper takes the form of five sections, including this introduction. Section two begins by presenting a brief overview of CC, and then describes how the baseline architecture and its characteristics have been defined. In the third section, a set of resilience specifications for discussing OR key issues in these environments is presented while the fourth section describes the proposed research framework. Finally, section five summarises the contributions.

5.2 Cloud Computing Architecture

The baseline architecture serves as a reference point to study how existing resilience specifications are affected by the CC adoption from an operational ICT perspective.

5.2.1 Overview of cloud computing

The most popular definition of CC is the National Institute of Standards and Technology (NIST) definition: “CC is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance, 2011, p. 2). Particularly, architectures that are part of this study have adopted it to some extent, therefore, there is a strong agreement for its three fundamental components: characteristics, service delivery models and service deployment models. (1) The five essential characteristics are: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service; (2) a taxonomy of three service delivery models: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) and (3) four deployment models describing how these services can be shared: private cloud, community cloud, public cloud, and hybrid cloud. Regarding the last two components, some architectures have identified a fourth type of service model that goes beyond SaaS, known as business process as a service (BPaaS) and the majority of them disregard the community deployment model. As this research has adopted the CC NIST definition, it maintains the 5x3x4 original scheme.

5.2.2 Baseline reference architecture – Methodology

A literature review approach was adopted and an online search was conducted in four online databases: ACM Digital Library, IEEE Xplore, ProQuest (ABI/INFORM), and ScienceDirect (Elsevier), resulting in the identification of eight main architectures. These architectures can be grouped into two types according to their main focus: Role-based and Layer-based, as show in Table 5.1.

Role-based	Layer-based
(1) SP 500-292: NIST Cloud Computing Reference Architecture (Liu et al., 2011)	(5) CSA Enterprise Reference Architecture (Cloud Security Alliance, 2013)
(2) IBM Cloud Computing Reference Architecture 2.0 (Behrendt et al., 2011)	(6) Cloud Computing Reference Architecture – CCRA (Liu et al., 2012)
(3) Oracle - Cloud Reference Architecture (Oracle Corporation, 2012)	(7) Cisco Cloud Reference Architecture Framework (Cisco Systems, 2011)
(4) DMTF - Architecture for Managing Clouds (DMTF - Open Cloud Standards Incubator, 2010)	(8) IETF Intercloud Architecture Framework-05 ICAF (Khasnabish et al., 2013)

Table 5.1: Classification of the Cloud Computing Architectures

The first step was to review the full text of each architecture. One of them, the DMTF, was discarded because it is exclusively focused on the IaaS model. The next step was to compare architectures by group. This task was relatively simple for the role-based group because there are many shared concepts and elements. On the other hand, the consolidation of characteristics into a meaningful set for the layer-based group was more demanding given the wider range of approaches. After this step, architectures (1), (2), (5) and (8) were chosen as the most relevant and the baseline architecture, main outcome of this process, was compiled.

5.2.3 Baseline reference architecture – Components

CC architectures are defined as generic high-level conceptual models for understanding the basic roles involved in CC and the relationships among them. Specifically, this research has adopted the definition of CC architecture by NIST (Liu et al., 2011, p. 2) that defines a set of elements that can be used to develop more specific architectures. Based on this, the baseline architecture is founded on a three-dimensional approach: principles, actors and architecture building blocks.

Most of the reference architectures identify guiding principles that are useful when designing a specific CC architecture. A summary of the most important principles is presented below (Behrendt et al., 2011; Liu et al., 2012; Oracle Corporation, 2012):

- Interoperability support: a CC architecture must be elastic, flexible and resilient in order to support multi-tenant and multi-landlord platforms.
- Leverage commonalities: management capabilities with reuse potential should be designed generically and share a common platform for the various layers required by both consumers and providers.
- Design for productivity and efficiencies: in order to support CC characteristics the cloud design should be strictly oriented to high cloud scale efficiencies and short time-to-delivery/time-to-change.
- Service management support: service orientation capabilities should be supported as well as their management processes throughout their lifecycle.
- Reliability, availability, security and privacy support: any CC based-system must conform to standards and regulations' requirements, consequently, responsibilities have to be shared among providers and consumers.

The amount of actors vary from two to five but at least two actors are always recognised as essentials: consumers and providers. However, cloud services can be too complex for consumers to manage and increasingly consumers are requesting services from cloud brokers instead of contacting providers directly. Therefore, this research has also adopted cloud broker, for a total of three main actors (Behrendt et al., 2011; Liu et al., 2011). (1) Consumer: a person or organisation that has a relationship with, and consumes service instances delivered from a particular cloud provider. (2) Provider: a person, organisation, or entity responsible for making a service available to interested parties. (3) Broker: an entity that designs and manages the use, performance and delivery of cloud services. It could be seen as a specific type of provider that is responsible for designing, creating, packaging, and deploying cloud services for end-users consumption.

In order to compile the additional components of the studied architectures, this research has adopted the concept of architecture building blocks (ABBs). According to The Open Group an ABB describes capabilities to meet business needs across an organisation capturing both business and technical requirements (The Open Group, 2011). All the identified ABBs can play an important role for all the actors, however, they are grouped by actor according to their relevance.

- Service integration compiles processes that enable the integration of cloud services with on-premise services.

- Service orchestration refers to the composition of system components to support CC providers' activities in arrangement, coordination and management of resources in order to provide services. It can be divided into four: access and service delivery; cloud service; cloud resources control and composition; and resources.
- Business management provides monitoring and administration of the cloud platform to keep it operating normally. It can be divided into two: (1) ICT Operation and Support (ICTOS) that represents a set of technical and operational management services to keep the systems going even in the event of a disaster, and (2) Business Support Services (BSS) entails the set of business-related services dealing with customers services.
- Service creation compiles processes and tools to create, deliver and manage value-added services.
- Operational risk and "consumability" compiles non-functional aspects across the environment providing a solid context for operations and support.
- Governance is an essential block to maintain control over the environment: systems, services and humans, which integrates activities such as corporate governance, enterprise risk management, and corporate compliance.

Consumers, providers and brokers have different degrees of control over a cloud environment compared to traditional ICT systems, where one organisation has control over the whole stack. Therefore, this baseline architecture (see Figure 5.1) reflects how all three actors collaboratively design, build, deploy, and operate the system. More important, all parties share the responsibilities in providing it with adequate protections.

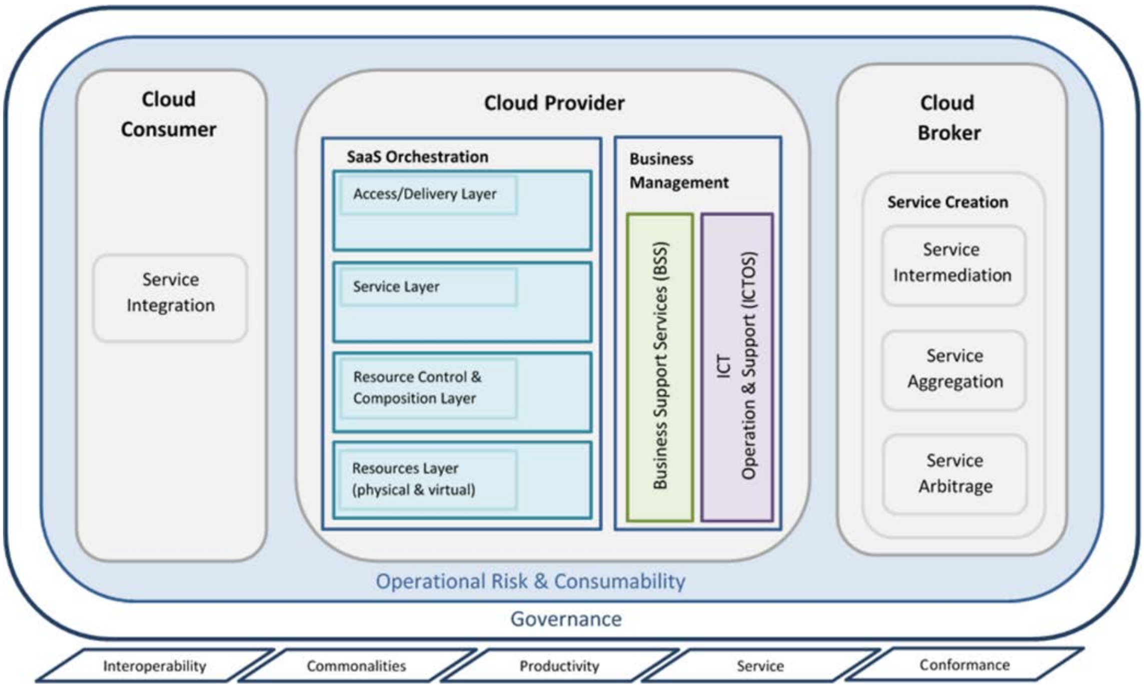


Figure 5.1: Baseline Architecture, based on (Behrendt et al., 2011; Cisco Systems, 2011; Cloud Security Alliance, 2013; Khasnabish et al., 2013; Liu et al., 2011; Liu et al., 2012; Oracle Corporation, 2012)

5.3 Organisational Resilience High-level Conceptual Model

Following the previous section structure, this section presents a brief overview of OR, describes the approach for compiling the specifications and states the general context and the specific ICT resilience processes.

5.3.1 Overview of organisational resilience

OR emerged in the field of management in the 1990s as an explanation for the ability of organisations to survive and also thrive when exposed to external shocks such as natural disasters, terrorist attacks and uncertain environments. It has been applied to areas such as crisis and disaster management, high-reliability organisations and ICT. In the latter, "mainly to understand how computing systems impact organisational performance, how to assess alternative methods and how to establish essential components" (Herrera & Janczewski, 2013, p. 5). Regardless the many areas of application, two general perspectives are recognised (Dalziell & McManus, 2004, p. 8): (1) engineering resilience that aims to maximise "the efficiency of systems and process to return and maintain the system at its desired state" and (2) ecological resilience than aims to design "flexible systems and processes that continue to function in the face of disturbances”. As this study is looking at key issues when handling disruptive incidents in CC environments, an ecological resilience approach has been adopted.

5.3.2 Organisational resilience requirements – Methodology

Following a literature review approach, using the same four online databases, six OR/BC frameworks were identified and classified into two groups, as shown in Table 5.2. Definitions and general specifications were derived from the first group and given the explicit perspective of this study processes were identified from the second group.

General purpose	ICT specialized
(ASIS SPC 1-2009) Organizational Resilience: Security, Preparedness and Continuity Management Systems (American National Standards Institute, 2009)	(BS ISO/IEC 27031:2011) Information technology. Security techniques. Guidelines for information and communication technology readiness for BC (British Standards Institute, 2011)
(NFPA 1600: 2013) Disaster/Emergency Management and BC Programs (National Fire Protection Association, 2004)	
(AS/NZS 5050:2010) BC – Managing disruption-related risk (Standards Australia/Standards New Zealand, 2010)	(RMM 2010) CERT – Resilience Management Model (Caralli et al., 2010b)
(ISO 22301:2012) Societal security – BC management systems (International Organization for Standardization, 2012)	

Table 5.2: Classification of the Organisational Resilience / Business Continuity Frameworks

5.3.3 Organisational resilience specifications

According to the first group of frameworks, the primary focus of OR is to control organisational behaviour and response, during times of disruption making their services resilient. OR is defined as the adaptive capacity of an organisation in a complex and changing environment that enables it to resist and return to an acceptable level of performance in an acceptable period of time after being affected by an event. In other words, OR is the result of harmonic and convergent efforts to adapt and thrive from disruptive incidents (in this research disruptive incidents that come from the use of computing power in a cloud environments). As a result, OR includes both developmental and operational activities in order to prevent; stabilise, continue critical services, recover and manage consequences; and improvement activities, as shown in Figure 5.2.

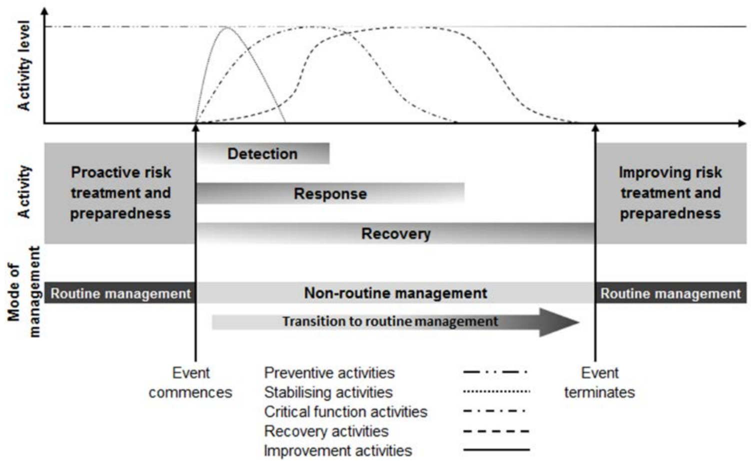


Figure 5.2: Activities vs. Incident Stages, adapted from "Relationship of treatments for disruption-related risk" (Standards Australia/Standards New Zealand, 2010)

The first type of activities, preventive activities, deals with strategies designed to minimize an asset's exposure to sources of disruption; some examples of such activities are processes, procedures, policies and controls. The second type, continue and management consequences activities includes stabilising, continuing critical functions and recovering activities. Thus, it focuses on strategies designed to keep assets operating as close to normal as possible when facing disruptive incidents through strategies such as processes, procedures, polices, plans and controls and also, on strategies that are aimed at returning to routine operations and a full recovery as soon as possible. Lastly, improvement activities translate into strategies designed to achieve continual improvement by correcting and/or adopting new strategies of both previous types.

Consequently, these frameworks follow the "Plan-Do-Check-Act" (PDCA) model to plan, establish, implement, operate, monitor, review, maintain and continually improve the effectiveness of an organisation's resilience. The number of stages vary from four to seven and this research has explicitly adopted the general structure of the ASIS SPC 1-2009 framework that provides a comprehensive summary in six stages. However, these stages are been slightly modified to capture additional specifications from the other frameworks (American National Standards Institute, 2009; International Organization for Standardization, 2012; National Fire Protection Association, 2004; Standards Australia/Standards New Zealand, 2010).

The model starts with the "know your organisation" stage that includes an organisation's strategic objectives, risk appetite and internal/external operational constraints for establishing OR objectives and therefore high-level OR requirements. After this step, the top management defines policies emphasising their commitment to the protection of human, environmental and physical assets; and business and operational continuity. Planning, the next stage, includes risk assessment, business impact analysis and their evaluation to assist in making decisions about which elements need treatment and the priority for implementation. Based on the previous outcomes, the implementation and operation stage develops and implements plan requirements, and strategies to prevent, handle, control and mitigate disruptive incidents. This stage is very important, however, strategies that have not been periodically tested are not really reliable, in this aspect lies the importance of the next stage, checking and corrective actions. It basically tests the appropriateness and efficacy of the organisation's OR activities. Finally, the management review stage involves regular surveillance in order to provide assurance of ongoing relevance, readiness and effectiveness of OR activities.

After the OR general context has been outlined, the second part of this section addresses specific ICT elements related with OR based on two frameworks: the BS ISO/IEC 27031 Information technology — Security techniques - Guidelines for ICT readiness for business continuity (British Standards Institute, 2011) and the Resilience Management Model (RMM) (Caralli et al., 2010b). The former encompasses all types of events that could have an impact on ICT infrastructure and systems, and introduces a management system to address ICT in support of a broader BC management system. It describes a systematic process to achieve a specific objective, however, it does not address explicit operational processes to improve and measure OR as the latter does. As this study is looking at the key areas where researchers can study how the characteristics of CC impact ICT operational resilience specifications, the RMM has been adopted as main ICT specialised framework.

The RMM developed by the Carnegie Mellon University's Computer Emergency Response Team seeks to manage ICT operational resilience across three disciplines: security management, business continuity and ICT operations management. It has 26 process areas that are organised into four high-level categories: engineering, enterprise management, operations, and process management (see Figure 5.3); it also defines six levels of resilience maturity: incomplete, preferred, managed, defined, quantitatively managed, and optimised.

Enterprise management	Operations
Communications [COMM] Compliance Management [COMP] Enterprise Focus [EF] Financial Resource Management [FRM] Human Resource Management [HRM] Organizational Training and Awareness [OTA] Risk Management [RISK]	External Dependency Management [EXD] Access Management [AM] Identity Management [ID] Incident Management and Control [IMC] Vulnerability Analysis and Resolution [VAR] Environmental Control [EC] Knowledge and Information Management [KIM] People Management [PM] Technology Management [TM]
Process management	**Engineering**
Monitoring [MON] Organizational Process Definition [OPD] Organizational Process Focus [OPF] Measurement and Analysis [MA]	Resilience Requirements Development [RRD] Resilience Requirements Management [RRM] Asset Definition and Management [ADM] Controls Management [CTRL] Resilient Technical Solution Engineering [RTSE] Service Continuity [SC]

Figure 5.3: RMM Processes by High-level Categories, based on (Caralli et al., 2010b)

5.4 Research Framework - Key Issues when Studying Organisational Resilience in Cloud Computing Environments

As organisations move their ICT services into CC environments a better understanding of what OR means when working in cloud environments is required. The proposed research framework illustrates some key areas where researchers can study how the adoption of CC, as an ICT service delivery model, impacts the existing ICT resilience processes and provides a starting point to identify new processes if required. Based on the literature presented in the previous sections, this section presents a multi-level framework that captures key issues when studying ICT operational resilience in CC environments from the macro level of CC's ABBs to the micro level of organisational resilience capabilities. The macro level, architectural, captures the three dimensions in which the baseline architecture is founded focusing on the ABBs. The micro level, capabilities, analyses linkages among resilience process areas in order to identify dependencies that should be considered when studying a specific process area.

5.4.1 Architectural level - Locating ICT resilience processes in the cloud computing baseline architecture

This level shows what kind of ICT resilience processes support certain ABBs' capabilities. It aims to provide a bridge between current ICT resilience processes and high-level cloud service requirements and structures, which enables researchers to identify where the main concerns arise in a generic cloud environment as shown in Figure 5.4. Specifically, it shows how the 26 processes are clustered in four ABBs as briefly explained below.

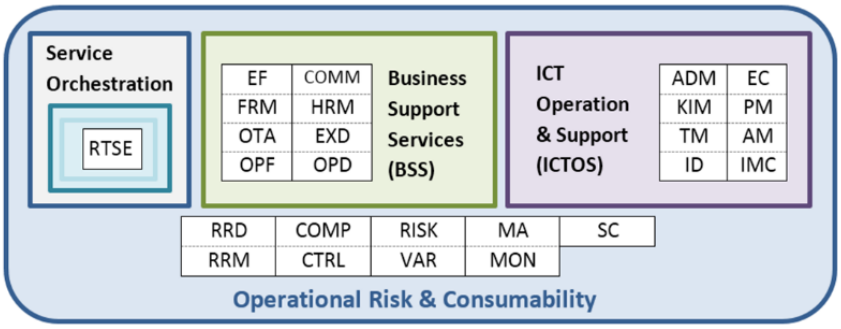


Figure 5.4: Proposed Research Framework – Architectural level

At the service orchestration block, which provides core capabilities from the physical layer to the access layer to support cloud services, only one process is placed. The "Resilient Technical Solution Engineering" (RTSE) states that applications "must be specifically designed and developed with consideration of the types of threats they will face, the operating conditions and changing risk environment in which they will operate" (Caralli et al., 2010b). CC characteristics such as the number of distributed components and their usual large-scale, make this topic a critical research problem. Therefore, traditional software reliability engineering techniques such as fault prevention, fault removal, fault tolerance, and fault forecasting should be studied in order to find a feasible approach for building highly reliable cloud applications. In CC, this topic has mainly focused on the first two techniques (Zhao, Melliar-Smith, & Moser, 2010) and researchers could considerer the other two techniques.

The BSS block provides guidance on understanding who the service customers are, the service offerings that are required to meet their needs, and the ICT capabilities and resources that are required to develop these offerings. This ABB mostly clusters enterprise-wide competences that help an organisation to improve and develop over the long term. For this type of competence researchers may need to extend traditional ICT governance knowledge to cloud governance (Peiris, Sharma, & Balachandran, 2011) and consider the involvement of business partners for establishing a robust communication plan over the life of the relationship (Rimal, Jukan, Katsaros, & Goeleven, 2011).

The ICTOS block carries out operational tasks in order to make sure that cloud services are delivered effectively and efficiently. Many resilient-concerns arise in this ABB. The first potential research area is the shared establishment and management of an appropriate level of control over the different types of assets (people, facilities, information, and technology) among the CC actors. Also, regular activities such as identity and access management seem to be a potential area of research given privacy concerns, especially for the multitenant deployment models (Xiaohui, Jingsha, & Ting, 2013). Finally, the establishment of processes in order to identify and analyse events, detect incidents, and determine an appropriate coordinated response is considered critical in cloud environments (Cao & Zhan, 2011).

The Operational risk and "consumability" block is the ABB that collects non-functional aspects that should be viewed from an end-to-end perspective in order to provide the core components to safeguard cloud services. Research areas focusing on the strengthening of resilience capacities to (1) determine appropriate requirements, control selection and oversee continuity of operations (Julisch & Hall, 2010) and (2) ensure that the consumer organisation has the capability to manage the risk of unmet requirements from providers and brokers (Dutta et al., 2013) should be considered. Therefore, not only a researcher needs to understand how to strengthen these resilience capabilities, they also need to consider new forms of monitoring that allows consumers to ensure compliance with relevant standards (Shim & Lim, 2013).

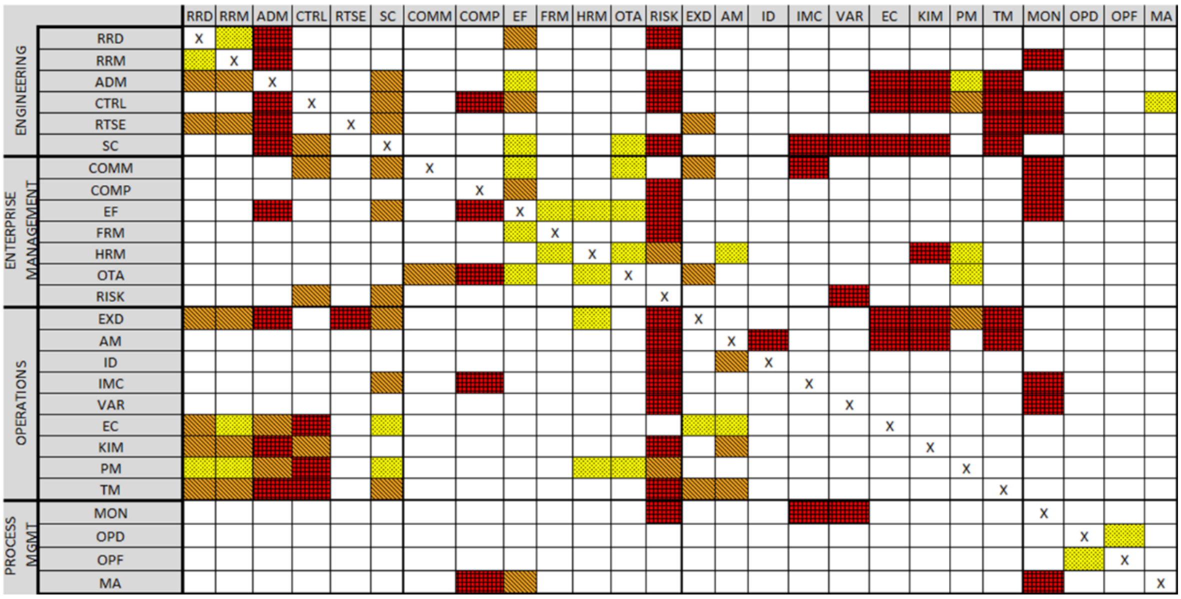
The architectural level illustrates some important areas for research into ICT operational resilience within cloud environments, however, it leaves out the interactions among processes that can also be helpful when studies focus on accomplishing a specific goal. For instance, after the "Service Orchestration" BB has been recognised as a critical research area in order to improve the reliability of cloud services, researchers need to link together the processes areas that contribute to satisfy this particular objective. For this example, RTSE is linked on specific capabilities of areas such as RRD, RRM, ADM, SC, EXD, TM and MON (Caralli et al., 2010b) to effectively develop resilient services. Therefore, understanding these relationships can help researchers in developing research roadmaps.

5.4.2 Capabilities level - Identifying potential impact levels introduced by cloud computing environments on the interactions among ICT resilience processes

This level analyses linkages among resilience process areas in order to identify dependencies that should be considered when conducting a comprehensive study of a specific process area or when pursuing a specific resilience-related objective. In order to identify key dependency issues, two main steps were followed: first, based on the RMM model a linkages-matrix among resilience-processes **M** has been defined. This matrix is the result of consolidating the sections "related-processes" in the RMM, which are part of the process descriptions and "list references to other process and reflects the high-level relationships among capabilities" (Caralli et al., 2010b, p. 31). Thus, this section identifies which other capabilities are complementary and should be considered when improving a specific process area. For instance, for the service continuity [SC] process "the consideration of consequences as a foundational element for developing service continuity plans is addressed in the Risk Management [RISK] process" (Caralli et al., 2010b, p. 34) or in other words the SC process area depends on a subset of the RISK process area capabilities. The main characteristics of matrix **M** are:

- It is a square matrix, where each row and column represent one of the 26 ICT resilience processes.
- An entry in the matrix $\mathbf{m_{i,j}}$ represents a high-level relationship between processes i and j. (1) entries in the main diagonal are invalid, (2) entries in the i-th row show complementary capabilities that the i-th process requires to satisfy its set of goals, and (3) entries in the j-th column show what processes depend on process j capabilities.
- Empty cells show non-existing relationships between two processes.

As a result of the second step the matrix M' has been created (see Figure 5.5). It shows the result of a systematic assessment of the potential impact of CC adoption on the ICT resilience processes and their linkages. This assessment has been conducted based on the CC baseline architecture and the RMM process areas documentation, specifically sections "Purpose" and "Specific Practices by Goal" (Caralli et al., 2010b). Three qualitative types of impact are defined:



		RRD	RRM	ADM	CTRL	RTSE	SC	COMM	COMP	EF	FRM	HRM	OTA	RISK	EXD	AM	ID	IMC	VAR	EC	KIM	PM	TM	MON	OPD	OPF	MA
ENGINEERING	RRD	X	🟨	🟥						🟧				🟥													
	RRM	🟨	X	🟥																				🟥			
	ADM	🟧	🟧	X			🟧			🟨				🟥						🟥	🟥	🟨	🟥				
	CTRL			🟥	X		🟧		🟥	🟧				🟥						🟥	🟥	🟧	🟥	🟥			🟨
	RTSE	🟧	🟧	🟥		X	🟧								🟧								🟥	🟥			
	SC			🟥	🟧		X			🟨			🟨	🟥				🟥	🟥	🟥	🟥		🟥				
ENTERPRISE MANAGEMENT	COMM				🟧		🟧	X		🟨			🟨		🟧			🟥						🟥			
	COMP								X	🟧				🟥										🟥			
	EF			🟥			🟧		🟥	X	🟨	🟨	🟨	🟥										🟥			
	FRM									🟨	X			🟥													
	HRM										🟨	X	🟨	🟧		🟨					🟥	🟨					
	OTA							🟧	🟥	🟨		🟨	X		🟧							🟨					
	RISK				🟧		🟧							X					🟥								
OPERATIONS	EXD	🟧	🟧	🟥		🟥	🟧					🟨		🟥	X					🟥	🟥	🟧	🟥				
	AM													🟥		X	🟥			🟥	🟥		🟥				
	ID													🟥		🟧	X										
	IMC						🟧		🟥					🟥				X						🟥			
	VAR													🟥					X					🟥			
	EC	🟧	🟨	🟧	🟥		🟨								🟨	🟨				X							
	KIM	🟧	🟧	🟥	🟧									🟥		🟧					X						
	PM	🟨	🟨	🟧	🟥		🟨					🟨	🟨	🟧								X					
	TM	🟧	🟧	🟥	🟥		🟧							🟥	🟧	🟧							X				
PROCESS MGMT	MON													🟥				🟥	🟥					X			
	OPD																								X	🟨	
	OPF																								🟨	X	
	MA								🟥	🟧														🟥			X

Figure 5.5: Proposed Research Framework – Capabilities Level Linkages-matrix

🟨 Low impact when the interaction between two processes is essentially the same in cloud environments. For instance, the entry **M’SC,OTA** (relationship between the processes SC and OTA); defined as “providing training for staff involved in service continuity plan testing and execution is addressed in the Organizational Training and Awareness process area” (Caralli et al., 2010b, p. 184); may need to modify training content but basically OTA does not require new mechanisms or additional activities in order to support SC. It also means that regardless of the impact that the adoption of CC could have on the SC process, its interaction with the OTA process will not add extra impact.

🟧 Medium impact when the interaction between two processes is partially affected by the CC adoption. For instance, for the entry **M’SC,CTRL;** described as “the development, implementation, and management of an internal control system to prevent risks and disruptive events is addressed in the Controls Management process area” (Caralli et al., 2010b, p. 184); CTRL faces its own changes when establishing control objectives. Therefore, its interaction with SC is also affected. This also means that regardless of the impact that the adoption of CC has on the SC process, its interaction with the CTRL process will add extra impact.

🟥 High impact when the interaction between two processes is very affected by the CC adoption. For instance, for the entry **M’SC,ADM**; described as “the association of assets to the high-value services they support is performed in the Asset Definition and Management process area” (Caralli et al., 2010b, p. 184); ADM faces important changes given that two out of the four types of organisational assets, information and technology, are the assets where CC focuses as an ICT service delivery model and its characteristics are directly related to them. Therefore, its interaction with SC is highly affected. It also means that regardless of the impact that the adoption of CC could have on the SC process, its interaction with the CTRL process will add significant extra impact.

This matrix allows for visual identification of critical research areas based on columns with numerous high impact entries such as risk management (RISK), asset definition and management (ADM), and monitoring (MON). For instances, determining how well the current practices on risk management are aligned to the CC characteristics should be a critical starting point not only because most than half of the processes depend on its capabilities but also because an improvement on this process will multiply its positive impact in the whole system. On the other hand, a column with no high impact entries such as organisational process definition (OPD) or focus (OPF) shows that as a consequences of the adoption of CC as an ICT delivery model, the establishment, maintenance and improvement of organisational processes should need limited additional research efforts, in order to maintain and improve OR.

Similarly rows with numerous high impact entries, such as controls management (CTRL), point out what are the complementary capabilities that an ICT resilience process should consider when working within a cloud environment at first, given the additional and significant impact that these interactions potentially can generate.

5.5 Conclusion

As organisations move their ICT services into CC environments a better understanding of what OR means for this type of environment is required. This paper presents a multi-level research framework designed to address the major issues related to the study of OR in cloud environments from an ICT perspective. The purpose of this framework is to identify the major differences in studying ICT operational resilience within CC environments versus an in-house environment. Therefore, this framework can support the design of a research roadmap from the academic perspective and it can also guide practitioners' efforts in understanding how the adoption of CC can impact the risk of business disruption of an organisation and specifically, the assessment of ICT's operational resilience.

The issues provided in this article are based on a literature review of CC architectures and existing OR specifications. However, it is only a suggested, not all-inclusive, roadmap of current key issues in this area and it is expected that this framework can be used to understand the relationships between CC environments and ICT operational resilience.

5.6 References

American National Standards Institute, I. (2009). Organisational resilience: security, preparedness, and continuity management systems – Requirements with guidance for use – ASIS SPC. 1-2009.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Gunho L., Patterson D., Rabkin A., Stoica I. & Zaharia, M. (2010). A view of cloud computing. *Commununications of the ACM, 53*(4), 50-58. doi: 10.1145/1721654.1721672.

Behrendt, M., Glasner, B., Kopp, P., Dieckmann, R., Breiter, G., Pappe, S., Kreger, H. & Arsanjani, A. (2011). Cloud computing reference architecture v2.0: IBM.

British Standards Institute. (2011). BS ISO/IEC 27031:2011 Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity.

Buyya, R., Ranjan, R., & Calheiros, R. (2010). InterCloud: utility-oriented federation of cloud computing environments for scaling of application services. In C.-H. Hsu, L. Yang, J. Park & S.-S. Yeo (Eds.), *Algorithms and Architectures for Parallel Processing* (Vol. 6081, pp. 13-31): Springer Berlin / Heidelberg.

Cao, C., & Zhan, Z. (2011). *Incident management process for the cloud computing environments.* Paper presented at the 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS).

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). CERT® Resilience management model v1.0: improving operational resilience processes (S. E. Institute, Trans.): Carnegie Mellon.

Chen, Y., Paxson, V., & Katz, R. H. (2010). What's new about cloud computing security?: University of California at Berkeley - Electrical Engineering and Computer Sciences.

Cisco Systems. (2011). Cloud: what an enterprise must know.

Cloud Security Alliance. (2011). Security guidance for critical areas of focus in cloud computing v3.0.

Cloud Security Alliance. (2013). Enterprise architecture v2.0.

Dalziell, E., & McManus, S. (2004). *Resilience, vulnerability and adaptive capacity: implications for system performance*. Paper presented at the International Forum for Engineering Decision Making.

DMTF - Open Cloud Standards Incubator. (2010). Architecture for managing clouds: Distributed Management Task Force.

Dutta, A., Peng, G. c. a., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of its experts. *Journal of Computer Information Systems, 53*(4).

Gibson, C. A., & Tarrant, M. (2010). A ‘conceptual models’ approach to organisational resilience. *The Australian Journal of Emergency Management, 25*(02), 6-12.

Herrera, A., & Janczewski, L. (2013). *Modelling organisational resilience in the cloud.* Paper presented at PACIS 2013 Proceedings. Paper 275.

International Organization for Standardization. (2012). 22301: Societal security - Business continuity management systems - Requirements terms and definitions. Switzerland.

Julisch, K., & Hall, M. (2010). Security and control in the cloud. *Information Security Journal: A Global Perspective, 19*(6), 299-309.

Khasnabish, B., Chu, J., Ma, S., So, N., Unbehagen, P., Morrow, M., Hasan, M., Demchenko, Y. & Meng, Y. (2013). Cloud reference framework: Internet Engineering Task Force.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). SP 500-292: NIST Cloud computing reference architecture. Gaithersburg, MD: US National Institute of Standards and Technology (NIST) - Information Technology Laboratory.

Liu, J., Zhang, L.-J., Hu, B., & He, K. (2012). *CCRA: Cloud computing reference architecture.* Paper presented at the 2012 IEEE Ninth International Conference Services Computing (SCC).

Mahowald, R. P., & Sullivan, C. G. (2012). Worldwide SaaS and cloud software 2012–2016 Forecast and 2011 Vendor Shares: International Data Corporation.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. *Decision Support Systems, 51*(1), 176-189. doi: http://dx.doi.org/10.1016/j.dss.2010.12.006.

Mell, P., & Grance, T. (2011). The NIST Definition of cloud computing special publication (SP) 800-145. Gaithersburg, MD: US National Institute of Standards and Technology (NIST).

National Fire Protection Association. (2004). NFPA 1600 standard on disaster/emergency management and business continuity programs (2013 ed.): NFPA - Technical Committee on Disaster Management.

Oracle Corporation. (2012). Cloud reference architecture.

Peiris, C., Sharma, D., & Balachandran, B. (2011). C2TP: a service model for cloud. *International Journal of Cloud Computing, 1*(1), 3-22.

Rimal, B. P., Jukan, A., Katsaros, D., & Goeleven, Y. (2011). Architectural requirements for cloud computing systems: an enterprise cloud approach. *Journal of Grid Computing, 9*(1), 3-26.

Shim, J., & Lim, Y. (2013). Implementation of real time alert system over cloud computing. *International Journal of Energy, Information & Communications, 4*(3).

Standards Australia/Standards New Zealand. (2010). Business continuity - Managing disruption-related risk (AS/NZS 5050:2010). Sydney & Wellington.

The Open Group. (2011). TOGAF 9.1 *37. Building blocks*: Van Haren Pub.

Xiaohui, L., Jingsha, H., & Ting, Z. (2013). A Service-oriented identity authentication privacy protection method in cloud computing. *International Journal of Grid & Distributed Computing*, *6*(1), 77-86.

Yang, H., & Tate, M. (2012). A descriptive literature review and classification of cloud computing research. *Communications of the Association for Information Systems*, *31*(1), 2.

Zhao, W., Melliar-Smith, P., & Moser, L. E. (2010). *Fault tolerance middleware for cloud computing.* Paper presented at the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD).

6 Resilient Organisations in the Cloud

Cloud computing is a way of delivering computing resources that promises numerous benefits, however, organisations worry about its extra levels of abstraction. This additional complexity represents a hurdle in the assessment of information and communication technologies (ICT) resilience and no consensus exists yet for its analysis. Therefore, CC failures and their effects in organisational resilience (OR) need to be understood. Here, OR is defined as the ability of organisations to survive and also thrive when exposed to disruptive incidents. Aiming to find out what the requirements are for setting up and running an effective ICT operational resilience management system in cloud computing environments (CCE), a conceptual model that helps organisations to maintain and improve OR when working within CCE is being developed. This paper addresses the research design of this investigation focusing on the foundations and challenges of the conceptual model.

6.1 Introduction

Given the rapid adoption of cloud computing environments (CCE) organisations are increasingly relying on computing services being consumed through providers with large data centres and not on in-house environments as was customary some years ago. Industry analysts have predicted an entire transformation of the computing industry based on its potential and accordingly have made billionaire revenue projections (Gartner, 2012; International Data Corporation, 2013; Ried & Kisker, 2011). These predictions also show that before the end of this decade, 80% of organisations will be dependent on cloud services and tens of millions of end-users will be consuming cloud services (Dekker, 2012). In spite of these figures, CCE have also raised various concerns and an increasing number of researchers and practitioners are developing new knowledge from technical to business issues (Yang & Tate, 2012). In the former, issues regarding portability, interoperability and security have been studied (Buyya et al., 2010; Chen et al., 2010). In the latter, researchers have been working specifically on economic impact, costs, reasons for adoption and growth trends (Marston et al., 2011). Specifically, CCE outages are gaining attention because hosting infrastructure across multiple locations spreads the risk of disruption and it is difficult to estimate how many end-users or organisations depend on a cloud provider. To compound this scenario, cloud services can be too complex for consumers to manage and progressively consumers are requesting services from cloud brokers instead of contacting providers directly, making even harder to estimate the full impact of an outage (Dekker, 2012; Dekker, Liveri, & Lakka, 2013; Winkler & Gilani, 2011).

According to the European Network and Information Security Agency (ENISA), this concentration of computing services into few CCE is a double-edged sword "on the one hand, large cloud providers can deploy state-of-the-art security and resilience measures and spread the associated costs across the customers. On the other hand, if an outage or a security breach occurs the consequences could be big, affecting a lot of data, many organisations and a large number of citizens at once" (Dekker, 2012, p. iii). In other words, as computing moves away from onsite data centres to cloud services, organisational resilience (OR) processes become much more complex (Arean, 2013). This specific topic has been identified as one of the main obstacles to and opportunities for the growth of CCE (Armbrust et al., 2010; Badger et al., 2012; Catteddu & Hogben, 2009; Cloud Security Alliance, 2011; Hancock & Hutley, 2012), showing the need to understand CCE failures and their effects in OR. This need is addressed in this research by proposing a conceptual model that represents how the dynamic phenomenon of using CCE as a computing service sourcing model impacts the OR domain (Wand & Weber, 2002).

OR emerged in the field of management in the 1990s as an explanation for the ability of organisations to survive and also thrive when exposed to external shocks such as natural disasters, terrorist attacks and uncertain environments. Scholars have applied this concept to areas such as crisis management (Kendra & Wachtendorf, 2003), disasters management (Dalziell & McManus, 2004; Paton & Johnston, 2001; Stephenson, 2010; Tierney, 2003), high-reliability organisations (Weick & Sutcliffe, 2001; Weick et al., 2008; Woods & Wreathall, 2008) and ICT (Caralli et al., 2010b). In the latter, "mainly to understand how computing systems impact organisational performance, how to assess alternative methods and how to establish essential components" (Herrera & Janczewski, 2013). Practitioners have also contributed to this field through OR/Business continuity (BC) frameworks (American National Standards Institute, 2009; British Standards Institute, 2011; National Fire Protection Association, 2004; Standards Australia/Standards New Zealand, 2010) mainly focusing on how to control organisational behaviour and response during times of disruption. OR is defined as the adaptive capacity in a complex and changing environment that enables an organisation to resist commotions and return to an acceptable level of performance in an acceptable period of time after being affected by an event (Wilson, 2010). Some of these frameworks and studies specifically focus on ICT readiness for OR. Particularly, the Resilience Management Model

(RMM) developed by the Carnegie Mellon University’s Computer Emergency Response Team explicitly suggest to study the impact of CCE adoption on the ICT resilience processes, showing again the relevance of this topic (Caralli et al., 2010b).

This paper is organised into three sections after this introduction. Section two describes how the main stages of this research have been defined by describing the research design. The third section begins by presenting the model’s foundations and its main challenges are briefly described. Finally, the fourth section briefly discusses the current progress and describes further steps.

6.2 Research Design

The main purpose of this paper is to present the model’s foundations, the main challenges that it faces and its high-level representation. However, as this model is part of a research that aims to find out what the requirements are for setting up and running an effective ICT operational resilience management system in CCE, a clearer context is needed. This section presents the research design and places the role of the model in it.

Three main research questions have been identified: (RQ1) How do the main reference architecture characteristics of CCE affect the ICT operational resilience requirements? (RQ2) How should the existing processes and controls be adjusted? (RQ3) What new processes and controls should be created? These research questions are dealing with real-world complexities and in these cases researchers (Adams & Courtney, 2004; Mingers, 2001; Nunamaker et al., 1991), in the field of information systems, have found that in order to achieve richer results a pluralist research approach is desirable because it allows to discover different dimensions. Based on this, the multi-methodological approach proposed by Mingers (2001) has been adopted. This approach argues that “research is not a discrete event but a process that has phases or, rather, different types of activities, which will predominate at different times” (p. 245) and it follows four major phases: appreciation, analysis, assessment and action.

The appreciation phase includes methods that allow the involvement of the researchers in the situation through any actors and prior literature review. The detailed identification of the phenomenon, and the initial conceptualization and design of the study are the main results of this phase. Initially, an exploratory study was proposed aiming to identify new categories of resilience-oriented requirements, however, after a preliminary assessment by researchers and practitioners in the field a different approach was chosen as there has been little research in this area. Thus, following a literature review approach and addressing specifically RQ1, the first study focuses in a conceptual understanding of key issues in the study of OR in CCE. As a result, a research framework designed to provide a roadmap from the academic perspective has been proposed (Herrera & Janczewski, 2014). The framework adopts the cloud definition by the National Institute for Standards and Technology (NIST) (Mell & Grance, 2011) and is constructed from a literature review of CCE derived from well-known reference architectures (Behrendt et al., 2011; Cloud Security Alliance, 2013; Khasnabish et al., 2013; Liu et al., 2011) and a compilation of OR specifications also derived from the most popular OR/BC standards and models (American National Standards Institute, 2009; British Standards Institute, 2011; Caralli et al., 2010b; Standards Australia/Standards New Zealand, 2010). This multi-level framework captures key issues from the macro level of cloud's architectural building blocks to the micro level of organisational resilience capabilities. The macro level captures three dimensions: principles, actors and architecture building blocks focusing on the latter. The micro level analyses linkages among resilience process areas in order to identify dependencies that should be considered when studying a specific process area. This framework specifically contributes to identify the major differences in studying ICT operational resilience within CCE versus an in-house environment. It is also expected to guide practitioners' efforts in understanding how the adoption of CCE impact the risk of business disruption of an organisation and specifically, the assessment of ICT's operational resilience.

Based on the above framework as well as on industry practices and standards, a sub set of processes and activities has been identified as a target to analyse how an organisation can handle disruptive incidents that come from the use of computing power in a CCE. This analysis constitutes the second phase of this research and specifically addresses the other two research questions RQ2 y RQ3. It includes methods to select strategies to propose an explanation of the phenomenon in terms of possible mechanisms or structures and how to improve specific weaknesses. A specific theoretical lens is used in order to understand this phenomenon: coordination theory that is going to be briefly described in the next section of this paper. As a result the main outcome of this research, a conceptual model that helps organisations to maintain and improve OR when working within CCE, from an ICT operational perspective, will be proposed. The foundations and other elements for its design are discussed in more detail in the next section. This study is meant to provide several contributions to both academics and practitioners. From the theoretical perspective, it contributes to an understanding of why coordination is a key element in order to maintain and improve OR within CCE. From a practitioner's perspective, this study specifies processes and mechanisms that show how the coordination concept can be used for improving an organisation's ICT readiness to ensure OR.

For the next phase, an assessment of the model is needed and consequently a third study has been proposed. This study will test the proposed model through the analysis of real incidents in New Zealand companies working within CCE. The main goal of this assessment is to provide a qualitative demonstration through walkthrough and tabletop exercises in order to analyse and improve the model. It will also provide empirical evidence of the role of coordination in achieving resilient organisations in the cloud.

Finally, the approach by Mingers (2001) proposes the "action" phase that intends to disseminate the research results. As Mingers states these four phases are not seen as discrete stages that are enacted one by one, consequently, efforts to achieve this goal have been incorporated in the three studies that are part of this research.

6.3 Conceptual Model

Wand and Weber (2002) define a conceptual model as "an abstract description of an organizational setting (of which part is the represented domain and part is the usage environment)" (p. 286). Following this definition, the conceptual model, which is being proposed by this research, represents how the dynamic phenomenon of using CCE as a computing service sourcing model impacts the OR domain. As this model is the main research outcome, this section addresses three essential aspects of its design: foundations, challenges and finally its high-level representation.

6.3.1 Model's foundations

As part of the second phase, analysis, and based on an extended literature review four foundations for the model have been identified:

F1 - OR General Perspective: In the literature two general perspectives of resilience are recognised: (1) engineering resilience that aims to maximise "the efficiency of systems and processes to return and maintain the system at its desired state" (Dalziell & McManus, 2004, p. 8) and (2) ecological resilience that aims to design "flexible systems and processes that continue to function in the face of disturbances" (Dalziell & McManus, 2004, p. 8). From an organisational perspective, "increasing the ecological resilience would increase the magnitude of consequences that an organisation could withstand before suffering irreparable damage"

(Dalziell & McManus, 2004, p. 8) and as this study is aiming to propose a conceptual model to continually improve the effectiveness of an organisation's resilience, an ecological resilience approach has been adopted.

F2 - Types of Activities: As stated before OR is the result of harmonic and convergent efforts to adapt to and thrive from disruptive incidents (in this research disruptive incidents that come from the use of computing power in a CCE). Thus, OR includes both developmental and operational activities in order to prevent; to stabilise, to continue critical services, to recover and manage consequences; and to improve activities, as shown in Figure 6.1.

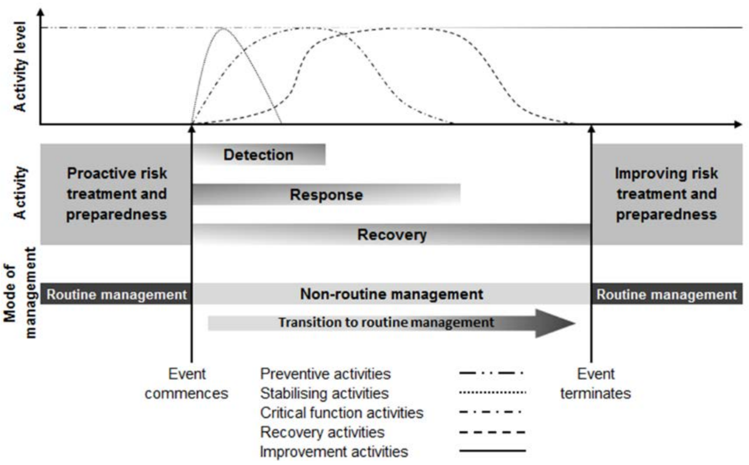


Figure 6.1: Activities vs. Incident Stages (Herrera & Janczewski, 2014, p. 36)

The first type of activities, preventive activities, deals with strategies designed to minimize an asset's exposure to sources of disruption; examples of such activities are processes, procedures, policies and controls. The second type, continue and management consequences activities, includes stabilising, continuing critical functions and recovering activities. Thus, it focuses on strategies designed to keep assets operating as close to normal as possible when facing disruptive incidents, through strategies such as processes, procedures, polices, plans and controls and, also, on strategies that are aimed at returning to routine operations and a full recovery as soon as possible. Lastly, improvement activities translate into strategies designed to achieve continual improvement by correcting and/or adopting new strategies of both previous types. Dependencies and coordination mechanisms among these types of activities when working in CCE are the focus of the model.

F3 - Underlying Theory for Analysing Activities: One of the main differences between a traditional in-house ICT environment and a CCE is the degree of control over the services. In the former, an organisation has control over the whole stack while in the latter; all actors collaboratively design, build, deploy, and operate the system. More important, all parties share the responsibility in providing the environment with adequate protections, creating dependencies. In Malone and Crowston (1994)'s view, actors in organisations face coordination problems arising from dependencies. Essentially their framework defines coordination as "managing dependencies" and defines coordination theory as "a body of principles about how activities can be coordinated, that is, about how actor can work together harmoniously" (Malone & Crowston, 1990, p. 358). Based on coordination theory and specifically in a taxonomy of organisational dependencies developed by Crowston (1994) that defines three main types of dependencies: synchronisation, resource allocation and goal decomposition; this study focuses on analysing dependencies and coordination mechanisms among ICT resilience processes in CCE.

F4 - Specific ICT Resilience Processes: The RMM has been explicitly adopted by this research given the emphasis on ICT readiness for OR. This model manages ICT operational resilience across three disciplines: security management, business continuity and ICT operations management. It has 26 process areas that are organised into four high-level categories: engineering, enterprise management, operations, and process management (see Figure 6.2) (Caralli et al., 2010b). It also defines six levels of maturity: incomplete, preferred, managed, defined, quantitatively managed, and optimised.

Based on the research framework (Herrera & Janczewski, 2014) specific areas of concern have been identified at both levels: macro and micro. At the macro level, the framework clusters the 26 process areas mainly into two architecture building blocks (ABBs): (1) the "business management" block that is divided into two sub-blocks: the "business support services (BSS)" deals with business-related services that provides monitoring and administration of the CCE to keep it operating normally and the "ICT operation and support (ICTOS)" groups a set of technical and operational management services in order to keep the systems going even in the event of a disaster. Many resilience concerns arise in this ABB, specifically, the need to extend traditional ICT governance knowledge to cloud governance (Peiris et al., 2011) involving business partners in order to establish a robust communication plan over the life of the relationship (Rimal et al., 2011). It also highlights the importance of establishing processes in order to identify and analyse events, detect incidents, and determine an appropriate coordinated response is considered critical in CCE (Cao & Zhan, 2011). (2) The "operational risk and consumability" block that compiles non-functional aspects across the CCE providing a solid context for operations and support collects non-functional aspects that should be viewed from an end-to-end perspective in order to provide the core components to safeguard cloud services. The framework highlights that research areas focusing on the strengthening of resilience capacities to (1) determine appropriate requirements, control selection and oversee continuity of operations (Julisch & Hall, 2010) and (2) ensure that the consumer organisation has the capability to manage the risk of unmet requirements from providers and brokers (Dutta et al., 2013) should be considered.

Enterprise management	**Operations**
Communications [COMM] Compliance Management [COMP] Enterprise Focus [EF] Financial Resource Management [FRM] Human Resource Management [HRM] Organizational Training and Awareness [OTA] Risk Management [RISK]	External Dependency Management [EXD] Access Management [AM] Identity Management [ID] Incident Management and Control [IMC] Vulnerability Analysis and Resolution [VAR] Environmental Control [EC] Knowledge and Information Management [KIM] People Management [PM] Technology Management [TM]
Process management	**Engineering**
Monitoring [MON] Organizational Process Definition [OPD] Organizational Process Focus [OPF] Measurement and Analysis [MA]	Resilience Requirements Development [RRD] Resilience Requirements Management [RRM] Asset Definition and Management [ADM] Controls Management [CTRL] Resilient Technical Solution Engineering [RTSE] Service Continuity [SC]

Figure 6.2: RMM Processes by High-level Categories (Herrera & Janczewski, 2014, p. 37)

At the micro level, the framework analyses linkages among resilience process areas in order to identify dependencies that should be considered when pursuing a specific resilience-related objective. In the context of this research and supporting F1 to F3, this objective is closely related to the establishment of processes in order to identify and analyse events, detect incidents, and determine an appropriate coordinated response. From this perspective, the RMM identifies seven process areas that drive threat and incident management (Caralli et al., 2010b), as shown in Figure 6.3. Therefore, this last foundation narrows down the scope of this research focusing on core activities and mechanisms within these seven processes: control management (CTRL), enterprise focus (EF), incident management and control (IMC), monitoring (MON), risk management (RISK), service continuity (SC) and vulnerability analysis and resolution (VAR).

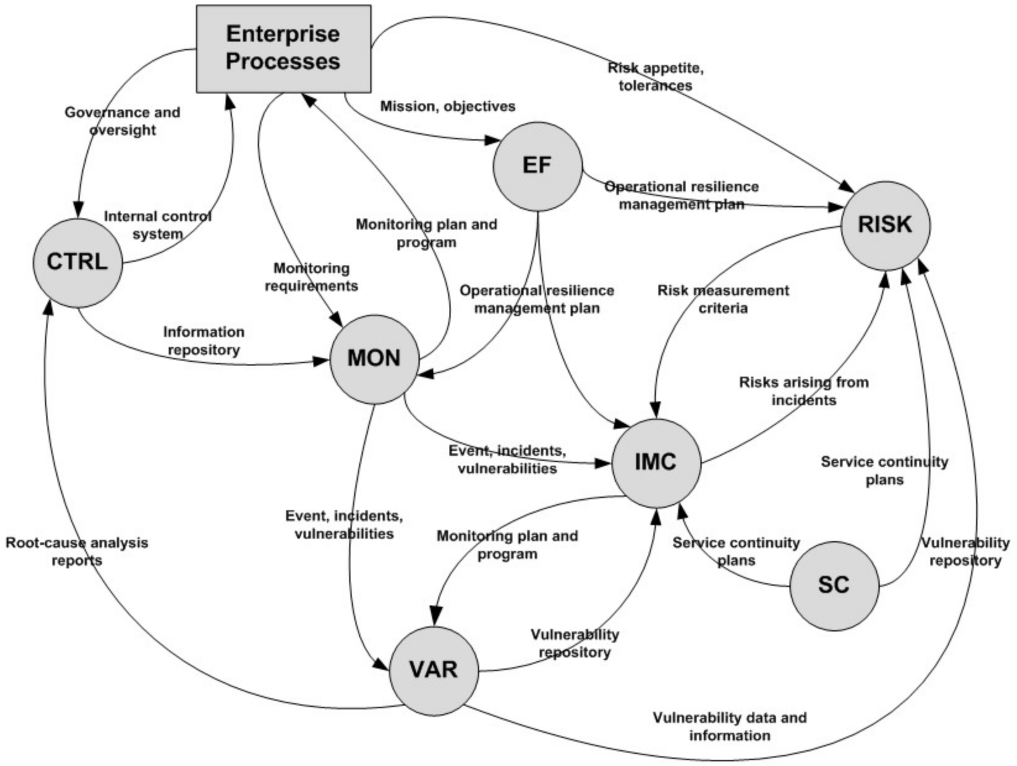

Enterprise Processes
Risk appetite, tolerances
Governance and oversight
Mission, objectives
EF
Operational resilience management plan
RISK
Internal control system
Monitoring plan and program
CTRL
Monitoring requirements
Operational resilience management plan
Risk measurement criteria
Information repository
MON
Risks arising from incidents
Event, incidents, vulnerabilities
IMC
Service continuity plans
Event, incidents, vulnerabilities
Root-cause analysis reports
Monitoring plan and program
Service continuity plans
Vulnerability repository
SC
Vulnerability repository
VAR
Vulnerability data and information

Figure 6.3: Relationship that Drive Incident Management (Caralli et al., 2010b, p. 45)

6.3.2 Model's challenges and its associated objectives

Thus far, the domain for the conceptual model has been explicitly identified by stating the four foundations and it is time to refocus on how the main characteristics of CC impact ICT operational resilience and therefore what are the challenges that the model is facing. Based on prior research (Almorsy, Grundy, & Ibrahim, 2011; Grobauer & Schreck, 2010; Kaliski Jr & Pauley, 2010; Wahlgren & Kowalski, 2013) and focusing on the cloud computing's five essential characteristics defined by the NIST (Badger et al., 2012), this study identifies and analyses specific OR-related challenges for CCE. A brief overview is presented in Table 6.1.

Characteristic	Definition	Challenge
On-demand self-service	A consumer can unilaterally provision computing capabilities	No human interaction takes away an important control mechanism
Broad network access	Capabilities are available over the network and accessed through heterogeneous client platforms	From a relatively static ICT landscape to a dynamic collection of end points of varying resilience needs and capabilities
Resource pooling	Computing resources are pooled to serve multiple consumers using a multi-tenant model	Resources are not known a priori and therefore cannot be assessed in advance
		Logical entities are subject to consumer's requirements and physical resources are mainly responsibility of the provider
		Each tenant may assign different impact levels (Low, Medium, or High) to incidents
		The dynamic resource allocation plus the variability of external requirements mean that an assessment is not possible based only on a priori model of the ICT environment
Rapid Elasticity	Capabilities can be rapidly and elastically provisioned to scale commensurate with demand	Need to handle increasing workloads among different clouds
		The assessment should cover the consumer and the specific provider and the provider's brokers, and so on recursively
Measured service	Resource usage can be monitored, and controlled providing transparency for both the provider and consumer	It implies much finer detail given the focus on cost and dynamic resource sharing

Table 6.1: Organisational Resilience Challenges by Cloud Computing Characteristics

These challenges have specific implications for each type of OR-Incident-Management activities in the model: For the first group, preventive activities, OR standard practices such as risk analysis and business impact should be focused on the correctness of the allocation mechanisms and the qualities of the overall pool of resources, instead of analysing deployed resources for a given ICT service. For the second group of activities, continue and management consequences activities, the model will be focused on mechanisms to generate and process event information in order to detect relevant events and activate appropriate OR strategies among actors when needed. For the last group of activities, continual improvement, the model will be focused on mechanisms to monitor the performance of all the other mechanisms. These implications have been inferred from the problem definition and the described foundations and constitute the objectives for the model.

6.3.3 High-level conceptual model

The high-level graphical representation of the conceptual model is presented in Figure 6.4. This model plus the foundations, challenges and objectives are being preliminarily assessed in order to obtain early feedback and if needed, it would be refined as briefly discussed in the final section of this paper. This preliminary assessment is considered part of the third stage of this research.

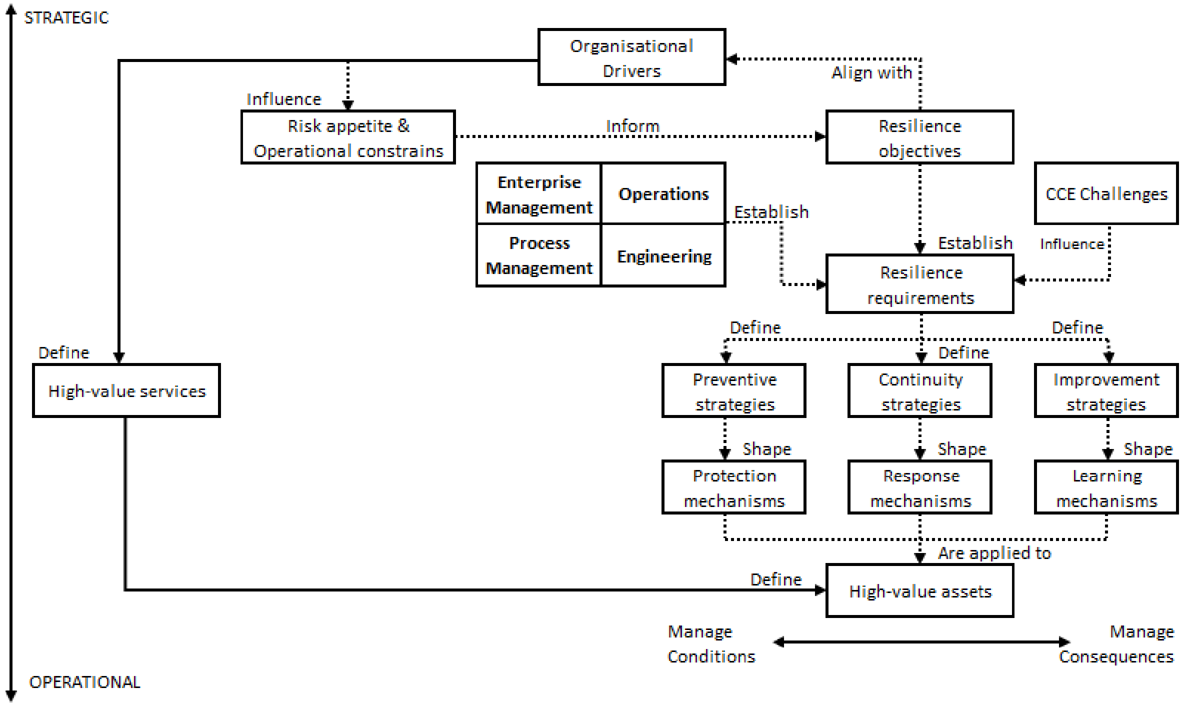


Figure 6.4: Model’s baseline

6.4 Discussion and Further Research

This research aims to find out what the requirements are for setting up and running an effective ICT operational resilience management system in CCE by studying the dependencies among incident management driven processes and their respective coordination mechanisms. This paper has presented the research design and specifically has stated the baseline to design the conceptual model, main contribution of this research. This baseline and the high-level model are being currently assessed by conducting semi-structured interviews with a small group of experts around the world. The data gathering stage has been completed and the data analysis is half way through. The following steps will be to refine the baseline, as required, and to propose the conceptual model accordingly. So far, two other process areas are starting to play an important role for the model: communications (COMM) and compliance management (COMP). The first one broadly addresses the way in which an organisation develops, deploys and manages internal and external communication to support resilience processes and given that in CCE all actors collaboratively design, build, deploy, and operate the system more elaborate communication schemes may be necessary. In the second case, COMP is focused on ensuring compliance with the relevant internal and external standards, legislation and other obligations. These findings among others are being analysed in order to define the final baseline and focus on the model itself. Finally, as soon as the model is ready the third study, main part of the assessment stage, will be conducted as described in the research design section.

This research is following a rigorous multi-method approach that so far has shown its benefits by providing a more comprehensive context of the research. It is expected to provide valuable contributions to both academics and practitioners. From the theoretical perspective, contributes to an understanding of the role of coordination in making resilient organisations in the cloud. From a practitioner’s perspective, this study specifies mechanisms that can be used for planning and decision-making to prevent, to respond and to learn from ICT disruptive incidents.

6.5 References

Adams, L. A., & Courtney, J. F. (2004, 5-8 Jan. 2004). Achieving relevance in IS research via the DAGS framework. Paper presented at the HICSS, 2004. Proceedings of the 37th Annual Hawaii International Conference on System Sciences.

Almorsy, M., Grundy, J., & Ibrahim, A. S. (2011). Collaboration-based cloud computing security management framework. Paper presented at the 2011 IEEE International Conference on Cloud Computing (CLOUD).

American National Standards Institute, I. (2009). Organisational resilience: security, preparedness, and continuity management systems – Requirements with guidance for use – ASIS SPC. 1-2009.

Arean, O. (2013). Disaster recovery in the cloud. Network Security, 2013(9), 5-7.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Gunho L., Patterson D., Rabkin A., Stoica I. & Zaharia, M. (2010). A view of cloud computing. *Commununications of the ACM, 53*(4), 50-58. doi: 10.1145/1721654.1721672.

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). SP 800-146: Cloud computing synopsis and recommendations.

Behrendt, M., Glasner, B., Kopp, P., Dieckmann, R., Breiter, G., Pappe, S., Kreger, H. & Arsanjani, A. (2011). Cloud computing reference architecture v2.0: IBM.

British Standards Institute. (2011). BS ISO/IEC 27031:2011 Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity.

Buyya, R., Ranjan, R., & Calheiros, R. (2010). InterCloud: utility-oriented federation of cloud computing environments for scaling of application services. In C.-H. Hsu, L. Yang, J. Park & S.-S. Yeo (Eds.), Algorithms and Architectures for Parallel Processing (Vol. 6081, pp. 13-31): Springer Berlin / Heidelberg.

Cao, C., & Zhan, Z. (2011). *Incident management process for the cloud computing environments.* Paper presented at the 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS).

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). CERT® Resilience management model v1.0: improving operational resilience processes (S. E. Institute, Trans.): Carnegie Mellon.

Catteddu, D., & Hogben, G. (2009). Cloud computing: benefits, risks and recommendations for information security: European Network and Information Security Agency.

Chen, Y., Paxson, V., & Katz, R. H. (2010). What’s new about cloud computing security? : University of California at Berkeley - Electrical Engineering and Computer Sciences.

Cloud Security Alliance. (2011). Security guidance for critical areas of focus in cloud computing V3.0.

Cloud Security Alliance. (2013). Enterprise architecture v2.0.

Crowston, K. (1994). A taxonomy of organizational dependencies and coordination mechanisms: Center for Coordination Science, Alfred P. Sloan School of Management, Massachusetts Institute of Technology.

Dalziell, E., & McManus, S. (2004). Resilience, vulnerability and adaptive capacity: implications for system performance. Paper presented at the International Forum for Engineering Decision Making.

Dekker, M. (2012). Critical cloud computing: a CIIP perspective on cloud computing services: European Network and Information Security Agency (ENISA).

Dekker, M., Liveri, D., & Lakka, M. (2013). Cloud security incident reporting: framework for reporting about major cloud security incidents: European Network and Information Security Agency (ENISA).

Dutta, A., Peng, G. c. a., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of its experts. Journal of Computer Information Systems, 53(4).

Gartner. (2012). Gartner says worldwide cloud services market to surpass $109 billion in 2012 [Press release]. Retrieved from http://www.gartner.com/newsroom/id/2163616

Grobauer, B., & Schreck, T. (2010). Towards incident handling in the cloud: challenges and approaches. Paper presented at the Proceedings of the 2010 ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA.

Hancock, I., & Hutley, N. (2012). Modelling the economic impact of cloud computing: KPMG and Australian Information Industry Association (AIIA).

Herrera, A., & Janczewski, L. (2013). Modelling organisational resilience in the cloud. Paper presented at the PACIS 2013 Proceedings. Paper 275.

Herrera, A., & Janczewski, L. (2014). Issues in the study of organisational resilience in cloud computing environments. *Procedia Technology, 16*(0), 32-41. doi: http://dx.doi.org/10.1016/j.protcy.2014.10.065.

International Data Corporation. (2013). Worldwide and regional public it cloud services 2013–2017 forecast [Press release]. Retrieved from http://www.idc.com/getdoc.jsp?containerId=242464

Julisch, K., & Hall, M. (2010). Security and control in the cloud. Information Security Journal: A Global Perspective, 19(6), 299-309.

Kaliski Jr, B. S., & Pauley, W. (2010). Toward risk assessment as a service in cloud environments. Paper presented at the Proceedings of the 2nd USENIX conference on Hot topics in cloud computing.

Kendra, J. M., & Wachtendorf, T. (2003). Elements of resilience after the world trade center disaster: reconstituting New York City's Emergency Operations Centre. Disasters, 27(1), 37-53.

Khasnabish, B., Chu, J., Ma, S., So, N., Unbehagen, P., Morrow, M., Hasan, M., Demchenko, Y. & Meng, Y. (2013). Cloud reference framework: Internet Engineering Task Force.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). SP 500-292: NIST Cloud computing reference architecture. Gaithersburg, MD: US National Institute of Standards and Technology (NIST) - Information Technology Laboratory.

Malone, T., & Crowston, K. (1990). What is coordination theory and how can it help design cooperative work systems? Paper presented at the Proceedings of the 1990 ACM conference on Computer-supported cooperative work.

Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. ACM Comput. Surv., 26(1), 87-119. doi: 10.1145/174666.174668.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. Decision Support Systems, 51(1), 176-189. doi: http://dx.doi.org/10.1016/j.dss.2010.12.006.

Mell, P., & Grance, T. (2011). The NIST Definition of cloud computing special publication (SP) 800-145. Gaithersburg, MD: US National Institute of Standards and Technology (NIST).

Mingers, J. (2001). Combining IS research methods: towards a pluralist methodology. Information systems research, 12(3), 240-259.

National Fire Protection Association. (2004). NFPA 1600 standard on disaster/emergency management and business continuity programs (2013 ed.): NFPA - Technical Committee on Disaster Management.

Nunamaker, J., Chen, M., & Purdin, T. D. M. (1991). Systems development in information systems research. Journal of Management Information Systems, 7(3), 89-106.

Paton, D., & Johnston, D. (2001). Disasters and communities: vulnerability, resilience and preparedness. Disaster Prevention and Management, 10(4), 270-277.

Peiris, C., Sharma, D., & Balachandran, B. (2011). C2TP: a service model for cloud. International Journal of Cloud Computing, 1(1), 3-22.

Ried, S., & Kisker, H. (2011). Sizing the cloud: understanding and quantifying the future of cloud computing: Forrester.

Rimal, B. P., Jukan, A., Katsaros, D., & Goeleven, Y. (2011). Architectural requirements for cloud computing systems: an enterprise cloud approach. Journal of Grid Computing, 9(1), 3-26.

Standards Australia/Standards New Zealand. (2010). Business continuity - Managing disruption-related risk (AS/NZS 5050:2010). Sydney & Wellington.

Stephenson, A. V. (2010). Benchmarking the resilience of organisations. (Doctoral thesis), University of Canterbury, Christchurch.

Tierney, K. J. (2003). Conceptualizing and measuring organizational and community resilience: lessons from the emergency response following the September 11, 2001 attack on the World Trade Center.

Wahlgren, G., & Kowalski, S. (2013). IT security risk management model for cloud computing: a need for a new escalation approach. Paper presented at the The International Conference on Digital Information Processing, E-Business and Cloud Computing (DIPECC2013).

Wand, Y., & Weber, R. (2002). Research commentary: information systems and conceptual modeling - A research agenda. Information systems research, 13(4), 363-376.

Weick, K. E., & Sutcliffe, K. M. (2001). Managing the unexpected: assuring high performance in an age of complexity. 2001. University of Michigan Business School Management Series.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: processes of collective mindfulness. Crisis management, 3, 81-123.

Wilson, R. L. (2010). Organizational resilience models applied to companies in bankruptcy. (Doctor of Management), University of Maryland University College, United States -- Maryland.

Winkler, U., & Gilani, W. (2011). Model-Driven framework for business continuity management service level agreements for cloud computing (pp. 227-250): Springer.

Woods, D. D., & Wreathall, J. (2008). Stress-strain plots as a basis for assessing system resilience. Resilience Engineering: Remaining Sensitive to the Possibility of Failure, 143-158.

7 Cloud Supply Chain Resilience: A Coordination Approach

Cloud computing is a service-based computing resources sourcing model that is changing the way in which companies deploy and operate information and communication technologies (ICT). This model introduces several advantages compared with traditional environments along with typical outsourcing benefits reshaping the ICT services supply chain by creating a more dynamic ICT environment plus a broader variety of service offerings. This leads to higher risk of disruption and brings additional challenges for organisational resilience, defined herein as the ability of organisations to survive and also to thrive when exposed to disruptive incidents. This paper draws on supply chain theory and supply chain resilience concepts in order to identify a set of coordination mechanisms that positively impact ICT operational resilience processes within cloud supply chains and packages them into a conceptual model.

7.1 Introduction

Cloud computing is an increasingly popular information and communication technology (ICT) sourcing model that introduces several advantages compared with traditional environments, such as dynamic scalability, rapid resource provisioning and the ability to pay for use on a short-term basis, along with typical outsourcing benefits such as operational cost savings. Based on its potential, industry analysts have predicted a complete transformation of the computing industry (Gartner, 2012; International Data Corporation, 2013; Staten et al., 2014). For example, it is expected that before the end of this decade, 80% of organisations will be dependent on cloud services and tens of millions of end users will be consuming cloud services (Dekker, 2012). In addition to these predictions, cloud computing environments (CCE) have also raised various concerns and an increasing number of researchers and practitioners are investigating both the technical and business issues involved (Willcocks et al., 2013b; Yang & Tate, 2012). These new and highly dynamic environments offer a broader variety of services and are reshaping the ICT services supply chain, making it larger and more complex with globally dispersed components (Lindner et al., 2010). Such environments represent more risks to consumers (Dekker et al., 2013; Winkler & Gilani, 2011), of course, but they also pose more risks to providers who are responsible for services outside their direct control. Effective supply chain management in this type of environment is a challenging task that can be even more difficult when facing unexpected disruptions. These disruptions can be found in a variety of forms from natural disasters to operational issues and if poorly handled can affect many consumer organisations and countless users (Dekker, 2012). In other words, cloud sourcing is on the rise, and because this type of dynamic and greatly distributed supply chain increases the potential of disruption, there is a need to strengthen the ability of organisations to not only survive but also to thrive when exposed to disruptive incidents within a CCE (Arean, 2013; IBM Global Technology Services, 2014).

Such an ability is referred to as organisational resilience (OR), which has been formally defined as “the ability of an organization to anticipate, prepare for, and respond and adapt to everything from minor everyday events to acute shocks and chronic or incremental changes” (British Standards Institute, 2014, p. 1). According to this definition, OR is a goal, not a fixed activity or state, and is enhanced by coordinating various operational disciplines that an organisation might have already implemented, such as risk management, business continuity management, crisis management, ICT readiness for OR, among others (Cockram, 2012). In addition, as an organisation interacts with other organisations it is essential to build resilience not only within the organisation but also across its networks. Therefore, an organisation needs to build resilience in partnership with others (Morisse & Prigge, 2014), particularly when some of its processes have moved outside the traditional organisational boundaries, as is the case with CCE.

Focusing on the ICT readiness for OR discipline and given that in a CCE all the supply chain actors collaboratively design, build, deploy and operate the system, and “all parties share the responsibilities in providing it with adequate protections” (Herrera & Janczewski, 2014, p. 35), the main objective of this paper is to understand how ICT resilience activities can best be coordinated across the cloud supply chain (CSC) in order to make this supply chain become more resilient. To explore this research problem, this paper draws insights from existing supply chain management theory and supply chain resilience concepts and considers specific characteristics of the CSC in order to identify coordination mechanisms that positively impact ICT operational resilience processes within this chain. A key concept driving this investigation is the notion of coordination, which can be defined as “managing dependencies among activities” (Malone & Crowston, 1994, p. 97). From this perspective, this paper understands coordination as “the essence of supply chain management” (Arshinder, Kanda, & Deshmukh, 2011; Fugate, Sahin, & Mentzer, 2006) and sees coordination mechanisms as tools for effectively managing dependencies among supply chain members (Xu & Beamon, 2006, p. 4).

The main contribution of this paper is a structured set of categories of coordination mechanisms for enhancing CSC resilience which are packaged into a conceptual model. From the theoretical perspective, it contributes to the existing body of knowledge by using established supply chain management and supply chain resilience concepts in order to deal with supply chain disruptions in the context of CCE. In addition, the conceptual model can be used as an instrument for managing ICT operational resilience knowledge within CSC. From a practitioner's perspective, this paper identifies categories of coordination mechanisms that can be used to select specific coordination mechanisms in order to manage dependencies throughout the different stages of a disruptive event. The paper is organized as follows. After this introduction, section II links the main components in the domain of interest with the supply chain approach. Section III then illustrates how this approach can be applied in the CSC context, and based on this the proposed conceptual model is presented. Finally, section IV presents conclusions and describes further research.

7.2 Linking the Research Domain and the Theoretical Lenses

This study is bounded by the domains of OR and CCE. Firstly, this section presents a brief overview of OR, focusing on the ICT operational resilience discipline and reviewing relevant literature. Second, literature relating to ICT services supply chains is reviewed and the concept of CSC and its main characteristics are introduced. Finally, the research approach is outlined and the theoretical concepts employed are linked to the research problem.

7.2.1 Organisational resilience – OR

Few areas of life have not been touched in one way or another by the resilience concept. It emerged from the field of ecology in the 1960s (Holling, 1973) but remains difficult to define due to its multiple interpretations. Nevertheless, researchers recognise resilience as a theoretical concept that may be viewed as a property or quality that enables a system (individual, organisation or community) to adapt and recover from a disturbance (Carpenter et al., 2001; Klein et al., 2003; The Resilience Alliance, 2012). Two general types of resilience are recognised: engineering resilience and ecological resilience. The first type focuses on efficiency while the second type focuses on persistency (Holling, 2010).

In the management literature, the concept of OR emerged in the 1990s as an explanation for the ability of organisations to survive and also to thrive when exposed to either external shocks such as natural disasters, terrorist attacks and uncertain environments (Weick et al., 1999;

Wilson, 2010); or operational risks such as equipment malfunctions and discontinuities in supply (Kleindorfer & Saad, 2005) that in one way or another can challenge their ability to get finished goods to market and provide services to customers. The survival part of this ability is generally associated with the engineering type of resilience that aims to maximise "the efficiency of systems and processes to return and maintain the system at its desired state" (Dalziell & McManus, 2004, p. 8) through preventive, detective, response and recovery activities. The second part of this ability, to thrive, is associated with the ecological type of resilience that aims to design "flexible systems and processes that continue to function in the face of disturbances" (Dalziell & McManus, 2004, p. 8) through learning activities in order to develop organisational adaptive capabilities. These activities will be discussed in more detail in section III and will be directly associated with the different stages of a disruptive event.

As part of OR, ICT operational resilience is defined as the ability of an organisation to support its high-value business services by prevention, detection and response to disruption and recovery from ICT services incidents (British Standards Institute, 2011; Caralli et al., 2010b; Maurer & Lechner, 2014). In order to do so, ICT operational resilience requires the organisation to establish resilience requirements based on organisational drivers, risk tolerances, and enterprise-level OR goals (Caralli et al., 2010b). However, an analysis of the information systems (IS) literature revealed that while disruptions and methods to keep businesses in ICT-based interorganisational networks running have not been greatly studied (Morisse & Prigge, 2014), the need for novel concepts for ICT and OR planning when using new ICT sourcing models such as cloud computing has been recognized (Caralli et al., 2010b; Maurer & Lechner, 2014; Morisse & Prigge, 2014). From the management perspective, some resilience-related issues of cloud environments have been studied such as incident management (Cao & Zhan, 2011; Grobauer & Schreck, 2010), risk management (Dutta et al., 2013; Kaliski Jr & Pauley, 2010; Martens & Teuteberg, 2011; Saripalli & Walters, 2010; Troshani & Wickramasinghe, 2011), real-time monitoring (Shim & Lim, 2013; Spring, 2011a), and the mechanisms that organisations are using to enhance OR among interorganisational ICT relationships (Järveläinen, 2012). Based on the above, this research is set in the context of how the ICT operational resilience discipline is affected by using CCE as an ICT services sourcing model.

7.2.2 ICT services supply chains

In the ICT services arena researchers have explored the supply chain concept in terms of traditional software implementation supply chains, service-based delivery model supply chains such as application-as-a-service and, most recently, the cloud computing context. For the traditional software implementation supply chains, Baxter and Simmons (2001) proposed the concept of a software supply chain referring to the whole process of software products moving through design, development and delivery to the end user. Using this definition, a number of authors have explored supply chain concepts such as the issues relating to a product-software supply chain versus those relating to a "traditional trades" supply chain (Chou, Ye, & Yuan, 2005); approaches to improve the coordination of software life cycle processes across the supply chain (Oberhauser & Schmidt, 2007); and a systemic risk management approach across software supply chains (Alberts, Dorofee, Creel, Ellison, & Woody, 2011; Du et al., 2013). For service-based delivery model supply chains, authors have focused on different coordination strategies and information-sharing mechanisms between application-service-providers and application-infrastructure-providers in order to improve the design and performance of a software-as-a-service supply chain (Demirkan, Cheng, & Bandyopadhyay, 2010; Yan, Guo, & Schatzberg, 2012). Lastly, researchers have also explored supply chain concepts in the context of CCE. As the focal ICT sourcing model of this research, the concept of CSC, its main characteristics, and the relevant research in this topic are described below.

Cloud computing is defined as a ICT sourcing model for enabling convenient, on-demand network access to a shared pool of easily accessible and usable virtualised resources (Mell & Grance, 2011, p. 2). This model has three fundamental components: (1) five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service; (2) three service delivery models: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS); and (3) four deployment models describing how these services can be shared: private cloud, community cloud, public cloud, and hybrid cloud. From the resilience perspective these three main components raise OR concerns. However, it has been argued (Herrera, Beltran, & Janczewski, 2014) that the main cloud OR challenges are derived from its characteristics because the key novelty of cloud, compared to other ICT service-based models, is its highly dynamic environment. In addition, Herrera and Janczewski (2014) identify three main types of actors interacting in a CSC:

- Consumer: an organisation that has a relationship with, and consumes a single or composite service delivered from a particular cloud provider over the CSC.
- Provider: organisation responsible for making a service available to interested parties and might be directly in contact with cloud consumers.
- Broker: an entity that combines or enriches a cloud service to create a composite cloud service; a specific type of provider that is responsible for designing, creating, packaging, and deploying cloud services for consumers' consumption.

The arrangement described above creates a setup that is typical of a supply chain insofar as cloud consumers obtain their services from providers who in turn depend on other providers to provide that service. Thus, in a CSC a disruption to one service immediately disrupts the interdependent services, resulting in a disruption to the overall service delivered to the cloud consumer, which could impact business services and potentially lead to organisational damage (Oppenheimer et al., 2003).

An extensive search of existing literature in the key information systems databases – IEEE Xplore, ACM, AISNET, ScienceDirect, BSP and ABI/INFORM – revealed that two studies have explored the concept of cloud computing as a supply chain (Fischer & Turner, 2009; ISACA, 2012) and that Lindner et al. (2010) first formally defined CSC as "two or more parties linked by the provision of cloud services, related information and funds" (p. 3) (Figure 7.1). However, the search also revealed that only a few studies have begun to apply supply chain concepts in the cloud context. Specifically, these studies have explored the requirements that need to be considered for migrating from a traditional ICT environment to a CCE (Lindner, McDonald, Conway, et al., 2011); discussed well-known concepts in supply chain theory such as the "bullwhip effect" (Lindner, McDonald, McLarnon, & Robinson, 2011; Lindner, Robinson, McLarnon, & McDonald, 2011) and the procurement process (Schrödl & Bensch, 2013); and identified the major coordination strategies used by both cloud service providers and consumers in ensuring successful design and performance of the supply chain (Simmonds, Collins, & Berndt, 2010). These studies all use known problems in traditional supply chains to identify problem areas and mitigation techniques in the context of CCE.

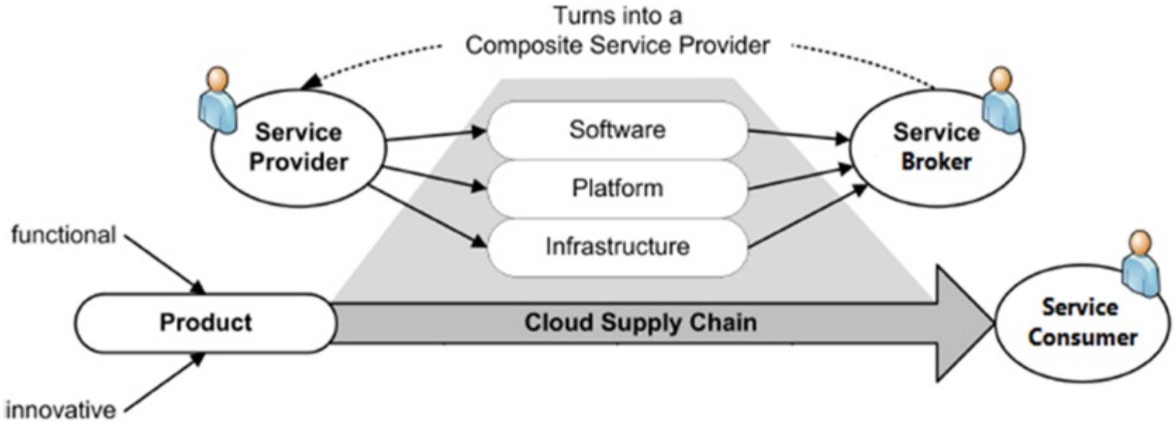


Figure 7.1: Cloud Supply Chain Definition (Lindner et al., 2010, p. 4)

How to manage CSC disruptions in order to meet CSC members' requirements is the main interest of this research. Based on this review of the literature and because disruptions have been extensively studied in traditional supply chains (Christopher, 2004; Christopher & Peck, 2004; Kleindorfer & Saad, 2005; Pettit et al., 2010; Ponomarov & Holcomb, 2009; Sheffi, 2005; Soni et al., 2014) given their critical nature, this study proposes to address the problem of resilience in CCE by adopting a supply chain approach. The last part of this section presents an overview of supply chain resilience concepts.

7.2.3 A Supply Chain Coordination Approach

A final key concept driving this work is the notion of coordination. This concept has repetitively appeared in the literature of both ICT services supply chains and traditional supply chains. Problems that arise from dependencies are referred to in the literature as coordination problems, in fact, Malone and Crowston (1994) define coordination as managing dependencies. Malone and Crowston (1994) and Crowston and Osborn (2003) introduce coordination theory as a framework for analysing complex processes in terms of actors performing interdependent activities. This theory identifies two types of activities within a process: “activities that directly contribute to the output of the process” (Simatupang et al., 2004, p. 257) and additional activities which, as coordination mechanisms, must be carried out in order to manage interdependencies among the first type of activities. Based on the above, disciplines such as emergency response have analysed coordination patterns occurring in the emergency response life cycle (Chen et al., 2008; Franke, Charoy, & El Khoury, 2013). In addition, supply chain management sees coordination within a supply chain “as a strategic response to the problems that arise from inter-organisational dependencies within the chain” (Xu & Beamon, 2006, p. 4) and coordination mechanisms as tools for effectively managing dependencies among supply chain members.

A specific problem that can arise from dependencies is the problem of disruption. In the supply chain literature an increasing interest in studying disruptions has led to the theorising of disruption management and its relation to supply chain resilience (Christopher & Peck, 2004; Kleindorfer & Saad, 2005; Pettit et al., 2010; Ponomarov & Holcomb, 2009; Sheffi, 2005; Soni et al., 2014). Supply chain resilience has been defined as "the adaptive capability of the supply chain to prepare for unexpected events, respond to disruptions, and recover from them" (Ponomarov & Holcomb, 2009, p. 131). A range of terms have been used to describe the elements that facilitate the attainment of resilience in a supply chain (Christopher & Peck, 2004; Kleindorfer & Saad, 2005; Pettit et al., 2010; Ponomarov & Holcomb, 2009; Sheffi, 2005; Soni et al., 2014). Specifically, Christopher and Peck (2004) define four principles that underpin resilience in a supply chain:

1. Supply chain (re)engineering: typically supply chains have been designed to optimise costs and customer service but are rarely designed to increase resilience. In this sense, the authors suggest that resilience should be "designed-in" to minimise, when possible, a supply chain's exposure to sources of disruption. This principle is enhanced by having a good understanding of the supply chain network, analysing multi-sourcing supplier environments and/or single supplier environments with multiple sites, and applying re-engineering practices to continuously improve resilience. Other authors have also recognised these elements as resilience enablers: knowing the supply chain structure (Soni et al., 2014); allowing for flexible and redundant strategies (Sheffi, 2005; Soni et al., 2014); and organisational learning (Pettit et al., 2010; Ponomarov & Holcomb, 2009; Sheffi, 2005; Soni et al., 2014).
2. Supply chain collaboration: all the studies reviewed agree that a high level of collaboration across a supply chain makes that chain significantly more resilient. The challenge is to create conditions for sharing information and working collaboratively. Christopher and Peck (2004) affirm that even though there has not been a history of such sharing, organisations within a supply chain are moving to adopt closer relationships with each other, and point out the potential of supply chain event management in this regard.
3. Creating a supply chain risk management culture: supply chain risks represent the most serious threat to supply chain resilience, therefore, Christopher and Peck (2004) affirm

that the only way to build supply chain resilience is by creating a risk management culture within its members. Risk sharing requires continuous risk analysis, assessment and report. Even though all the reviewed studies recognise the role of risk management in achieving supply chain resilience, only two explicitly agree on this principle (Pettit et al., 2010; Soni et al., 2014).

4. Agility: according to Christopher (2004, p. 19), “one of the most powerful ways of achieving resilience in the supply chain is to create networks which are capable of more rapid response to changed conditions”. This principle refers to both the individual members within the supply chain and the supply chain itself; two key components have been identified. The first component, visibility, highlights the importance of knowing the conditions and the standard practices within the supply chain. The second, velocity, constantly monitors how rapidly the supply chain can react to changes. Of the studies reviewed for this research, the only one that does not refer explicitly to this principle is Ponomarov and Holcomb (2009).

This section has explored the cloud sourcing model as a supply chain and identified the need for a conceptual model in the domain of ICT operational resilience for this type of supply chain. The theoretical concepts from the related disciplines discussed above can be borrowed and adjusted to the CSC specific context in order to develop such a conceptual model, the process of which is described in the next section.

7.3 Organisational Resilience in the Cloud Era: a View from Supply Chain Theory

This study aims to understand how activities in the ICT operational resilience discipline are affected by using CCE as an ICT services sourcing model. In order to do so, theories from supply chain management and supply chain resilience concepts have been analysed and the specific characteristics of CSC have been described. This section presents a conceptual model that borrows several key elements from the previously reviewed theories and concepts to explain the studied phenomenon (see Figure 7.2).

The model states that in a CSC each member establish their own resilience requirements at the enterprise level based on organisational drivers, risk tolerances and resilience objectives (Caralli et al., 2010b), and then manage OR activities by using appropriate coordination mechanisms across the chain in order to prevent disruptions; continue and manage consequences of unexpected events; and adapt in order to meet these specific requirements. The proposed model organises OR activities and coordination mechanisms across the three supply chain disruption stages: (P) preventive, (R) continuity, and (A) improvement that are derived from the three stages of the emergency response life cycle (Chen et al., 2008). The resilience activities are derived from the two general resilience perspectives and are organised by stages. The first type of activities, preventive activities, deal with strategies designed to minimise a service/asset's exposure to sources of disruption. The second type, continuity activities, include stabilising, continuing critical functions, and recovering activities. Thus the focus is on strategies designed to keep services/assets operating as close to normal as possible when facing disruptive incidents and on strategies that are aimed at returning to routine operations, including a full recovery, as soon as possible. The third type of activities, improvement activities, are strategies designed to achieve continual improvement by correcting and/or adopting new strategies of both previous types (Herrera & Janczewski, 2014). The conceptual model is focused on coordination mechanisms, which main goal is to manage dependencies among these activities in a CSC (Crowston & Osborn, 2003).

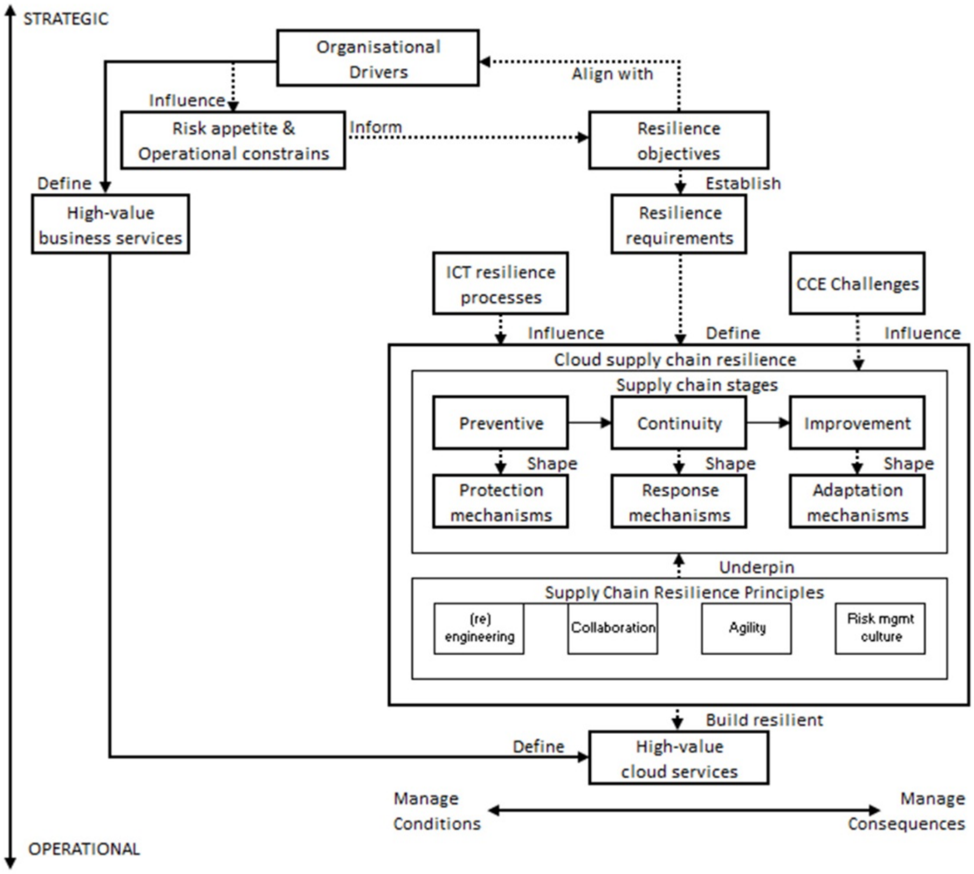


Figure 7.2: Resilient Organisations in the Cloud - Conceptual Model

The four principles that underpin resilience in supply chains are also incorporated in the model. Some modifications were made in order to capture particular requirements, which are explained below:

1. Supply chain (re)engineering: for this principle the three described key elements were adopted as previously discussed.
2. Supply chain collaboration: as the main objective of this principle is to ensure collaborative work among the CSC members, three elements derived from the reviewed literature were identified. The first element is "situational awareness"; according to (Soni et al., 2014) collaboration includes an organisation's willingness to share even sensitive information, which is known as event management (Christopher & Peck, 2004) or situational awareness (Sheffi, 2005). It can be defined as the information that needs to be shared in order to establish a base for trust among the members and to have a baseline of the current conditions in order to take action as quickly as possible (Sheffi, 2005). The second element, "synchronisation", enables effective information-sharing channels for CSC members that support decision-making processes particularly, during disruption responses (Simatupang & Sridharan, 2008; Soni et al., 2014). Finally, Sheffi (2001) stresses that collaboration is equally important after the disruptions are overcome in order to share experience among members. Building that shared knowledge is the third element of supply chain collaboration and is identified as "alignment" in this model.
3. Creating a supply chain risk management culture: the original elements, risk analysis, assessment and report, are appropriated as part of the model, but are modified. Risk analysis and assessment are grouped under the "vulnerability assessment" element (Kleindorfer & Saad, 2005; Sheffi, 2005) and report is added to a new element: "control and measure", capturing the essential wisdom of "you cannot manage what you do not measure" (Kleindorfer & Saad, 2005). This element highlights the importance of qualification and quantification in the risk management field. Finally, a third element, "embedment", is included in order to ingrain the risk culture in the CSC. From the reviewed studies, only (Sheffi, 2005) does not explicitly underlines the importance of fully integrate risk management activities in the supply chain management.
4. Agility: the original elements of visibility and velocity are appropriated as part of the model, and a third element, "innovation", is defined. According to (Ponomarov & Holcomb, 2009), the dynamic nature of the global business environment requires that

a supply chain be capable of efficiently and effectively handling unexpected events in order to maintain its competitive advantage. However, this implies not only the need to be prepared but also the need to build a capacity for continuous innovation in order to build a competitive advantage that is sustainable. In the proposed model, the innovation element aims to take advantage of all the knowledge within the CSC in order to significantly improve its condition.

The relationships between the three stages and the four principles define categories of coordination mechanisms that can positively impact CSC resilience. These relationships are presented in Table 7.1. This table can be seen as a more detailed description of this part of the model and is discussed next.

Mechanisms **Principles**	**Protection**	**Response**	**Adaptation**
(Re)engineering	Architectural mechanisms - Service delivery architecture baseline	Flexibility mechanisms - Incident detection and reporting procedures	Learning mechanisms - Root-cause analysis report
Collaboration	Situational awareness mechanisms - Communication guidelines and standards	Synchronisation mechanisms - Communication channels deployment	Alignment mechanisms - Post-incident analysis report
Risk Management Culture	Vulnerability assessment mechanisms - Resilience policy	Control mechanisms - Incident documentation	Embedment mechanisms - Policies and guidelines enforcement
Agility	Visibility mechanisms - Governance scorecard repository	Velocity mechanisms - Real-time monitoring	Innovation mechanisms - Trends analysis

Table 7.1: Categories of Operational Resilience Coordination Mechanisms for Cloud Supply Chain

7.3.1 Categories of coordination mechanisms

As stated above, coordination mechanisms are tools to address particular coordination issues. Therefore, a category of coordination mechanisms is a set of specific coordination mechanisms that could be used to address the same type of coordination issue. In other words, mechanisms grouped in a specific category pursue the same coordination goal. The proposed model defines three main types of coordination mechanisms: protection, response, and adaptation, and their coordination goals are directly derived from the main expected outcomes of each stage. For example, in the emergency response life cycle the main goal of preparing for a disruptive event is to implement proactive mechanisms and controls that can make potentially disruptive events less frequent or severe (Herrera & Janczewski, 2014). Therefore, coordination mechanisms in this group are designed to deal with coordination issues that jeopardise the achievement of these goals, which are (see goal P below). Following the same procedure, the main coordination goal for "coordination mechanisms for response – R" and "coordination mechanisms for adaptation – A" were stated.

These three categories of coordination mechanisms are still very generic. However, the adopted CSC resilience principles, which by definition facilitate the attainment of resilience in a supply chain, divide them into four subcategories that underpin their achievement. In order to make explicit the coordination goals across the 12 subcategories of OR coordination mechanisms, the following steps were taken. Based on the reviewed literature related to the ICT operational resilience processes (Caralli et al., 2010b) and the identified OR challenges (Herrera et al., 2014), an initial set of coordination goals was defined. Then, an assessment of the resulting set was conducted by comparing them with typical coordination goals in the field of emergency response, in particular the framework of Chen et al. (2008). In total a set of three first-level coordination goals and 12 second-level coordination goals were identified.

(P) To prevent the realisation of ICT operational risk to high-value services in the CSC and to build capabilities to handle a disruptive event in an effective way – *Coordination mechanisms for protection.*

1. Dynamically establish the CSC architecture and understand its nature (members, relationships, characteristics, among others) – Architectural mechanisms
2. Identify information and valuable mechanisms that allow CSC members to know what is going on around them in the supply chain – Situational awareness mechanisms
3. Identify and analyse vulnerabilities in the CSC according to the level of control over the specific cloud service – Vulnerability assessment mechanisms
4. Establish a clear view and well-known environment – Visibility mechanisms

(R) To sustain a high-value service in the CSC if a risk is realised, addressing its consequences to the CSC members effectively, and to return the CSC to the normal state – *Coordination mechanisms for response*

1. Provide alternatives to meet the CSC expected level of resilience – Flexibility mechanisms
2. Provide effective channels to share information, particularly to support decision-making activities – Synchronisation mechanisms
3. Identify and collect information across the CSC about risk-control activities and mechanisms in order to assess their effectiveness and make improvements – Control and measure mechanisms
4. Assess how rapidly the CSC reacts to disruptive events – Velocity mechanisms

(A) To systematically improve the achievement of the two previous goals in the CSC – *Coordination mechanisms for adaptation*

1. Assess the CSC resilience ability maturity and implement improvement actions – Learning mechanisms
2. Build CSC knowledge based on shared-experiences maintaining OR efforts aligned – Alignment mechanism
3. Ensure that resilience activities and coordination mechanisms are embedded in the CSC daily operations – Embedment mechanisms
4. Significantly change or improve resilience activities and/or coordination mechanisms across the CSC - Innovation mechanisms

By using the findings of previous research in supply chain management and specifically in supply chain resilience as theoretical underpinnings for its development, this conceptual model and the structured set of coordination mechanisms represents the first step towards conceptualises how ICT resilience activities can best be coordinated across the CSC in order to make this supply chain become more resilient.

7.4 Conclusions and Further Research

This research contributes to the existing body of knowledge by using concepts and theories from related disciplines in order to gain insights into how the adoption of cloud computing as an ICT services sourcing model impacts the ICT operational resilience discipline. By doing so, this paper has taken a first step by providing a theoretical underpinning for such research. In a CSC, coordinated activities across its members are essential in order to build OR. From a methodological perspective, the contribution of this paper lies in its viewing the cloud model as a supply chain in order to apply some of the well-known coordination concepts in the supply chain literature. Based on this application, a structured set of categories of coordination mechanisms that positively impacts CSC resilience has been proposed from an ICT operational perspective. From the practitioner's perspective the conceptual model provides additional insight into the area of OR where managerial decisions are especially important and the model can be used for selecting and/or enhancing specific coordination mechanisms in order to manage dependencies throughout the three disruption stages in a CSC.

This paper has presented a conceptual model that only includes OR challenges derived from the cloud essentials characteristics. The other two components of the cloud model, service delivery models and deployment models, definitely shape the specific CSC structure and therefore its resilience. However, it is expected that their impact is mainly related to selecting specific coordination mechanisms across the proposed categories.

The opportunities for further research are abundant. The next logical step is to empirically test the proposed model. Specifically, analysis of real incidents in CSC could be done through walkthrough and tabletop exercises in order to assess the model and to identify specific coordination mechanisms that are effectively being used along the CSC. Once a decision on a specific cloud type and service setup has been made, the comprehensive supply chain can be determined and built up, requiring further conceptualisation. As many, if not all, of the identified categories of coordination mechanisms require information sharing, there is a clear research opportunity in this area as well.

As the evolution of cloud computing continues, CSC will take on a greater role within the organisation. Likewise, as ICT delivery models change and become more complex, the business environment is fast becoming more interconnected and volatile, and the consequences of external events more substantial. This dynamic environment will be further complicated by higher expectations on the part of cloud consumers and CSC resilience activities will need to improve in terms of higher levels of availability, performance and responsiveness, all of which demonstrates the potential of this emergent research area.

7.5 References

Alberts, C. J., Dorofee, A. J., Creel, R., Ellison, R. J., & Woody, C. (2011). *A systemic approach for assessing software supply-chain risk.* Paper presented at the 2011 44th Hawaii International Conference on System Sciences (HICSS).

Arean, O. (2013). Disaster recovery in the cloud. *Network Security, 2013*(9), 5-7.

Arshinder, K., Kanda, A., & Deshmukh, S. (2011). A review on supply chain coordination: coordination mechanisms, managing uncertainty and research directions. *Supply chain coordination under uncertainty* (pp. 39-82): Springer.

Baxter, L. F., & Simmons, J. E. (2001). *The software supply chain for manufactured products: reassessing partnership sourcing.* Paper presented at the International Conference on Management of Engineering and Technology, 2001. PICMET'01. Portland.

British Standards Institute. (2011). BS ISO/IEC 27031:2011 Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity.

British Standards Institute. (2014). BS 65000:2014 Guidance on organizational resilience.

Cao, C., & Zhan, Z. (2011). *Incident management process for the cloud computing environments.* Paper presented at the Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). CERT® Resilience management model v1.0: improving operational resilience processes (S. E. Institute, Trans.): Carnegie Mellon.

Carpenter, S., Walker, B., Anderies, J. M., & Abel, N. (2001). From metaphor to measurement: resilience of what to what? *Ecosystems, 4*(8), 765-781.

Chen, R., Sharman, R., Rao, H. R., & Upadhyaya, S. J. (2008). Coordination in emergency response management. *Communications of the ACM, 51*(5), 66-73.

Chou, M., Ye, H.-Q., & Yuan, X.-M. (2005). *Analysis of a software focused products and service supply chain.* Paper presented at the 3rd IEEE International Conference on Industrial Informatics, 2005. INDIN'05. 2005.

Christopher, M. (2004). Creating resilient supply chains. *Logistics Europe, 11*.

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The international journal of logistics management, 15*(2), 1-14.

Cockram, D. (2012). Organisational resilience. In T. B. W. Group (Ed.), *A BCI Working Group White Paper*: Business Continuity Institute.

Crowston, K., & Osborn, C. S. (2003). A coordination theory approach to process description and redesign. In T. W. Malone, K. Crowston & G. A. Herman (Eds.), *Organizing business knowledge: the MIT process handbook*: MIT press.

Dalziell, E., & McManus, S. (2004). *Resilience, vulnerability and adaptive capacity: implications for system performance*. Paper presented at the International Forum for Engineering Decision Making.

Dekker, M. (2012). Critical Cloud Computing: A CIIP perspective on cloud computing services: European Network and Information Security Agency (ENISA).

Dekker, M., Liveri, D., & Lakka, M. (2013). Cloud security incident reporting: framework for reporting about major cloud security incidents: European Network and Information Security Agency (ENISA).

Demirkan, H., Cheng, H. K., & Bandyopadhyay, S. (2010). Coordination strategies in an SaaS supply chain. *Journal of Management Information Systems, 26*(4), 119-143.

Du, S., Lu, T., Zhao, L., Xu, B., Guo, X., & Yang, H. (2013). *Towards an analysis of software supply chain risk management.* Paper presented at the Proceedings of the World Congress on Engineering and Computer Science.

Dutta, A., Peng, G. c. a., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of its experts. *Journal of Computer Information Systems, 53*(4).

Fischer, F., & Turner, F. (2009). Cloud computing as a supply chain. *Walden University*.

Franke, J., Charoy, F., & El Khoury, P. (2013). Framework for coordination of activities in dynamic situations. *Enterprise Information Systems, 7*(1), 33-60.

Fugate, B., Sahin, F., & Mentzer, J. T. (2006). Supply chain management coordination mechanisms. *Journal of Business Logistics, 27*(2), 129-161.

Gartner. (2012). Gartner says worldwide cloud services market to surpass $109 billion in 2012 [Press release]. Retrieved from http://www.gartner.com/newsroom/id/2163616.

Grobauer, B., & Schreck, T. (2010). *Towards incident handling in the cloud: challenges and approaches*. Paper presented at the Proceedings of the 2010 ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA.

Herrera, A., Beltran, F., & Janczewski, L. (2014). *Resilient organisations in the cloud.* Paper presented at the The 25th Australasian Conference on Information Systems, Auckland, New Zealand.

Herrera, A., & Janczewski, L. (2014). Issues in the study of organisational resilience in cloud computing environments. *Procedia Technology, 16*(0), 32-41. doi: http://dx.doi.org/10.1016/j.protcy.2014.10.065.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics, 4*(ArticleType: research-article / Full publication date: 1973 / Copyright © 1973 Annual Reviews), 1-23. doi: 10.2307/2096802.

Holling, C. S. (2010). Engineering resilience versus ecological resilience. In L. H. Gunderson, C. R. Allen & C. S. Holling (Eds.), *Foundations of ecological resilience* Washington : Island Press, c2010.

IBM Global Technology Services. (2014). Resilience in the era of enterprise cloud computing *Thought leadership white paper*.

International Data Corporation. (2013). Worldwide and regional public it cloud services 2013–2017 forecast [Press release]. Retrieved from http://www.idc.com/getdoc.jsp?containerId=242464.

ISACA. (2012). Guiding principles for cloud computing adoption and use *Cloud Computing Vision Series*.

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security, 20*(5), 332-349.

Kaliski Jr, B. S., & Pauley, W. (2010). *Toward risk assessment as a service in cloud environments.* Paper presented at the Proceedings of the 2nd USENIX conference on Hot topics in cloud computing.

Klein, R. J. T., Nicholls, R. J., & Thomalla, F. (2003). Resilience to natural hazards: how useful is this concept? *Global Environmental Change Part B: Environmental Hazards, 5*(1–2), 35-45. doi: 10.1016/j.hazards.2004.02.001.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and operations management, 14*(1), 53-68.

Lindner, M., Galán, F., Chapman, C., Clayman, S., Henriksson, D., & Elmroth, E. (2010). *The cloud supply chain: A framework for information, monitoring, accounting and billing.* Paper presented at the 2nd International ICST Conference on Cloud Computing (CloudComp 2010).

Lindner, M., McDonald, F., Conway, G., & Curry, E. (2011). *Understanding cloud requirements-a supply chain lifecycle approach.* Paper presented at the Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization CLOUD COMPUTING 2011.

Lindner, M., McDonald, F., McLarnon, B., & Robinson, P. (2011). *Towards automated business-driven indication and mitigation of VM sprawl in cloud supply chains.* Paper presented at the Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on.

Lindner, M., Robinson, P., McLarnon, B., & McDonald, F. (2011). *The bullwhip effect and VM sprawl in the cloud supply chain.* Paper presented at the Towards a Service-Based Internet. ServiceWave 2010 Workshops.

Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. *ACM Comput. Surv., 26*(1), 87-119. doi: 10.1145/174666.174668.

Martens, B., & Teuteberg, F. (2011). *Risk and compliance management for cloud computing services: designing a reference model.* Paper presented at the AMCIS.

Maurer, F., & Lechner, U. (2014). *From disaster response planning to e-resilience: a literature review.* Paper presented at the BLED 2014. Paper 32.

Mell, P., & Grance, T. (2011). The NIST Definition of cloud computing special publication *(SP) 800-145*. Gaithersburg, MD: US National Institute of Standards and Technology (NIST).

Morisse, M., & Prigge, C. (2014). *Business continuity in network organizations–a literature review.* Paper presented at the Twentieth Americas Conference on Information Systems, Savannah.

Oberhauser, R., & Schmidt, R. (2007). *Improving the integration of the software supply chain via the semantic web.* Paper presented at International Conference on the Software Engineering Advances, 2007. ICSEA 2007.

Oppenheimer, D., Ganapathi, A., & Patterson, D. A. (2003). *Why do Internet services fail, and what can be done about it?* Paper presented at the USENIX Symposium on Internet Technologies and Systems.

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: development of a conceptual framework. *Journal of Business Logistics, 31*(1), 1-21.

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The international journal of logistics management, 20*(1), 124-143.

Saripalli, P., & Walters, B. (2010). *QUIRC: A quantitative impact and risk assessment framework for cloud security*. Paper presented at the IEEE 3rd International Conference on Cloud Computing (CLOUD), 2010.

Schrödl, H., & Bensch, S. (2013). *E-Procurement of cloud-based information systems–a product-service system approach*. Paper presented at the Thirty Fourth International Conference on Information Systems, Milan.

Sheffi, Y. (2001). Supply Chain Management under the Threat of International Terrorism. *The international journal of logistics management, 12*(2), 1-11. doi: doi:10.1108/09574090110806262.

Sheffi, Y. (2005). The resilient enterprise: overcoming vulnerability for competitive advantage. *MIT Press Books, 1*.

Shim, J., & Lim, Y. (2013). Implementation of real time alert system over cloud computing. *International Journal of Energy, Information & Communications, 4*(3).

Simatupang, T. M., & Sridharan, R. (2008). Design for supply chain collaboration. *Business Process Management Journal, 14*(3), 401-418.

Simatupang, T. M., Victoria Sandroto, I., & Hari Lubis, S. (2004). Supply chain coordination in a fashion firm. *Supply Chain Management: An International Journal, 9*(3), 256-268.

Simmonds, D., Collins, R. W., & Berndt, D. (2010). *Coordinating the relationship between it services providers and clients: the case of cloud computing*. Paper presented at the Proceedings of SIGSVC Workshop.

Soni, U., Jain, V., & Kumar, S. (2014). Measuring supply chain resilience using a deterministic modeling approach. *Computers & Industrial Engineering, 74*, 11-25.

Spring, J. (2011). Monitoring cloud computing by layer, part 1. *Security & Privacy, IEEE, 9*(2), 66-68.

Staten, J., Nelson, L., Bartoletti, D., Herbert, L., Martorelli, W., Baltazar, H., O'Donnell, G., & Caputo, M. (2014). Predictions 2015: The days of fighting the cloud are over: Forrester.

The Resilience Alliance. (2012). Key concepts. Retrieved November 2012, from http://www.resalliance.org/index.php/key_concepts

Troshani, G. R., & Wickramasinghe, N. (2011). *Cloud nine? an integrative risk management framework for cloud computing*. Paper presented at the Proceedings of Bled Conference.

Weick, K., Sutcliffe, K., & Obstfeld, D. (1999). Organizing for high reliability: processes of collective mindfulness. *Research in organizational behavior, 21*, 23-81.

Willcocks, L. P., Venters, W., & Whitley, E. A. (2013). *Moving to the cloud corporation: how to face the challenges and harness the potential of cloud computing*: Palgrave Macmillan.

Wilson, R. L. (2010). *Organizational resilience models applied to companies in bankruptcy.* (Doctor of Management), University of Maryland University College, United States -- Maryland.

Winkler, U., & Gilani, W. (2011). Model-Driven Framework for business continuity management. *Service Level Agreements for Cloud Computing* (pp. 227-250): Springer.

Xu, L., & Beamon, B. M. (2006). Supply chain coordination and cooperation mechanisms: an attribute ‐ based approach. *Journal of Supply Chain Management, 42*(1), 4-12.

Yan, J., Guo, Y., & Schatzberg, L. (2012). Coordination mechanism of IT service supply chain: an economic perspective. *Electronic Markets, 22*(2), 95-103.

Yang, H., & Tate, M. (2012). A descriptive literature review and classification of cloud computing research. *Communications of the Association for Information Systems, 31*(1), 2.

8 Cloud Supply Chain Resilience Model: Development and Validation

Cloud computing is reshaping the information and communication technology (ICT) supply chain and creating a more dynamic ICT environment. However, this transformation is accompanied by a greater risk of disruption and brings new organisational resilience (OR) challenges. Focusing on OR in relation to the cloud supply chain (CSC), this paper adopts a two-stage qualitative research design to investigate how ICT resilience activities can best be coordinated across a CSC. It proposes and empirically validates a conceptual model as a tool for guiding efforts to maintain and improve resilience in CSCs. The model is based on existing supply chain management and supply chain resilience theories and considers specific characteristics of the CSC in order to identify coordination mechanisms that positively impact ICT resilience processes within it. Empirical validation with New Zealand companies established the value of the model in terms of structuring the OR conversation across the CSC.

8.1 Introduction

Cloud computing is an increasingly popular information and communication technology (ICT) sourcing model that enables convenient, on-demand network access to a shared pool of easily accessible and usable virtualized resources (Mell & Grance, 2011, p. 2). Based on its potential, industry analysts have predicted a complete transformation of the computing industry (Gartner, 2012; International Data Corporation, 2013; Ried & Kisker, 2011), with 80% of organisations depending on cloud services and tens of millions of end users consuming cloud services by the end of this decade (Dekker, 2012). As part of this transformation, cloud computing is reshaping the ICT services supply chain, making it larger and more complex with globally dispersed components (Lindner et al., 2010).

Effective management in this type of supply chain is a challenging task, especially with the threat of unexpected disruptions. Researchers and industry organisations (Armbrust et al., 2010; Cloud Security Alliance, 2011; Dekker, 2012) have therefore described cloud computing as a double-edged sword: “on the one hand, large cloud providers can deploy state-of-the-art security and resilience measures and spread the associated costs across the customers. On the other hand, if an outage occurs the consequences could be big, affecting a lot of data, many organisations and a large number of citizens at once” (Dekker, 2012, p. iii). In other words, as computing moves away from onsite data centres to dynamic and widely distributed cloud supply chains (CSC), organisations are more prone to being affected by disruptions, and therefore there is a need to strengthen their ability to not only survive but also thrive when exposed to CSC disruptive events (Arean, 2013; IBM Global Technology Services, 2014).

Such an ability is referred in the literature as organisational resilience (OR), which has been defined as “the ability of an organization to anticipate, prepare for, and respond and adapt to everything from minor everyday events to acute shocks and chronic or incremental changes” (British Standards Institute, 2014, p. 1). Accordingly, OR is a goal and is enhanced by coordinating various disciplines that an organisation might have already implemented, such as risk management, business continuity, and ICT readiness for OR (Cockram, 2012). This concept also recognises that organisations interact with other organisations and therefore it is essential to build OR in partnership with others (Morisse & Prigge, 2014), particularly when some of their processes have moved outside of their traditional boundaries, as is the case with cloud services.

Focusing on OR in relation to the CSC, this research first investigates how ICT operational resilience activities can best be coordinated across the CSC in order to make this supply chain more resilient. It then proposes a conceptual model as a tool for guiding efforts to maintain and improve resilience in this type of supply chain. The model is based on existing supply chain management and supply chain resilience theories and considers specific characteristics of the CSC in order to identify coordination mechanisms that positively impact ICT operational resilience processes within this chain.

The remainder of this article proceeds as follows. Section 8.2 outlines the two-stage research methodology adopted. The subsequent sections present and discuss the findings from these stages: model development and its empirical validation. In the last section the authors draw conclusions, present contributions, and consider limitations and directions for future research.

8.2 Research Design

The authors identified the interpretivist paradigm as the most appropriate for this research and adopted a two-stage qualitative approach to propose a model of coordination mechanisms for enhancing CSC resilience. In Stage 1, an extensive literature review identified four potential foundations for the model which were refined with data gathered by interviewing experts. This early validation resulted in a supply chain approach being adopted to further develop the model.

In Stage 2, the model was verified by analysing six cloud incidents in New Zealand medium and large companies using two methods. First, primary data were collected from semi-structured interviews to reconstruct the incidents in terms of the model. The second method involved validating the model's perceived usefulness by conducting a tabletop exercise.

8.3 Stage 1 – Developing the Model

A preliminary literature review allowed the authors to identify and understand the phenomenon under study (Herrera & Janczewski, 2013) adopting an ICT operational resilience processes perspective (Caralli et al., 2010b). The review also revealed a lack of literature on the specific topic (Morisse & Prigge, 2014). Based on the preliminary findings, this stage was divided in two parts: (1) validation of the initial conceptualisation, and (2) definition of the conceptual model. This section first defines the central concepts in this research and then it presents the main results from the two parts.

8.3.1 Central concepts

Three concepts define the boundaries of this research. Cloud computing is an ICT sourcing model defined by three essential components: (1) five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service; (2) three service delivery models: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS); and (3) four deployment models: private, community, public, and hybrid cloud. From the resilience perspective these three main components raise OR concerns. It has been argued (Herrera et al., 2014) that the main OR challenges are derived from its characteristics because the key novelty of cloud computing, compared to other ICT service-based models, is its highly dynamic environment.

OR is not a new concept; the first publications appeared in the early 1990s (Wilson, 2010). However, an analysis of the information systems (IS) literature revealed that while disruptions and methods to keep businesses in ICT-based interorganisational networks running have not been greatly studied (Morisse & Prigge, 2014), the need for novel concepts for ICT and OR planning when using new ICT sourcing models such as cloud computing has been recognized (Caralli et al., 2010b; Maurer & Lechner, 2014; Morisse & Prigge, 2014). From the management perspective, some resilience-related issues of cloud environments have been studied such as incident management (Cao & Zhan, 2011; Grobauer & Schreck, 2010) , risk management (Dutta et al., 2013; Kaliski Jr & Pauley, 2010; Martens & Teuteberg, 2011;

Saripalli & Walters, 2010; Troshani & Wickramasinghe, 2011), real-time monitoring (Shim & Lim, 2013; Spring, 2011a, 2011b), and the mechanisms that organisations are using to enhance OR among interorganisational ICT relationships (Järveläinen, 2012).

A key concept driving this investigation is the notion of dependency. Problems that arise from dependency are referred in the literature as coordination problems, in fact, Malone and Crowston (1994) define coordination as managing dependencies. Malone and Crowston (1994) and Crowston and Osborn (2003) introduce coordination theory as a framework for analysing complex processes in terms of actors performing interdependent activities. This theory identifies two types of activities within a process: "activities that directly contribute to the output of the process" (Simatupang et al., 2004, p. 257) and coordination mechanisms, which are additional activities that must be carried out in order to manage dependencies among the first type of activities. With the main concepts defined, the next subsection describes the initial validation of the proposed model.

8.3.2 Initial conceptualisation validation

Based on an extensive literature review and the identification of the key conceptual issues in the study of OR in cloud environments (Herrera & Janczewski, 2014), a previous study identifies four potential foundations for the model (Herrera et al., 2014). These foundations were derived from the literature and associated interview questions were composed.

- F1: designing flexible processes to not only maintain and return to the desired state but also to continue to function in the face of disturbance (Dalziell & McManus, 2004).
- F2: analysing how cloud characteristics affect the three distinct sets of OR activities: protect and prepare, respond, and adapt (British Standards Institute, 2014).
- F3: managing dependencies as all parties share responsibility in providing the environment with adequate protections (Herrera & Janczewski, 2014).
- F4: determining the coordination mechanisms for ICT resilience processes highly impacted by cloud adoption (Caralli et al., 2010b; Herrera & Janczewski, 2014).

Primary data from semi-structured interviews with 10 experts were collected in order to validate the foundations. The authors considered that due to the limited academic literature on the topic, experts' opinions would be of significant value (Linstone & Turoff, 2002). Participants were recruited from among members of special interest groups such as the New Zealand Information Security Forum, the IT Disaster Recovery and Service Continuity

Professionals group, and the Cloud Security Alliance and selected due to their expertise in both OR and ICT. Each interview lasted approximately 45–60 minutes and were audio-recorded (McCracken, 1988; Myers, 2009). After an overview of the study was given, the interviewee was asked open-ended questions from an OR perspective that were structured around three main categories: (1) the main changes introduced by consuming cloud services; (2) the main challenges of managing dependencies in a cloud environment; and (3) the main mechanisms used to coordinate efforts among all involved parties. The main findings are presented below.

Main changes: Many participants stressed that OR activities should not change to a great extent with the shift to cloud computing. All participants agreed that even though cloud consumers transfer some of their responsibility to providers, their accountability is not transferable. One expert stated,

"You have to remind your provider that you are right there. They cannot forget you … at the end of the day OR activities have to be driven by the accountable party."

Another expert said firmly,

"Consumers have to understand that sourcing ICT services from a cloud provider implies free time that should be focused on something else than trying to control OR processes as they used to … it is about aligning, coordinating and verifying."

Due to the nature of cloud services and the relinquishment of some control, changes should converge on identifying and deploying flexible mechanisms to align, measure, and reinforce OR activities. As explained by one expert,

"Some changes in OR processes [should occur] such as risk management perhaps … however, it is only another provider so it should be managed as another supply chain."

A different expert stated,

"I would not look at this problem as changing things here and there … The best way to look at this is to simplify it to a supply chain analysis … if the organisation does not look at the impacts to the supply chain (upstream and downstream) there would most definitely be gaps in achieving OR expectations by the business."

Main challenges: All participants agreed that consistent and constant communication is needed and a key challenge is to create conditions that encourage open communication. As stated by one expert,

"Communication is imperative to ensure an effective approach to recovery—it is what I call sharing the passion... a common language is fundamental to ensure a consistent approach along the supply chain."

Another expert commented,

"The problem is committing to keeping parties informed, which implies technical challenges, costs and … you know, some risks too, how that information is going to be used."

Regarding information sharing, participants repeatedly mentioned that accurate and current information in a highly dynamic environment is difficult to obtain and properly use. In this direction, one participant observed,

"OR activities need to be aligned to the provider's capability that means you have to monitor and manage, [an] important challenge in such a dynamic environment … What you can measure you can manage, so measure properly!"

Mechanisms to coordinate efforts: The majority of interviewees indicated that OR efforts should be focused on taking proper account of cloud characteristics. One observed,

"Cloud is an outsourcing model with unique features, we should focus on that … example: real-time measurement".

Another expert indicated,

"I like the idea of focusing on doing what we know how to do but with different rules … team players in an extremely dynamic environment".

However, one expert indicated that this approach was not enough:

"You know, cloud encompasses several service models—SaaS, PaaS and IaaS—and deployment models as well … OR concerns and mechanisms will vary greatly case by case."

Regarding key mechanisms, all participants considered that preventive mechanisms should be the focal point. Speaking to this, one expert said,

> *"Coordinating preventive mechanisms, no doubt! Even now our time and efforts are focused on prevention! We do not want to get used to other types of strategies and if you need to get other people on board, it is going to be time consuming".*

Overall, three of the model foundations were accepted (F1-F3) but a key concern regarding F4 and the adopted approach was raised. The expert interview analysis shows that coordination is undoubtedly a key foundation (F3) for the model. It also shows that a focus on cloud characteristics is important, even though other cloud components can affect OR activities (F2). However, not much evidence was found regarding what type of resilience should be the focus. Participants placed similar importance on mechanisms for maintaining and returning OR as they did on mechanism for increasing the magnitude of consequences that an organisation could withstand (F1), and preventive mechanisms were identified as fundamental by all interviewees. More importantly, the analysis identified that the problem under study is perceived and framed in practice from a supply chain perspective. Almost all the interviewees stated that it would be more beneficial to analyse how OR activities can best be coordinated across the CSC instead of identifying changes in specific ICT operational processes derived from sourcing ICT services from a cloud (F4). Taking into account this analysis of the experts' opinions, the next subsection presents the proposed model.

8.3.3 Model definition: A supply chain approach

After the analysis of the expert interviews, an additional literature review was conducted in order to revalidate and reframe the research problem. First the cloud computing definition presented in the previous section and the main actors interacting in a cloud environment were reviewed (Herrera & Janczewski, 2014): consumer, providers and brokers. This arrangement certainly creates a setup that is typical of a supply chain insofar as cloud consumers obtain their services from providers who in turn depend on other providers or brokers to provide that service. Thus, in a CSC a disruption to one service immediately disrupts the interdependent services, resulting in a disruption to the overall service delivered to the cloud consumer, which could impact business services and potentially lead to organisational damage (Oppenheimer et al., 2003). Lindner et al. (2010, p. 3) first formally defined CSC as "two or more parties linked by the provision of cloud services, related information and funds" but few studies have explored the concept of cloud computing as a supply chain (Fischer & Turner, 2009; ISACA, 2012; Lindner, McDonald, Conway, et al., 2011). This creates an opportunity to apply theoretical concepts from supply chain coordination mechanisms and supply chain resilience adjusted to CSC's specific features and challenges in order to develop a conceptual model.

Supply chain management sees coordination as "a strategic response to the problems that arise from inter-organisational dependencies within the chain" (Xu & Beamon, 2006, p. 4) and coordination mechanisms as tools for effectively managing those dependencies. A specific problem that can arise from dependencies is the problem of disruption. In the literature an increasing interest in studying disruptions has led to the theorising of disruption management and its relation to supply chain resilience (Christopher & Peck, 2004; Kleindorfer & Saad, 2005; Pettit et al., 2010; Ponomarov & Holcomb, 2009; Sheffi, 2005; Soni et al., 2014). Supply chain resilience is defined as "the adaptive capability of the supply chain to prepare for unexpected events, respond to disruptions, and recover from them" (Ponomarov & Holcomb, 2009, p. 131). Following Christopher and Peck (2004), resilience is underpinned by four principles:

- (Re)engineering: resilience should be "designed-in" to minimise, when possible, a supply chain's exposure to sources of disruption.
- Collaboration: "using knowledge generated and shared by partners in the supply chain" (Christopher & Peck, 2004, p. 9) is fundamental to reducing uncertainty.
- Risk management culture: supply chain risks represent the most serious threat to OR, therefore risk management has to be made a concern of everyone and should be extended beyond the boundaries of corporate risk to create a supply chain risk management culture.
- Agility: achieving resilience in the supply chain implies the creation of networks which are capable of more rapid response to changed conditions.

Building on foundations F1–F3 and adjusting the studied concepts from supply chain coordination mechanisms and supply chain resilience to CSC characteristics, a model of coordination mechanisms for enhancing CSC resilience is proposed (Figure 8.1).

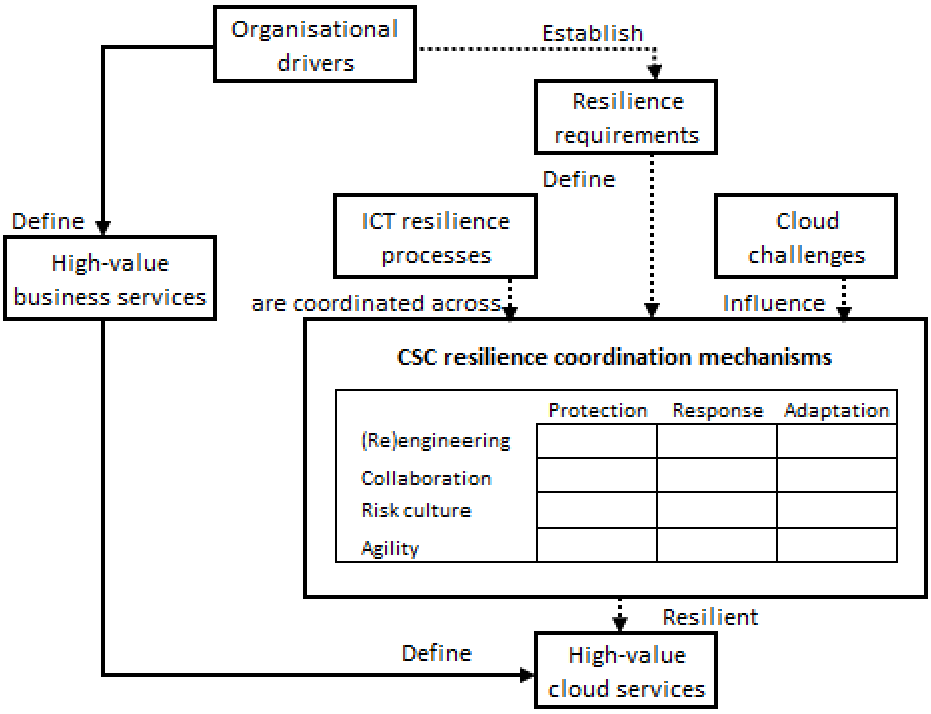


Figure 8.1: Cloud Supply Chain Resilience Model

In brief, the model states that in a CSC each member establish their own OR requirements at the enterprise level based on organisational drivers (Caralli et al., 2010b) and then manage OR activities by using appropriate coordination mechanisms across the chain in order to prevent (P), respond (R), and adapt (A). The relations between the four supply chain resilience principles and these three stages define 12 categories of coordination mechanisms that can positively impact CSC resilience. As stated above, coordination mechanisms are tools to address specific coordination issues, and therefore mechanisms grouped in a specific category pursue the same goal. In order to identify coordination goals for each category, a systematic review of ICT operational resilience activities (Caralli et al., 2010b) and the typical coordination goals in the emergency response field, specifically the framework by Chen et al. (2008), was conducted (Herrera & Janczewski, 2015).

Re(engineering): mechanisms enhancing this principle are focused on (P) establishing a clear baseline architecture; (R) providing alternatives to meet expected level of resilience; and (A) assessing and improving CSC resilience.

Collaboration: mechanisms creating appropriate conditions for collaborative work across CSC members are focused on (P) understanding the environment by developing a common base of valuable information; (R) providing effective channels to share information, particularly, when facing disruptive events; and (A) building on experiences in order to maintain collaborative mechanisms aligned.

Risk management culture: mechanisms embedding risk management in a CSC are focused on (P) analysing vulnerabilities; (R) measuring controls' effectiveness; and (A) reinforcing resilience activities.

Agility: the achievement of this principle is based upon close collaboration by using CSC information to respond rapidly to changing conditions. Mechanisms are focused on (P) establishing a well-known environment; (R) assessing mechanisms to improve reaction time; and (A) analysing trends.

Incorporating foundations derived from an extensive literature review, analysis of expert interviews, and findings from previous research in supply chain resilience as theoretical underpinnings, the proposed model has made the first step towards conceptualises how ICT resilience activities can best be coordinated across the CSC in order to make it more resilient. However, in order to address the identified need of guiding organisational efforts in maintaining and improving OR in this type of supply chain, an empirical study was conducted to corroborate the first stage's findings and assess the perceived usefulness of the model. Results from this study are discussed next.

8.4 Stage 2 – Empirical Findings

The next logical step was to validate the model. An empirical analysis of coordination mechanisms in CSC was conducted. This analysis aimed to provide answers to the following questions: (1) is the model able to capture the richness of a real cloud incident? and (2) is the model perceived as useful tool for guiding efforts in maintaining and improving CSC resilience? The unit of analysis was a cloud incident across the three stages of the resilience life cycle: preventive, continuity, and improvement (British Standards Institute, 2014). Participant firms are considered major players in different CSCs in the New Zealand cloud services market -consumer, broker, or provider- and data from six incidents were collected using two methods. Interviewees were senior employees, at least two from each firm where possible, with ICT backgrounds and experience in incident response. First, data about the incident were collected through semi-structured interviews (Table 8.1). All the incidents were documented in terms of the model and the relevant literature was used as a secondary source for the analysis.

Opening

- Personal introductions / Overview of the study

Initial prompts

- Background organisation, service and service agreement / Tell me about an incident

Additional questions

- How do you coordinate activities with your customer/provider along the incident life cycle?
- How do you determine the "success/failure" of these activities with your customer/provider?

Additional unplanned/floating prompts

- How? / Can you tell me more about that? / Can you give me examples? / How does that work?

Table 8.1: Incident Interview Protocol

All the incident interpretations were presented, discussed, and refined when necessary. Then simple tabletop exercises[2] (U.S. Department of Homeland Security, 2011) based on the studied scenarios were conducted to identify additional mechanisms that could positively impact their CSC resilience.

A background of the cloud services involved and a brief overview of the incidents is presented in Table 8.2. Several key insights came from analysing data collected from these incidents. This section first discusses the general CSC findings before presenting the specific findings regarding the four resilience principles and identifying the most common OR coordination mechanisms. A brief description of the outcomes of the tabletop exercises follows, along with the perceived usefulness of the model.

[2] A tabletop exercise is a facilitated analysis of an emergency scenario in an informal and stress-free environment

Incident	Business service	Cloud service	Incident summary
1	HV*: 8 RTO/RPO: 4/4 Role: Consumer	SM: SaaS - Single tenant DM: Outsourced-private SC: Dyadic (SaaS - Consumer)	S: Non-scheduled change C: Service outage, some data loss D: A week Breached SLA: Yes
2	HV: 9 RTO/RPO: 4/4 Role: Consumer	SM: SaaS DM: Public SC: Triad (IaaS - SaaS - Consumer) Consumer only interacts with SaaS provider)	S: Scheduled change, business area did not run the full set of tests C: Service outage, no data loss D: Three days Breached SLA: Yes
3	HV: 8 RTO/RPO: 4/0.25 Role: Consumer	SM: SaaS DM: Public SC: 4 (IaaS - SaaS - Broker - Consumer) Consumer integrates SaaS and Broker's services interacting with both of them	S: Unpatched software vulnerability C: Denial-of-service attack, service outage. No data loss D: 1.5hrs Breached SLA: Yes, vulnerability management is covered but no in terms of availability
4	HV: 8 RTO/RPO:* Role: Broker	SM: SaaS DM: Public SC: Triad relationship (IaaS - Broker - Consumer) Consumers integrate IaaS and Broker's services interacting with both	S: Hardware failure (IaaS Provider) C: Service outage, no data loss D: 24hrs Breached SLA: Not ours. Customers have their own SLA with the IaaS provider, “we were not affected”
5	HV: 6 RTO/RPO:* Role: Broker	SM: SaaS DM: Public SC: Triad (IaaS - Broker - Consumer) Consumers only interact with Broker	S: Scheduled maintenance was not carried out C: SSL certificate expired, availability okay but the trust mechanism was undermined D: +24hrs Breached SLA: No, but image was compromised
6	HV: 9 RTO/RPO:* Role: Provider	SM: Not a specific service, technology issue affecting one SAN providing virtual machines DM: Public SC: Dyadic and triad mainly	S: 3 disks failed at the same time C: Service outage, no data loss (Except a large SQL server some transactions were rebuilt) D: 20hrs, recovery process was driven by priorities some customers were back in minutes Breached SLA: No

HV=High-value service (1-10, being 10 the most critical)
RPO and RTO in hours
SM=Service model, DM=Deployment model

SC=Supply chain structure – Main actors in the relationship
S=Source, C=Consequences, and D=Duration
SAN=Storage Area Network

*Customised according to customers’ requirements

Table 8.2: Cloud Incidents Overview

8.4.1 Capturing past experience

All the studied incidents were associated with cloud services supporting high-value business processes and therefore service-level-agreements (SLAs) guaranteed recovery-time-objectives (RTOs) and recovery-point-objectives (RPOs) of 24 hours or less. All participants stated that their SLAs explicitly included OR conditions that they have negotiated to some extent. This finding is aligned with a study of cloud contracts by Hon, Millard, and Walden (2012) that shows that a multiplicity of approaches are emerging and niche providers and brokers are more willing to tailor SLAs, leaving behind the idea of cloud services as "one size fits all." Previous research has identified cloud brokers as a key role in the CSC and service brokerage as a growing market (Grivas, Kumar, & Wache, 2010; Hon et al., 2012). The majority of CSCs impacted by the incidents are not the exception to this tendency. Five cases show some type of service aggregation, demonstrating that cloud services are reshaping the ICT services supply chain, making it larger and more complex. The main findings of this study follow, by resilience principle:

Re(engineering): according to Bhatia, Lane, and Wain (2013) a critical area regarding "designing resilience-in" is the supply chain's transparency in terms of hidden dependencies that can lead to cascading failures. This was not a concern in the studied cases; all participants said they had established a clear baseline of their CSC structure and their cloud service architecture. However, most participants stressed how difficult it is to maintain that information given the highly dynamic environment. Many participants identified the use of standards as a common design coordination mechanism (Clemons & Chen, 2011; Simmonds et al., 2010) in their CSC. However, the majority of them also expressed their concern regarding building synergies along the service chain. One customer said,

> *"There are quite a few ICT resilience standards and guidelines, so many companies are working on these topics but usually their approach is on a single organisation … in this case, each member has to keep doing their job and see how to join efforts to their partners, building shared knowledge that is the toughest part."*

Collaboration: communication is essential in OR (Caralli et al., 2010b), however in supply chains there has not been a history of sharing information among members (Christopher & Peck, 2004). In the studied cases, all three types of CSC actors interviewed claimed their willingness to work collaboratively. As stated by one provider, *"They often rely on us to have some disaster recovery for them but we can only do it from the technical perspective, we encourage them to think about it and we are willing to come on board and give some suggestions and work through that, you know in coordination with us."*

Regarding information-sharing mechanisms for activities such as capacity planning, however, they agreed it is not a common practice, as expressed by two participants -a provider and a customer-,

"Unfortunately, often customers will not think that what they are doing will have any impact, it is part of benefit, right … they put it in the cloud and they don't need to know... They just scale magically, forecasting is something that we do on our own."

And,

"Telling our provider about demand changes? No, we expect them to meet our requirements, that simply! Not sure what we want to tell them."

Risk management culture: In a supply chain risks are magnified and cannot be mitigated by individual actors (Bhatia et al., 2013). Risk sharing requires continuous risk analysis, assessment, and report, however all participants agreed that specific internal and external drivers make CSC members more aware regarding risk-sharing management. One provider remarked,

"There are two cases: one where customers have not even thought about it, unfortunately! And the other where actually they heavily monitor us. Customers that really worry are generally larger, highly regulated or with some kind of mission-critical service with us."

Another participant observed,

"There is no formal policy, I mean there is a focus on risks but no regulatory environment … that changes the equation."

This shows that organisations that require high service levels or have to comply with regulations were most concerned about extending risk management culture into their CSC (Hon et al., 2012).

Agility: An accurate monitoring process is key to responding rapidly to changing conditions in a CSC (Lindner et al., 2010), however over half of the interviewees indicated monitoring their cloud services was not a high priority. Speaking to this point, a consumer explained, *“We do not want to know more than the basic stuff—that is why we went cloud with this service.”*

A broker stated,

“We have the capability to real-time monitor our service but that is a cost consumed by the hardware guys or by the customer and usually they do not want to take it up.”

And finally a provider observed,

“Well some of our customers don’t care and they don’t want to know, some just want to know they got the ability to, even if they don’t look at it and very few are really keen to know exactly what’s going on.”

In total over 70 different mechanisms were found and nearly half of them (32) concentrated on preventing the realisation of ICT operational risks to high-value services and on building capabilities to handle disruptive events. This finding aligns perfectly with the experts interviewed in Stage 1 who identified preventive mechanisms as a focal point (Section 8.3.2). Table 8.3 summarizes the top four coordination mechanisms by category and their occurrences. These six incidents provided a means for capturing rich data which was used to validate the potential utility the proposed model. All the participants found value in the model in terms of “structuring the OR conversation across the CSC.” Finally, while not the focus of this research, all participants emphasised that pre-contractual due diligence should not be overlooked.

8.4.2 Planning efforts

In OR tabletop exercises are the simplest type of exercise to conduct in terms of planning, preparation, and training (U.S. Department of Homeland Security, 2011). As described in the beginning of this section, simple tabletop exercises were conducted in order to identify coordination mechanisms that could improve CSC resilience in similar incident scenarios. The main findings are briefly outlined by resilience principle below and Table 8.3 ranks the mechanisms according to their occurrence (*).

	Protection	Response	Adaptation
(Re)engineering	*Architectural mechanisms* (6) Service delivery architecture baseline (5) RTO/RPO (4) Designing resilient services guidelines (3) Change control procedures *(3) Assets discovery tools *(2) Change schedule *(2) Change control procedures *(2) Collaborative capacity forecasting	*Flexibility mechanisms* (6) Incident detection and reporting procedures (4) Incident escalation procedures (2) Incident knowledgebase *(2) Incident knowledgebase	*Learning mechanisms* (5) Root-cause analysis report (2) Change procedures assessment (2) Updating plans (2) Updating incident knowledgebase *(4) Design guidelines assessment *(2) Change procedures assessment *(2) Updating plans *(2) Updating incident knowledgebase
Collaboration	*Situational awareness mechanisms* (6) Communication tools and techniques (6) Communication guidelines and standards (3) Base and derived measures (2) Stakeholders list *(3) Contextual information for interpreting results *(2) Stakeholders list *(1) Base and derived measures	*Synchronisation mechanisms* (6) Incident status report (6) Incident closure criteria (4) Incident escalation criteria (3) Communication channels deployment	*Alignment mechanisms* (4) Post-incident analysis report (4) Disputes resolution procedures (2) Communication channels assessment (2) Updating guidelines *(2) Post-incident analysis report *(2) Disputes resolution procedures *(1) Communication channels assessment

Risk management culture	*Vulnerability assessment mechanisms* (6) Frameworks/certification/codes of conduct (5) Resilience policy (4) Compliance guidelines and standards (2) Operational risk sources (taxonomy) *(4) Compliance knowledgebase *(4) Vulnerabilities repository - resolution status *(2) Vulnerabilities identification tools and techniques *(2) External/internal audits	*Control mechanisms* (6) Incident documentation (4) Requirements tracking (3) Evidence recording *(3) Evidence retention *(3) Evidence preservation *(2) Requirements tracking	*Embedment mechanisms* (2) Policies and guidelines enforcement (2) Remediation plans definition (2) Corrective actions tracking to closure (2) Resilience promotion *(4) Risk procedures assessment *(4) Remediation plans definition *(4) Corrective actions tracking to closure *(3) Compliance report analysis
Agility	*Visibility mechanisms* (6) Vital records, contracts and SLA repository (5) Monitoring scope definition (4) Collection, organisation and distribution of data (4) Governance scorecard repository *(3) Resilience awareness and training needs definition *(3) OR awareness / training material repository *(2) OR plans repository with updates *(2) Resilience exercises schedule	*Velocity mechanisms* (6) Incident analysis report (4) Real-time monitoring (2) Restoration procedures (2) Exercises documentation *(3) Potential non-compliance risk analysis *(2) Restoration procedures *(2) Exercises documentation	*Innovation mechanisms* (2) Update awareness/training requirements (2) Exercises assessment (1) Scorecard variance analysis *(4) Awareness/training activities assessment *(2) Update awareness/training requirements *(2) Exercises assessment *(1) Trends analysis

*Denotes coordination mechanisms that emerged from tabletop exercises

Table 8.3: CSC Resilience Coordination Mechanisms Ranked According to their Occurrence

Re(engineering): over half of the cases identified coordination mechanisms focused on strengthening collective engagement and taking advantage of their own experiences and lessons learnt from other organisations as key element to achieve continuous improvement.

Collaboration: in four cases, the interviewees observed a lack of understanding on the type of information that would be valuable to share across the service chain and how this flaw can led to false expectations. Speaking to this point, a participant stated,

"Creating content to be better prepared is a regular activity in OR but we need a common information model".

This finding supports the "motivation but actually lack of information sharing" found during the incidents analysis and is entirely supported by previous research in CSC (Lindner et al., 2010) that also considers a common vocabulary, widely understood and supported across the industry, as a key element to ensure appropriate integration in the service provision chain process. However, half of the cases agreed that sharing information in an international environment is not easy and most of time is discouraged because organisations could be held liable for the information they are disclosing (Hon et al., 2012).

Risk: four cases claimed to have focused most of their effort on implementing risk sharing mechanisms. They also stated that stablishing a systematic approach to aggregate information and have an accurate picture of the CSC risk is being challenging, however, embedding risk culture in the CSC has not been a priority even though it is perceived as a key element. In this direction most of the identified desirable mechanisms are pursuing this goal.

Agility: all participants agreed that when speaking of a high-value cloud services, supply chain members should be able to synthesise external and internal data and rapidly take action to minimise the exposure to and the impact of disruptions. However, continuously monitoring such dynamic is quite challenging, as a consumer explained,

"Customers can monitor themselves their OR conditions, for us it is absolutely critical and we do not have the expertise … we have gotten a measurement service broker, so far so good!"

Through the tabletop exercises evidence of lack of information flow mechanisms was discovered and discussed with the participants. The majority of them also commented that the exercise have provided them with,

"[A] systematic approach to identify key points that are being covered or need some attention".

8.5 Conclusions

There is widespread agreement in both industry and academia that cloud services are here to stay and will grow strongly in the future. The possibility of downtime and its potential impact on business is a serious concern for organisations and certainly a coordinated service supply chain approach is necessary to minimise risk. Following a two-stage qualitative inquiry, this research has proposed a conceptual model of coordination mechanisms for enhancing CSC resilience. Specifically, the model provides means for (1) identifying and organising actual coordination mechanisms by principles that underpin resilience in a supply chain and across resilience life cycle stages; and (2) guiding efforts to maintain and improve OR in CSC. From a methodological perspective, the contribution of this research lies in its viewing the cloud model as a supply chain to address the identified research problem by applying some of the well-known coordination concepts in the supply chain literature.

Using empirical data, this research has explored and described the OR coordination mechanisms that are being used by CSCs in order to prepare, handle, and learn from their disruptive incidents. This first observational validation was based on perceived utility, however the findings enhance the research community's understanding of the implications that adopting cloud as an ICT service sourcing model has on the OR domain. In addition, from a practitioner's perspective the model provides additional insight in the area of OR, where managerial decisions are especially important and the model can be used for guiding effort on selecting and/or enhancing specific coordination mechanisms in order to manage dependencies throughout the three disruption stages in a CSC.

Even more important, this paper identifies opportunities for future research particularly related to information flow mechanisms. This study's methodological limitations also point towards other opportunities. Findings from qualitative research are derived from perceptions and opinions of a limited number of informants. The empirical study only analysed coordination mechanisms among consumers, brokers, and providers, however cloud services also depend on internet connectivity which usually involves relationships with telecommunication providers. The authors do not discuss this link in CSCs which represents a possible point of failure. Also, cloud consumers may have their own individual end users; this relationship was outside this study's scope. Therefore, this study should be extended to cover a complete CSC through an in-depth case study as more data is required to refine and generalise its findings.

In the future CSCs will need to become more resilient to meet higher expectations of cloud consumers and specific coordination mechanisms will be needed to improve performance and responsiveness, all of which demonstrates the potential of this emergent research area.

Acknowledgment

The authors would like to thank the experts and the New Zealand companies for their contribution to the results.

8.6 References

Arean, O. (2013). Disaster recovery in the cloud. *Network Security, 2013*(9), 5-7.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Gunho L., Patterson D., Rabkin A., Stoica I. & Zaharia, M. (2010). A view of cloud computing. Commununications of the ACM, 53(4), 50-58. doi: 10.1145/1721654.1721672.

Bhatia, G., Lane, C., & Wain, A. (2013). Building resilience in supply chains: World Economic Forum.

British Standards Institute. (2014). BS 65000:2014 Guidance on organizational resilience.

Cao, C., & Zhan, Z. (2011). *Incident management process for the cloud computing environments.* Paper presented at the 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS).

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). CERT® Resilience management model v1.0: improving operational resilience processes (S. E. Institute, Trans.): Carnegie Mellon.

Chen, R., Sharman, R., Rao, H. R., & Upadhyaya, S. J. (2008). Coordination in emergency response management. *Communications of the ACM, 51*(5), 66-73.

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The international journal of logistics management, 15*(2), 1-14.

Clemons, E. K., & Chen, Y. (2011). *Making the decision to contract for cloud services: managing the risk of an extreme form of IT outsourcing.* Paper presented at the 44th Hawaii International Conference on System Sciences (HICSS),.

Cloud Security Alliance. (2011). Security guidance for critical areas of focus in cloud computing V3.0.

Cockram, D. (2012). Organisational resilience. In T. B. W. Group (Ed.), *A BCI Working Group White Paper*: Business Continuity Institute.

Crowston, K., & Osborn, C. S. (2003). A coordination theory approach to process description and redesign. In T. W. Malone, K. Crowston & G. A. Herman (Eds.), *Organizing business knowledge: the MIT process handbook*: MIT press.

Dalziell, E., & McManus, S. (2004). *Resilience, vulnerability and adaptive capacity: implications for system performance*. Paper presented at the International Forum for Engineering Decision Making.

Dekker, M. (2012). Critical Cloud Computing: A CIIP perspective on cloud computing services: European Network and Information Security Agency (ENISA).

Dutta, A., Peng, G. c. a., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of its experts. *Journal of Computer Information Systems, 53*(4).

Fischer, F., & Turner, F. (2009). Cloud computing as a supply chain. *Walden University*.

Gartner. (2012). Gartner says worldwide cloud services market to surpass $109 billion in 2012 [Press release]. Retrieved from http://www.gartner.com/newsroom/id/2163616.

Grivas, S. G., Kumar, T. U., & Wache, H. (2010). *Cloud broker: bringing intelligence into the cloud.* Paper presented at the IEEE 3rd International Conference on Cloud Computing (CLOUD), 2010.

Grobauer, B., & Schreck, T. (2010). *Towards incident handling in the cloud: challenges and approaches*. Paper presented at the Proceedings of the 2010 ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA.

Herrera, A., Beltran, F., & Janczewski, L. (2014). *Resilient organisations in the cloud.* Paper presented at the The 25th Australasian Conference on Information Systems, Auckland, New Zealand.

Herrera, A., & Janczewski, L. (2013). *Modelling organisational resilience in the cloud.* Paper presented at the PACIS 2013 Proceedings. Paper 275.

Herrera, A., & Janczewski, L. (2014). Issues in the study of organisational resilience in cloud computing environments. *Procedia Technology, 16*(0), 32-41. doi: http://dx.doi.org/10.1016/j.protcy.2014.10.065

Herrera, A., & Janczewski, L. (2015). *Cloud supply chain resilience: a coordination approach.* Paper presented at the 14th International Information Security South Africa Conference (ISSA), Johannesburg.

Hon, W. K., Millard, C., & Walden, I. (2012). Negotiating cloud contracts-looking at clouds from both sides now. *Stanford Technology Law Review, 16*(1), 79-128.

IBM Global Technology Services. (2014). Resilience in the era of enterprise cloud computing *Thought leadership white paper*.

International Data Corporation. (2013). Worldwide and regional public it cloud services 2013–2017 forecast [Press release]. Retrieved from http://www.idc.com/getdoc.jsp?containerId=242464.

ISACA. (2012). Guiding principles for cloud computing adoption and use. *Cloud Computing Vision Series*.

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security, 20*(5), 332-349.

Kaliski Jr, B. S., & Pauley, W. (2010). *Toward risk assessment as a service in cloud environments.* Paper presented at the Proceedings of the 2nd USENIX Workshop on Hot Topics in Cloud Computing.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and operations management, 14*(1), 53-68.

Lindner, M., Galán, F., Chapman, C., Clayman, S., Henriksson, D., & Elmroth, E. (2010). *The cloud supply chain: a framework for information, monitoring, accounting and billing.* Paper presented at the 2nd International ICST Conference on Cloud Computing (CloudComp 2010).

Lindner, M., McDonald, F., Conway, G., & Curry, E. (2011). *Understanding cloud requirements-a supply chain lifecycle approach.* Paper presented at the Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization CLOUD COMPUTING 2011.

Linstone, H. A., & Turoff, M. (2002). *The delphi method: techniques and applications* (Vol. 53): Addison-Wesley.

Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. *ACM Computing Surveys, 26*(1), 87-119. doi: 10.1145/174666.174668

Martens, B., & Teuteberg, F. (2011). *Risk and compliance management for cloud computing services: designing a reference model.* Paper presented at the AMCIS.

Maurer, F., & Lechner, U. (2014). *From disaster response planning to e-resilience: a literature review.* Paper presented at the BLED 2014 Proceedings. Paper 32.

McCracken, G. (1988). *The long interview* (Vol. 13): Sage.

Mell, P., & Grance, T. (2011). The NIST Definition of cloud computing special publication *(SP) 800-145*. Gaithersburg, MD: US National Institute of Standards and Technology (NIST).

Morisse, M., & Prigge, C. (2014). *Business continuity in network organizations–a literature review.* Paper presented at the Twentieth Americas Conference on Information Systems, Savannah.

Myers, M. D. (2009). *Qualitative research in business and management*. London, UK: SAGE Publications.

Oppenheimer, D., Ganapathi, A., & Patterson, D. A. (2003). *Why do Internet services fail, and what can be done about it?* Paper presented at the USENIX Symposium on Internet Technologies and Systems.

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: development of a conceptual framework. *Journal of Business Logistics, 31*(1), 1-21.

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The international journal of logistics management, 20*(1), 124-143.

Ried, S., & Kisker, H. (2011). Sizing the cloud: understanding and quantifying the future of cloud computing: Forrester.

Saripalli, P., & Walters, B. (2010). *QUIRC: A Quantitative impact and risk assessment framework for cloud security.* Paper presented at the IEEE 3rd International Conference on Cloud Computing (CLOUD), 2010.

Sheffi, Y. (2005). *The resilient enterprise: overcoming vulnerability for competitive advantage* (Vol. 1): MIT Press Books.

Shim, J., & Lim, Y. (2013). Implementation of real time alert system over cloud computing. *International Journal of Energy, Information & Communications, 4*(3).

Simatupang, T. M., Victoria Sandroto, I., & Hari Lubis, S. (2004). Supply chain coordination in a fashion firm. *Supply Chain Management: An International Journal, 9*(3), 256-268.

Simmonds, D., Collins, R. W., & Berndt, D. (2010). *Coordinating the relationship between it services providers and clients: the case of cloud computing.* Paper presented at the Proceedings of SIGSVC Workshop.

Soni, U., Jain, V., & Kumar, S. (2014). Measuring supply chain resilience using a deterministic modeling approach. *Computers & Industrial Engineering, 74*, 11-25.

Spring, J. (2011a). Monitoring cloud computing by layer, part 1. *Security & Privacy, IEEE, 9*(2), 66-68.

Spring, J. (2011b). Monitoring cloud computing by layer, part 2. *Security & Privacy, IEEE, 9*(3), 52-55.

Troshani, G. R., & Wickramasinghe, N. (2011). *Cloud nine? an integrative risk management framework for cloud computing.* Paper presented at the Proceedings of Bled Conference.

U.S. Department of Homeland Security. (2011). Communications-Specific Tabletop Exercise Methodology (pp. 110): SAFECOM.

Wilson, R. L. (2010). *Organizational resilience models applied to companies in bankruptcy.* (Doctor of Management), University of Maryland University College, United States -- Maryland.

Xu, L., & Beamon, B. M. (2006). Supply chain coordination and cooperation mechanisms: an attribute-based approach. *Journal of Supply Chain Management, 42*(1), 4-12.

9 Conclusion

This thesis has explored the topic of organisational resilience in cloud computing environments from an ICT readiness perspective. Four main research questions were developed and explored within a conceptual framework that was constructed through the writing of the five original articles presented in Chapters 4–8. This concluding chapter first summarises the key findings of this research. Next, the contributions of the research and its practical implications are summarised. Finally, the limitations of the research and directions for future studies are discussed.

9.1 Summary of the Research

According to Carroll and Swatman (2000), a conceptual framework includes the research themes, which set out the main areas of interest; the literature, which provides the current knowledge and theories in the areas of interest; the insights from personal experiences, experts in the field and practitioners, which provides contextual knowledge; and the theoretical foundations, which clarify the researcher’s assumptions and expectations about the world. These elements were incorporated into the framework which, following the process proposed by Mingers (2001), was divided into three main stages: Exploration, Analysis, and Validation.

As often happens with qualitative research, this research was motivated by the explicit interest of the researcher – based on her professional and academic experience – in the topic of ICT operational resilience preparedness in cloud computing environments, and began by reviewing the relevant research landscapes. Using the conceptual framework discussed in Chapter 3 and presented in Figure 9.1, the researcher was able to refine the research topic and focus the investigation. This section summarises the key findings from this research process.

The main purpose of the first stage, Exploration, was to identify the specific research problem within its context. An initial literature review allowed the researcher to gain some understanding of the research area and led to the research problem being defined as:

> *Research Problem: There is a need to strengthen the ability of organisations to not only survive but also thrive when exposed to disruptive incidents within a cloud environment.*

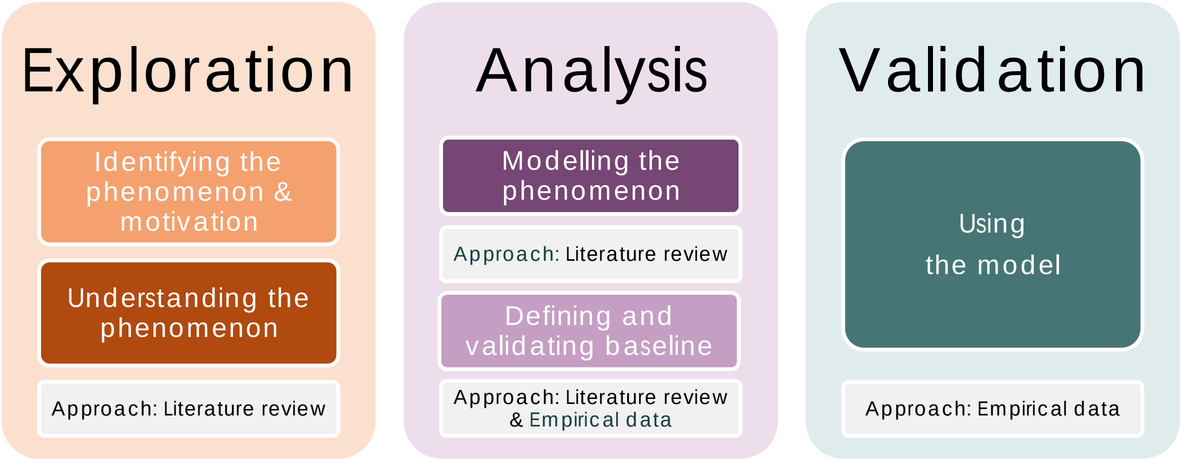

Exploration
Identifying the phenomenon & motivation
Understanding the phenomenon
Approach: Literature review
Analysis
Modelling the phenomenon
Approach: Literature review
Defining and validating baseline
Approach: Literature review & Empirical data
Validation
Using the model
Approach: Empirical data

Figure 9.1: Conceptual Framework

At this stage the researcher also became aware of the importance of building organisational resilience in partnership with others. Article I therefore suggested that coordination theory (Malone & Crowston, 1994) should be applied to analyse organisational resilience processes in terms of different actors performing interdependent activities, particularly when some processes have moved outside of the traditional organisational boundaries, as is the case with cloud services. Consequently, this research then focused on identifying how ICT operational resilience activities and coordination mechanisms among them should be adjusted within a cloud environment in order to make it more resilient. Article I proposed developing a conceptual model as a tool for guiding efforts in this direction and this led to the research objective being defined as:

> *Research Objective: To provide a conceptual tool for guiding efforts to maintain and improve resilience within a cloud environment.*

With this objective in mind, a conceptual understanding of the phenomenon was needed as there has been little research in this area. A review of the literature on cloud computing as an ICT sourcing model and on organisational resilience from an ICT operational perspective led to the development of the first research question:

> *Research Question 1: How do the main reference architecture characteristics of cloud computing environments affect the ICT operational resilience requirements?*

Article II presented a multi-level research framework designed to address the major issues related to the study of organisational resilience in cloud computing environments from an ICT perspective. The purpose of this framework was to identify the major differences between ICT operational resilience within a cloud computing environment compared to an in-house environment. Based on the cloud computing baseline reference architecture compiled, Article II suggested that regardless of the many forms that cloud services can take according to their delivery models and deployment models, the five essential characteristics - on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service - that distinguish them from other ICT service-based sourcing models always apply, together with the highly dynamic environment that results from them. Accordingly, Article II also argued that the conceptual model should focus on organisational resilience challenges derived from these characteristics.

The next step was to incorporate the conceptual understanding gained about the research topic into the conceptual tool. Therefore the main purposes of the second stage, Analysis, were to define a sound baseline as the starting point for the model and to propose the model itself. Regarding the former, based on the research framework and on an extensive review of the relevant literature, Article III identified three essential elements for the model's baseline: the foundations on which the model is developed; the specific organisational resilience challenges that the model addresses; and the high-level representation.

Given the importance of this baseline, a preliminary assessment by a group of domain experts was organised. The main findings and insights of this assessment were presented in the first section of Article V, "Initial Conceptualisation Validation". As part of the research process and in order to incorporate these findings, a deliberate reflection and critical analysis took place, which revealed that the problem under study is perceived and framed in practice from a supply chain perspective. Almost all the interviewees stated that it would be more beneficial to analyse how organisational activities can best be coordinated across the cloud supply chain instead of identifying changes in specific ICT operational processes and the coordination mechanisms among them derived from sourcing ICT services from a cloud environment.

The most important outcome of this first part of the Analysis stage, in addition to the baseline itself, was the conceptual framework's evolution, enabling its review and refining its theoretical perspective. The domain experts' insights provided additional contextual knowledge, allowing the researcher to reframe the research problem in terms of a supply chain approach. Accordingly, the research problem and the main objective were reworded as:

> *Research Problem: There is a need to strengthen the ability of organisations to not only survive but also thrive when exposed to disruptive incidents within a cloud supply chain.*

> *Research Objective: To provide a conceptual tool for guiding efforts to maintain and improve resilience in cloud supply chains.*

In the second part of the Analysis stage, previous research on supply chain resilience and coordination mechanisms was reviewed, which led to the development of the second research question:

> *Research Question 2: How can ICT resilience activities best be coordinated across the cloud supply chain in order to make this supply chain become more resilient?*

Article IV examined elements that facilitate the attainment of resilience in a supply chain and proposed a conceptual model with a set of coordination mechanisms that positively impact ICT operational resilience processes across cloud supply chains based on the four principles that underpin resilience in a supply chain defined by Christopher and Peck (2004): (re)engineering, collaboration, risk management culture and agility. Article IV also proposed that in order to analyse the ways in which coordination is accomplished and how coordination mechanisms adapt to non-routine conditions in this type of supply chain, distinctions between the three stages of the organisational resilience lifecycle – preventive, continuity and improvement – need to be made.

The main purpose of the last stage of this research, Validation, was to validate the proposed model. An empirical analysis of coordination mechanisms in cloud supply chains was therefore developed, leading to the formulation of the last two research questions:

> *Research Question 3: Is the model able to capture the richness of a real cloud incident?*

> *Research Question 4: Is the model perceived as a useful tool for guiding efforts in maintaining and improving cloud supply chain resilience?*

Primary data from cloud incidents faced by major players in different cloud supply chains in the New Zealand cloud services market were collected through two methods. First, using semi-structured interviews the incidents were reconstructed in terms of the model. Second, in order to validate the model's perceived usefulness tabletop exercises were conducted. Article V argued that the model provides a means for capturing rich data from cloud incidents structuring the organisational resilience conversation across cloud supply chains. It also provided a systematic approach to identify key points that are being covered or need attention in order to maintain and improve cloud supply chain resilience.

By following this approach, this thesis has explored coordination mechanisms that can be used for planning and decision making to prevent, respond to and learn from ICT disruptive incidents across a cloud supply chain. Table 9.1 summarises the research problem, the specific research objective and the four associated research questions.

Research Problem	There is a need to strengthen the ability of organisations to not only survive but also thrive when exposed to disruptive incidents within a cloud supply chain
Research Objective	To provide a conceptual tool for guiding efforts to maintain and improve resilience in cloud supply chains
Research Question 1	How do the main reference architecture characteristics of cloud computing environments affect the ICT operational resilience requirements?
Research Question 2	How can ICT resilience activities best be coordinated across the cloud supply chain in order to make this supply chain become more resilient?
Research Question 3	Is the model able to capture the richness of a real cloud incident?
Research Question 4	Is the model perceived as a useful tool for guiding efforts in maintaining and improving cloud supply chain resilience?

Table 9.1: Summary of Research Problem, Research Objective and Associated Research Questions

The answers to these research questions should be of interest and value to academic researchers in the information systems and organisational resilience fields, as well as to practitioners such as operational risk advisors, business continuity professionals, ICT services advisors, and cloud services architects, as there is widespread agreement in both industry and academia that cloud services are here to stay and will grow strongly in the future. The possibility of downtime due to disruptions and its potential impact on business is a serious concern for organisations and a coordinated service supply chain approach is undoubtedly needed to minimise risk.

9.2 Contributions to Research and Practical Implications

This section summarises the multiple contributions of this research, and identifies its practical implications for practitioners in the field. From the research perspective, there are four major contributions.

First, this research advances knowledge on inter-organisational coordination mechanisms, specifically coordination mechanisms for dealing with cloud services disruptive events. By drawing on supply chain resilience formative concepts, this research proposed a set of mechanisms to handle coordination issues that jeopardise the attainment of resilience in a cloud supply chain. There has been a call to find “new ways of dealing with and overcoming inevitable supply chains disruptions” (van der Vegt et al., 2015, p. 12). Focusing specifically on cloud supply chains, this thesis suggests that coordination plays a key role in order to analyse organisational resilience processes in terms of different actors performing interdependent activities. Most previous research has focused on how or why coordination occurs within a single organisation and findings have shown that in dynamic environments with a high level of vertical disintegration on a cross-border basis such as in a cloud supply chain, traditional mechanisms are often insufficient for coordinating the resulting interdependencies among organisations (Gittell & Weiss, 2004). Hence, it is appropriate to focus research efforts on exploring inter-organisational coordination mechanisms in both routine and non-routine conditions in order to address the risk of disruption across members in a cloud supply chain.

Second, by examining organisational resilience as ICT services move into cloud computing environments from an ICT operational perspective, this research provides a greater understanding of the relationships between organisational resilience and this type of ICT services sourcing model by proposing a multi-level research framework. The macro level of the framework captures three dimensions: principles (Behrendt et al., 2011; Liu et al., 2012; Oracle Corporation, 2012); actors (Behrendt et al., 2011; Liu et al., 2011); and architecture building blocks (Behrendt et al., 2011; Cisco Systems, 2011; Cloud Security Alliance, 2013; Liu et al., 2011; Liu et al., 2012; Oracle Corporation, 2012). The micro level of the framework analyses linkages among resilience process areas (Caralli et al., 2010b) in order to identify dependencies that should be considered when studying a specific process area. This multi-level research framework was designed to address the major issues related to the study of organisation resilience in cloud computing environments from an ICT perspective. While this research framework is not an all-inclusive roadmap of current key issues in this area, the issues covered by the framework are based on a literature review of cloud computing architectures and existing organisational resilience specifications and it is intended as a potential starting point for researchers wanting to understand the relationships between cloud computing environments and ICT operational resilience.

Third, this research provides a conceptual model of coordination mechanisms for enhancing cloud supply chain resilience. Specifically, the model provides means for (1) identifying and organising existing coordination mechanisms by the supply chain resilience principles and across resilience life cycle stages; and (2) guiding efforts to maintain and improve organisational resilience in this type of supply chain. The main contribution of this research to the body of knowledge is the conceptualisation and underpinning of the ICT operational resilience development in cloud environments founded on the four supply chain resilience principles. This research therefore contributes to the ICT resilience and business continuity literature that mostly focuses on standard processes and mechanisms within a single organisation (Järveläinen, 2012). In addition, the model incorporates the three stages of the organisational resilience lifecycle, allowing for a better understanding of the ways in which coordination is accomplished and how coordination mechanisms change according to different operating conditions in this type of supply chain.

Fourth, this research empirically validates the proposed conceptual model by studying how major players in different cloud supply chains in the New Zealand cloud services market – consumers, brokers and providers – perform coordinated ICT operational resilience activities and by identifying the main challenges they face, particularly during non-routine conditions. The empirical findings suggest the value of the model in terms of structuring the organisational resilience conversation across cloud supply chains. Based on the specific resilience goals defined by the four supply chain resilience principles, the model provides coordination mechanisms which integrate parties in a cloud supply chain, enabling them to work collectively on interdependent resilience activities in order to achieve those goals. For instance, whereas the (re)engineering principle ensures resilience is designed to increase the number of changes that the cloud supply chain is able to cope with, agility focuses on the efficiency of the cloud supply chain's coordination mechanisms throughout the three stages. In addition, since cloud supply chain resilience is an inter-organisational concept, all parties need to align efforts in both routine and non-routine conditions in order to handle potential risk events. Collaboration in this area relates to the cloud supply chain members' willingness to share even sensitive risk information, creating a risk management culture within the cloud supply chain. This unique perspective allows researchers to design and validate new inter-organisational coordination mechanisms and thereby contribute to the cloud supply chain resilience literature.

This research also has significant practical implications. The research framework developed in this thesis is intended to guide organisations in understanding how sourcing ICT services from a cloud supply chain can impact their ICT operational activities. The framework highlights the dynamic nature of cloud services and the need to meet demands for inter-organisational coordination throughout the service supply chain.

Specifically at the capabilities level, the framework suggests a targeted improvement roadmap according to the linkages among resilience process areas and dependencies that arise from highly dynamic cloud environments and from moving some of these processes outside traditional corporate boundaries. For instance, the Monitoring process area that “focuses on the activities the organization performs to collect, record, and distribute relevant data to the organization for the purposes of managing resilience and providing data for measuring process effectiveness” (Caralli, Allen, Curtis, White, & Young, 2010c, p. 1) is identified as a key issue when sourcing ICT services from a cloud supply chain. Some essential characteristics of cloud services, such as being “measured services”, require the collection of much more detailed information given the focus on costs and dynamic resources sharing. Many activities depend on monitoring capabilities, for instance supply chain members need to be able to synthesise external and internal data, and to rapidly take action to minimise the exposure to, and impact of, disruptions. These findings reinforce the key role of monitoring in this type of supply chain and the need for an infrastructure that supports and enables cloud services monitoring needs and capabilities and methods to analyse vast amounts of operating conditions data. This also ties into the finding from the validation of the conceptual model during which participants repeatedly mentioned that accurate and real-time information in a highly dynamic environment is difficult to collect, share, and properly use.

Next, the conceptual model represents a fundamental shift from the traditional ICT operational resilience readiness model, which is based upon a single firm. An organisation’s organisational resilience is directly related to the resilience of the other organisations on which it depends and therefore the proposed model clearly establishes a shared responsibility among all parties in a cloud supply chain – consumers, brokers and providers – in making it more resilient. Therefore, in order for a cloud supply chain to meet individual organisational drivers such as an organisation’s strategic objectives, risk appetite and operational constraints, coordination mechanisms must be in place throughout the entire service chain to achieve both developmental and operational goals across the three stages of the organisational resilience lifecycle. For organisations looking to source, or are currently sourcing, their ICT services from a cloud supply chain, this fundamental shift raises awareness of the need to rethink their ICT resilience readiness in terms of building resilience across their networks.

Furthermore, the researcher believes that the main implication of this thesis for practitioners – specifically operational risk advisors, business continuity professionals, ICT services advisors, and cloud services architects – is the set of resilience coordination mechanisms provided by the cloud supply chain resilience model. These coordination mechanisms can be used to strengthen the ability of organisations to not only survive but also thrive when exposed to disruptive incidents within a cloud supply chain. The coordination mechanisms are organised across the three supply chain resilience stages and address coordination issues that jeopardise the attainment of the four supply chain resilience principles:

> *Coordination mechanisms for protection*: To prevent the realisation of ICT operational risk to high-value services in the cloud supply chain and to build capabilities to handle a disruptive event in an effective way.
>
> *Coordination mechanisms for response*: To sustain a high-value service in the cloud supply chain if a risk is realised, addressing its consequences to the cloud supply chain members effectively, and to return the cloud supply chain to the normal state.
>
> *Coordination mechanisms for adaptation*: To systematically improve the achievement of the two previous goals in the cloud supply chain.

Thus, the conceptual model addresses the cloud supply chain's ability to cope with disruptive events, to return to its original operations, or to move to a new, more desirable state after being disturbed by leveraging knowledge from supply chain resilience research, which offers a complementary perspective in order to guide efforts to maintain and improve ICT operational resilience in cloud supply chains.

9.3 Limitations and Future Work

This section summarises the limitations of this research and makes suggestions for future work in this area.

With regard to limitations, firstly this research focused solely on the cloud computing's essential characteristics as a key difference between this type of ICT services sourcing model and other ICT services-based sourcing models, therefore specific organisational resilience challenges derived from a particular delivery and/or deployment model are not explicitly addressed. Future studies should examine potential challenges that come from these other cloud components. A second limitation is that both the initial conceptualisation of the validation and the empirical study were derived from perceptions and opinions of a limited number of informants. The latter only analysed coordination mechanisms among cloud consumers, cloud brokers, and cloud providers, however cloud supply chains rely on network connectivity which generally involves relationships with telecommunication providers. This additional type of actor represents a possible point of failure in a cloud supply chain, however the role of telecommunication providers was not explicitly discussed in this research. Similarly, cloud consumers may have their own end users and this relationship was also outside the scope of this research. The researcher believes that studying an entire cloud supply chain through an in-depth case study, including these two additional actors, would substantially benefit our understanding of the cloud supply chain resilience concept. A third limitation is that many, if not all, of the identified categories of coordination mechanisms require intensive information sharing. An important challenge when sharing information, particularly in a competitive and cross-border market such as the cloud services market, is legal liability. Organisations sometimes worry that information sharing will put them at a competitive disadvantage or expose them to possible legal risks, and this reality could definitely limit the applicability of the proposed model.

This research has provided a conceptual tool for guiding efforts to maintain and improve resilience in cloud supply chains. Despite the positive results from the empirical study regarding its perceived usefulness, more work is required on validating this particular aspect. The researcher believes that studying the performance of cloud supply chains over a longer period of time in order to collect enough data to analyse the relationship between the model and/or specific types of coordination mechanisms, and their ability to improve cloud supply chain resilience, is needed.

The researcher also acknowledges that organisational resilience can be interpreted as a complex organisational behaviour and that consequently many other theoretical lenses could be applied to investigate how to maintain and improve resilience in a cloud supply chain. This opens a number of research avenues, for instance an investigation into the factors that determine how a cloud supply chain transform its resilience ability into concrete cloud supply chain demonstrations of resilience. In this direction, other concepts such as emergent and evolving behaviours, especially trust establishment and mutuality (Campbell, 1997), could be addressed by future studies explicitly in the context of cloud supply chains in order to analyse their role in achieving mutual resilience goals.

In addition, future research should consider the cost of creating resilient cloud supply chains. Coordination itself implies costs, particularly when big amounts of data need to be collected, properly analysed, and distributed. The challenge then is to find ways to make a cloud supply chain more resilient while maintaining its economic viability.

In conclusion, it is clear that as the evolution of cloud computing continues, cloud supply chains will take on a greater role within organisations. Likewise, as ICT delivery models change and become more complex, the business environment is fast becoming more interconnected and volatile, and the consequences of external events and disruptions more substantial. This dynamic environment will be further complicated by higher expectations on the part of cloud consumers and cloud supply chains resilience activities will need to improve in terms of higher levels of availability, performance and responsiveness, all of which demonstrates the potential of this emergent research area.

10 APPENDIX ONE – PRELIMINARY ASSESSMENT

PARTICIPANT INFORMATION SHEET

DEPARTMENT OF INFORMATION SYSTEMS AND OPERATIONS MANAGEMENT

PROJECT TITLE: RESILIENT ORGANISATIONS IN THE CLOUD

Researchers: Andrea Herrera PhD candidate, Dr. L Janczewski Supervisor and Dr. F Beltrán Co-supervisor

THE UNIVERSITY OF AUCKLAND
BUSINESS SCHOOL

Owen G. Glenn Building
4th floor, 12 Grafton Road
Auckland 1142, New Zealand
Telephone 64 9 373 7599
Facsimile 64 9 373 7430
www.isom.auckland.ac.nz

The University of Auckland
Private Bag 92019
Auckland 1142
New Zealand

My name is Andrea Herrera. I am a doctoral student at The University of Auckland at the Department of Information Systems and Operations Management. Together with my supervisors, Dr. L Janczewski and Dr. F Beltrán, we are investigating organisational resilience (OR) in cloud computing environments (CCE) from an ICT perspective. You are being invited to participate in this research project and I would appreciate any assistance that you can offer me.

Project description

The purpose of the research is to investigate how the adoption of cloud computing affects OR requirements particularly from an ICT operational perspective. It aims to formulate a conceptual model that integrates key theoretical and practical requirements for ICT operational resilience management focusing on the changes that cloud environments introduce. It is expected that this model can be used by organisations as a method for planning and decision making to anticipate, prevent, prepare for, and respond to an ICT disruptive incident when working in this type of environment. A single method approach will collect information from industry experts, academics, governmental representatives and non-governmental organisations in order to develop knowledge and models to gain a better understanding of the changes and challenges that CCE introduce in operational resilience activities. Practical applicability of the results is a major aim of this study and will be demonstrated through a conceptual model including potential mechanisms to coordinate joint resilience-efforts among consumers and providers. You have expressed interest of participating in this research and given your expertise in this field, my supervisors and I are very interested in the opinions and insights that you can provide us with.

Project procedures

Semi-structured interviews involve the use of some pre-formulated questions but some new questions might emerge during the conversation. Each interview should not require more than 1 hour. The participants of this study on OR are all experts in the field albeit with different backgrounds. This study will be conducted either face-to-face at the University's facilities or over Skype depending on the preference and location of the participant.

Participation and withdrawal

I would like to audio-record the interview, however, you can ask me to stop recording at any point during the interview. Also, you may choose to stop participating at any time during the interview and you may choose to withdraw your data any time up to two weeks after the interview.

Confidentiality and use of data

All information you provide during the interview will be kept confidential by the researchers. The data you provide will be used in my doctoral thesis and in academic publications. Your data will be made de-identified to attempt that you cannot be identified as the source of information. However, as an expert in this field you may be identifiable. You can request a copy of any publications resulting from this research.

Storage and disposal of data

All consent forms and data gathered will be stored securely at the University of Auckland for a period of 6 years, and will be securely destroyed at the end of this period. All electronic data will be password-protected and will be securely erased at the end of this period. If you agree to participate in this research, please read and sign the attached consent form.

Thank you very much for your time and help in making this study possible. Should you require any further information please do not hesitate to contact us.

Researcher

Andrea Herrera
a.herrera@auckland.ac.nz
ISOM Department
The University Of Auckland, Private Bag 92019
Auckland 1142, New Zealand

Supervisor

Dr L Janczweski
lech@auckland.ac.nz
Telephone 64 9 373 7599 x 87538
ISOM Department
The University Of Auckland, Private Bag 92019,
Auckland 1142, New Zealand

Co-supervisor

Dr F Beltrán
f.beltran@auckland.ac.nz
Telephone 64 9 373 7599 x 87850
ISOM Department
The University Of Auckland, Private Bag 92019,
Auckland 1142, New Zealand

Head of Department

Professor Michael Myers
m.myers@auckland.ac.nz
Telephone 64 9 373 7599 x 87468
ISOM Department
The University Of Auckland, Private Bag 92019,
Auckland 1142, New Zealand

For ethical concerns, contact The Chair of the Ethics Committee

The University of Auckland Human Participants Ethics Committee,
Office of the Vice-Chancellor,
The University Of Auckland, Private Bag 92019,
Auckland 1142, New Zealand
Telephone: 64 9 373 37599 x83711

APPROVED BY THE UNIVERSITY OF AUCKLAND HUMAN PARTICIPANTS ETHICS COMMITTEE ON 09th April 2014 for (3) years. Reference Number 011218

INTERVIEW PROTOCOL

THE UNIVERSITY OF AUCKLAND
BUSINESS SCHOOL

Department of ISOM
Level 4, Owen G Glenn Building
12 Grafton Road
Auckland
New Zealand

Telephone: (+64)93737599
The University of Auckland
Private Bag 92019
Auckland
New Zealand

Project Title: Resilient Organisation in the Cloud

Researcher: Andrea Herrera

Supervisors: Dr Lech Janczewski, and Dr Fernando Beltrán

Interviewer: ______________________

Please note that in a semi-structured interview, data gathering tends to be open-ended. Therefore, data gathered from one interview session could suggest directions to pursue in subsequent interview sessions. Therefore, it is not possible to present a complete inventory of all the questions that might be asked in the interviews. However, all questions are structured around three main categories: (1) the main changes introduced by consuming cloud services; (2) the main challenges of managing dependencies in a cloud environment; and (3) the main mechanisms used to coordinate efforts among all involved parties. The following questions give you an idea of the issues that will be explored. It is important to mention that all these questions are going to be conversed from an organisational resilience (OR) / business continuity (BC) perspective:

1. What are the main changes that the adoption of cloud computing environments (CCE) as ICT service delivery model introduces from a consumer's perspective?

2. From an operational management perspective, what category of processes (Enterprise[3], Engineering[4], Operations[5] and Process[6]) is the most affected by the adoption of CCE? Why?
3. Classifying resilience strategies into preventive, continuity and improvement which of them is the most affected by the adoption of CCE? Why?
4. The definition and management of high-value organisational assets is fundamental in all OR /BC programs, how does this process change by the introduction of an ICT service delivery model such as CCE?
5. From a cloud consumer perspective there is a clear strong external dependency on its CC providers, what are the main challenges of the ongoing management of those dependencies to ensure that appropriate resilience measures are in place to protect and sustain the consumer organisation's services and assets?
6. Exercising continuity strategies plays a fundamental role in all OR/BC programs, how joint continuity strategies should be tested to ensure their effectiveness?
7. When facing disruptive incidents, what processes and mechanisms should be used to communicate and coordinate activities among incident response teams?
8. What are the main challenges when implementing those communication and coordination processes and mechanisms?
9. Monitoring is an enterprise-wide activity that organisations use to "take the pulse" of their day-to-day operations, how monitoring activities are affected by the adoption of CCE?
10. How lessons learned from identifying, analysing, and responding to incidents should be translated into actions to improve resilience strategies, particularly those that require a joint effort between providers and consumers?

APPROVED BY THE UNIVERSITY OF AUCKLAND HUMAN PARTICIPANTS ETHICS COMMITTEE ON 09th April 2014 for (3) years. Reference Number 011218

[3] Represent processes and mechanisms that are essential to broadly supporting OR

[4] Processes and mechanisms that establish the basic building blocks for resilience and create the foundation to protect and sustain assets and consequently the business processes that those assets support

[5] Represent the core activities for managing the operational resilience of assets and services in the operations life-cycle phase

[6] Represent those that are focused on measuring, managing, and improving OR

11 APPENDIX TWO – MODEL VALIDATION

PARTICIPANT INFORMATION SHEET

DEPARTMENT OF INFORMATION SYSTEMS AND OPERATIONS MANAGEMENT

PROJECT TITLE: RESILIENT ORGANISATIONS IN THE CLOUD

Researchers: Andrea Herrera PhD candidate, Dr. L Janczewski Supervisor and Dr. F Beltrán Co-supervisor

THE UNIVERSITY OF AUCKLAND
BUSINESS SCHOOL

Owen G. Glenn Building
4th floor, 12 Grafton Road
Auckland 1142, New Zealand
Telephone 64 9 373 7599
Facsimile 64 9 373 7430
www.isom.auckland.ac.nz

The University of Auckland
Private Bag 92019
Auckland 1142
New Zealand

My name is Andrea Herrera. I am a doctoral student at The University of Auckland at the Department of Information Systems and Operations Management. Together with my supervisors, Dr. L Janczewski and Dr. F Beltrán, we are investigating organisational resilience (OR) in organisations working in cloud computing environments (CCE) from an ICT perspective. You are being invited to participate in this research project and I would appreciate any assistance that you can offer me.

Project description

The purpose of the research is to investigate how the adoption of cloud computing affects OR requirements particularly from an ICT operational perspective. It aims to formulate a conceptual model that integrates key theoretical and practical requirements for ICT operational resilience management focusing on the changes that cloud environments introduce. It is expected that this model can be used by organisations as a method for planning and decision making to anticipate, prevent, prepare for, and respond to an ICT disruptive incident when working in this type of environment. A double method approach will collect information from companies working in CCE: consumers, providers and brokers; in order to gain a better understanding of the changes and challenges that these environments have introduced in their operational resilience activities. Particularly, we will be analysing how the incident management process has changed by the adoption of CCE. Practical applicability of the results is a major aim of this study and will be demonstrated through a conceptual model including potential mechanisms to coordinate joint resilience-efforts among CCE actors. You have been identified as a key informant and my supervisors and I are very interested in the information that you can provide us with.

Project procedures

Semi-structured interviews involve the use of some pre-formulated questions but some new questions might emerge during the conversation. Each interview should not require more than 1 hour and we will discuss about incident-handling related activities. As a participant of this study on OR, you should be aware of resilience / business continuity activities regardless your background. This study will be conducted face-to-face either at the University's facilities or the Company's facilities depending on the preference of the participant.

Participation and withdrawal

Your participation in this project is entirely voluntary. You may choose not to take part without giving a reason. I would like to audio-record the interview, however, you can ask me to stop recording at any point during the interview. Also, you may choose to stop participating at any time during the interview and you may choose to withdraw your data any time up to two weeks after the interview.

Confidentiality and use of data

All information you provide during the interview will be kept confidential by the researchers. The data you provide will be used in my doctoral thesis and in academic publications. Your data will be made de-identified to ensure that you and your organisation cannot be identified as the source of information. You can request a copy of any publications resulting from this research.

Storage and disposal of data

All consent forms and data gathered will be stored securely at the University of Auckland for a period of 6 years, and will be securely destroyed at the end of this period. All electronic data will be password-protected and will be securely erased at the end of this period. If you agree to participate in this research, please read and sign the attached consent form.

Thank you very much for your time and help in making this study possible. Should you require any further information please do not hesitate to contact us.

Researcher

Andrea Herrera
a.herrera@auckland.ac.nz
ISOM Department
The University Of Auckland, Private Bag 92019
Auckland 1142, New Zealand

Supervisor

Dr L Janczweski
lech@auckland.ac.nz
Telephone 64 9 373 7599 x 87538
ISOM Department
The University Of Auckland, Private Bag 92019,
Auckland 1142, New Zealand

Co-supervisor

Dr F Beltrán
f.beltran@auckland.ac.nz
Telephone 64 9 373 7599 x 87850
ISOM Department
The University Of Auckland, Private Bag 92019,
Auckland 1142, New Zealand

Head of Department

Professor Michael Myers
m.myers@auckland.ac.nz
Telephone 64 9 373 7599 x 87468
ISOM Department
The University Of Auckland, Private Bag 92019,
Auckland 1142, New Zealand

For ethical concerns, contact The Chair of the Ethics Committee

The University of Auckland Human Participants Ethics Committee,
Office of the Vice-Chancellor,
The University Of Auckland, Private Bag 92019,
Auckland 1142, New Zealand
Telephone: 64 9 373 37599 x83711

APPROVED BY THE UNIVERSITY OF AUCKLAND HUMAN PARTICIPANTS ETHICS COMMITTEE ON 09th April 2014 for (3) years. Reference Number 011218

INTERVIEW PROTOCOL

Department of ISOM
Level 4, Owen G Glenn Building
12 Grafton Road
Auckland
New Zealand

Telephone: (+64)93737599
The University of Auckland
Private Bag 92019
Auckland
New Zealand

Project Title: Resilient Organisation in the Cloud

Researcher: Andrea Herrera

Supervisors: Dr Lech Janczewski, and Dr Fernando Beltrán

Interviewer: ______________________

Please note that in a semi-structured interview, data gathering tends to be open-ended. Therefore, data gathered from one interview session could suggest directions to pursue in subsequent interview sessions. Therefore, it is not possible to present a complete inventory of all the questions that might be asked in the interviews. The following table shows the structure of the interview:

Opening
- Personal introductions / Overview of the study

Initial prompts
- Background organisation, service and service agreement / Tell me about an incident

Additional questions
- How do you coordinate activities with your customer/provider along the incident life cycle?
- How do you determinate the “success/failure” of these activities with your customer/provider?

Additional unplanned/floating prompts
- How? / Can you tell me more about that? / Can you give me examples? / How does that work?

The following questions give you an idea of the issues that will be explored.

1. What types of cloud computing services does your organisation provide / consume?
2. Have you had any cloud-computing-related incident in your organisation?
3. If so, can you describe one specific incident and its main consequences?
4. What processes and mechanisms are being used as a joint effort between your company and your provider(s) / consumer(s) in order to prevent this kind of incidents?
5. What type of testing program has been implemented to ensure those processes and mechanisms meet their stated objectives?
6. What are the processes and mechanisms being used as a joint effort between your company and your provider(s) / consumer(s) for detecting, reporting and analysing this kind of incident?
7. Once an incident has been declared, what processes and mechanisms are used to communicate and coordinate activities among incident response teams?
8. What are the strengths and limitations of those communication and coordination processes and mechanisms?
9. How ongoing incident communications are made?
10. How are the lessons learned, from identifying, analysing, and responding to incidents, being translated into actions to improve resilience strategies? Particularly, those that require a joint effort between your company and your provider(s) / consumer(s).

12 APPENDIX THREE – INCIDENT SUMMARY SHEETS

Conventions and abbreviations:

CSC = Cloud supply chain
High-value business service = from 1-10, being 10 the most critical
IaaS = Infrastructure as a service
ISACA = International professional association focused on ICT governance
ITIL = Set of practices for ICT service management
OR = Organisational resilience
RPO = Recovery time objective
RTO = Recovery point objective
SaaS = Software as a service
SAN = Storage Area Network
SLA = Service level agreement
SSL Certificate = Standard security technology

SUMMARY INCIDENT 1 - I1

A. Organisation overview

Organisation: Large organisation in the education sector
Role in the CSC: Cloud consumer
Deployed resilience frameworks and models: ISACA Risk ICT methodology + ITIL – ICT Service management processes
Length of time deployed frameworks in place: +5 years

B. Business service info

Type of service: Internal and external users
Seasonal service?: Clear peak seasons, however we have not experienced performance issues over these periods
High-value business service (1-10): 8
RTO/RPO: 4 hours / 4 hours

C. ICT Service info

Service model: SaaS – single tenancy
The population of this service could be around few thousand concurrent users during a peak season otherwise few dozens
Deployment model: outsourced-private – Private cloud where the server side is outsourced to hosting company
CSC structure: Mainly a dyadic relationship (SaaS Provider - Consumer). Even though there are multiple entities directly involved in the upstream of the service

D. Event info

Summary: This particular service has a customised module as an interface that connects to an internal ICT service (business process requirement), an scheduled change affected this interaction

Duration: A week Source of the event: Scheduled change that was not notified at all to the consumer Consequences: manual operation contingency was activated by the business area (increasing workload). Some users' data were lost, the organisation had to formally apologise and asked users to enter their information again (negative impact in the image of the organisation)
E. Lessons learnt Avoid customisation, it increases risks and complexity of new releases management We have a customer relationship manager, however, communication through this channel is not ideal and both parties … specially from our side, we are aware that something has to be done however we have not made any decision yet

I1: INCIDENT RECONSTRUCTION - Coordination Mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Service delivery architecture baseline RTO/RPO	*Flexibility mechanisms* Incident detection and reporting procedures	*Learning mechanisms* Root-cause analysis report
Collaboration	*Situational awareness mechanisms* Communication tools and techniques Communication guidelines and standards	*Synchronisation mechanisms* Incident status report Incident closure criteria	*Alignment mechanisms* None
Risk Management Culture	*Vulnerability assessment mechanisms* Frameworks/certification/codes of conduct	*Control mechanisms* Incident documentation	*Embedment mechanisms* None
Agility	*Visibility mechanisms* Vital records, contracts and SLA repository	*Velocity mechanisms* Incident analysis report	*Innovation mechanisms* None

I1: TABLETOP EXERCISE – Coordination mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Change schedule Change control procedures Resilient services design guidelines Replication, backups and retention procedures	*Flexibility mechanisms*	*Learning mechanisms*
Collaboration	*Situational awareness mechanisms*	*Synchronisation mechanisms*	*Alignment mechanisms* Post-incident analysis report Dispute resolution procedures
Risk Management Culture	*Vulnerability assessment mechanisms* Resilience policy	*Control mechanisms* Requirements tracking	*Embedment mechanisms* Remediation plans definition Corrective actions tracking to closure
Agility	*Visibility mechanisms* Monitoring scope definition Collection, organisation and distribution of data Governance scorecard repository	*Velocity mechanisms*	*Innovation mechanisms*

SUMMARY INCIDENT 2 - I2

A. Organisation overview Organisation: Large organisation in the education sector Role in the CSC: Cloud consumer Deployed resilience frameworks and models: ISACA Risk IT methodology + ITIL – IT Service management processes Length of time deployed frameworks in place: +5 years
B. Business service info Type of service: Internal users Seasonal service?: Not so clear, maybe some seasonal peaks High-value business service (1-10): 9 RTO/RPO: 4 hours / 4 hours
C. ICT Service info Service model: SaaS Deployment model: public The population of this service is around 50 thousand users, however, in terms of concurrent user we are talking about few hundreds CSC structure: Mainly a triad relationship (IaaS provider – SaaS provider - Consumer) with few other entities directly involved in the upstream of the service
D. Event info Summary: The business area was notified of a scheduled change. They ran a set of tests however an important set of functionalities wasn’t included causing non-availability of the service after the new release was deployed in production Duration: A week Source of the event: Scheduled change that was not properly test Consequences: Manual operation contingency was activated by the business area (increasing workload, very painful)
E. Lessons learnt Increase the involvement of the IT internal organisation in defining and approving “release and deployment procedures” Formalise procedures

I2: INCIDENT RECONSTRUCTION - Coordination Mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Service delivery architecture baseline Change schedule Change control procedures RTO/RPO	*Flexibility mechanisms* Incident detection and reporting procedures	*Learning mechanisms* Root-cause analysis report
Collaboration	*Situational awareness mechanisms* Communication tools and techniques Communication guidelines and standards	*Synchronisation mechanisms* Incident status reports Incident closure criteria	*Alignment mechanisms* None
Risk Management Culture	*Vulnerability assessment mechanisms* Resilience policy Frameworks/certification/codes of conduct	*Control mechanisms* Incident documentation	*Embedment mechanisms* None
Agility	*Visibility mechanisms* Vital records, contracts and SLA repository Monitoring scope definition	*Velocity mechanisms* Incident analysis report	*Innovation mechanisms* None

I2: TABLETOP EXERCISE – Coordination mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Resilient services design guidelines Replication, backups and retention procedures	*Flexibility mechanisms*	*Learning mechanisms* Change procedures assessment Updating plans
Collaboration	*Situational awareness mechanisms*	*Synchronisation mechanisms*	*Alignment mechanisms* Post-incident analysis report Disputes resolution procedures
Risk Management Culture	*Vulnerability assessment mechanisms*	*Control mechanisms* Requirements tracking	*Embedment mechanisms* Remediation plans definition Corrective actions tracking to closure
Agility	*Visibility mechanisms* Resilience awareness and training needs definition OR awareness / training material repository Collection, organisation and distribution of data Governance scorecard repository	*Velocity mechanisms*	*Innovation mechanisms*

SUMMARY INCIDENT 3 - I3

A. Organisation overview

Organisation: Large organisation

Type of Industry: Government

Role in the CSC: Consumer

Deployed resilience frameworks and models: yes, customised organisational resilience frameworks! Resilience is an ongoing priority for us.

Length of time deployed frameworks in place: +20 years

B. Business service info

Type of service: External users mainly

Seasonal service? Well, perhaps but it is not a clear characteristic of this particular service

High-value business service (1-10): 8

RTO/RPO: 2 hours / 0.25hours (well no data should be lost, actually)

C. ICT Service info

Service model: SaaS

Deployment model: public cloud

The population of this service could be around million users

CSC structure: Four main members (IaaS provider – SaaS provider - Cloud Broker - Consumer). We integrate services from the SaaS provider and the Broker, so we have different contracts and do all the coordination/interaction with each of them "separately"

D. Event info

Summary: Denial-of-service attack involving a service outage

Duration: 1.5 hours in total. Less than 30 minutes detecting and diagnosing the incident. We teamed up with our broker during this first stage and an hour or so controlling, recovering, testing, etc. So yeah in about 1.5 hours we were back

Source of the event: Unpatched software vulnerability – SaaS provider did not apply the correspondent patch timely. That vulnerability was known … they did not do it when they were supposed to and well we did not double check … We gave it for granted!

Consequences: No breached SLAs, not in terms of availability …our RTO for this service is 2 hours and we were back in less than that … no data lost so we also met our RPO. However, our SLA covers vulnerability management and the SaaS provider failed to meet this part of it

E. Lessons learnt

We went through the post-incident analysis stage and we had to give our SaaS provider a hard time … not in terms of monetary compensation because actually according to our conditions it doesn't apply but in terms of the process itself … Well, we have to find a way to closely monitor them in these aspects … at the end it is our service!

I3: INCIDENT RECONSTRUCTION - Coordination Mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Service delivery architecture baseline RTO/RPO Resilient services design guidelines Change schedule Change control procedures Replication, backups and retention procedures	*Flexibility mechanisms* Incident detection and reporting procedures Incident escalation procedures Incident knowledgebase	*Learning mechanisms* Root-cause analysis report Change procedures assessment Updating plans Updating incident knowledgebase
Collaboration	*Situational awareness mechanisms* Communication tools and techniques Communication guidelines and standards Base and derived measures Stakeholders list	*Synchronisation mechanisms* Incident status report Incident closure criteria Incident escalation criteria Communication channels deployment	*Alignment mechanisms* Communication channels assessment Post-incident analysis report Updating guidelines Disputes resolution procedures
Risk Management Culture	*Vulnerability assessment mechanisms* Frameworks/certification/codes of conduct Resilience policy Compliance guidelines and standards Operational risk sources (taxonomy) Vulnerabilities identification tools and techniques	*Control mechanisms* Incident documentation Evidence recording Evidence retention Evidence preservation Requirements tracking	*Embedment mechanisms* Policies and guidelines enforcement Remediation plans definition Corrective actions tracking to closure Resilience promotion

	External/internal audits		
Agility	*Visibility mechanisms* Vital records, contracts and SLA repository Monitoring scope definition Monitoring requirements definition Collection, organisation and distribution of data Governance scorecard repository Resilience exercises schedule Resilience awareness and training needs definition OR awareness / training material repository OR plans repository with updates	*Velocity mechanisms* Incident analysis report Real-time monitoring Restoration procedures Exercises documentation Potential non-compliance risk analysis	*Innovation mechanisms* Update awareness/training requirements Exercises assessment Scorecard variance analysis

I3: TABLETOP EXERCISE – Coordination mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Asset profiles definition Assets discovery tools Collaborative capacity forecasting	*Flexibility mechanisms*	*Learning mechanisms* Design guidelines assessment
Collaboration	*Situational awareness mechanisms* Contextual information for interpreting results	*Synchronisation mechanisms*	*Alignment mechanisms*
Risk Management Culture	*Vulnerability assessment mechanisms* Vulnerabilities repository - resolution status Compliance knowledgebase	*Control mechanisms*	*Embedment mechanisms* Compliance report analyses Risk procedures assessment
Agility	*Visibility mechanisms* Awareness / training activities schedule	*Velocity mechanisms*	*Innovation mechanisms* Assessment awareness/training activities Trends analysis

SUMMARY INCIDENT 4 - I4

A. Organisation overview

Organisation: IT Security firm (Medium size – niche player)

Type of Industry: IT serving private and public sectors (highly regulated sectors)

Role in the CSC: Cloud broker

Deployed resilience frameworks and models: Not a particular resilience framework. Best practices in our industry, +25 experience and specific customers' compliance requirements

Length of time deployed frameworks in place: +5 specifically for cloud solutions

B. Business service info

Type of service: External users

Seasonal service?: Not really

High-value business service (1-10): 8

RTO/RPO: It does depend in our customers, actually we manage different SLAs and partner up with different IaaS providers according to their requirements

C. ICT Service info

Service model: SaaS

Deployment model: public cloud, however we have local/overseas IaaS providers according to our customers' data jurisdiction and other legal requirements

Service dimension: some customers are in the few dozens of users while others in the thousands of users. Concurrently, we manage hundred thousand users

CSC structure: Triad relationship mainly, even though there are multiple entities directly involved in the upstream and downstream of the service. Particular our customers using our "local IaaS provider" solution know all the relevant players in the supply chain

D. Event info

Summary: Local IaaS hardware failure

Duration: 24 hours

Source of the event: A series of hardware faults

Consequences: our customers had to activate their last-level contingencies (operational strategies). It's not much what we can do to help them out. This outage breach some of our SLAs however, as it was not our fault, penalties were directly applied to the IaaS provider

E. Lessons learnt

We do not know exactly what happened, we don't know if it was a firewall or the proper server. If we can pinpoint exactly what it was we would know whose fault was ultimately. Ok, maybe it is not essential to know whose fault was but also what the solution was to the issue so if the same issue occurs again knowing how it was resolved it would be beneficial.

Making our evaluation/selection process more specific in order to advise our customers. I say advice because in this particular case as our customers get to choose the provider and they manage directly the relationship with them, our role is more as advisors

The provider needs to have transparency with their partners in indicating what the issue was exactly and we did not know that. So moving forward if another issue would occur again, we want to know exactly what happened and how it was handled and how is going to be prevented otherwise we would evade to continue partnering up with that provider

I4: INCIDENT RECONSTRUCTION - Coordination Mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Service delivery architecture baseline RTO/RPO Resilient services design guidelines Asset profiles definition	*Flexibility mechanisms* Incident detection and reporting procedures Incident escalation procedures	*Learning mechanisms* None
Collaboration	*Situational awareness mechanisms* Communication tools and techniques Communication guidelines and standards	*Synchronisation mechanisms* Incident status report Incident closure criteria Incident escalation criteria Communication channels deployment	*Alignment mechanisms* Post-incident analysis report Disputes resolution procedures
Risk Management Culture	*Vulnerability assessment mechanisms* Frameworks/certification/codes of conduct Resilience policy Compliance guidelines and standards	*Control mechanisms* Incident documentation Requirements tracking	*Embedment mechanisms* None
Agility	*Visibility mechanisms* Vital records, contracts and SLA repository Monitoring scope definition Monitoring requirements definition	*Velocity mechanisms* Incident analysis report Real-time monitoring	*Innovation mechanisms* None

	Collection, organisation and distribution of data Governance scorecard repository		

I4: TABLETOP EXERCISE – Coordination mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Change schedule Change control procedures	*Flexibility mechanisms* Incident knowledgebase	*Learning mechanisms* Root-cause analysis report Updating incident knowledgebase Design guidelines assessment
Collaboration	*Situational awareness mechanisms* Contextual information for interpreting results Stakeholders list Base and derived measures	*Synchronisation mechanisms*	*Alignment mechanisms* Communication channels assessment
Risk Management Culture	*Vulnerability assessment mechanisms* Operational risk sources (taxonomy) Compliance knowledgebase Vulnerabilities identification tools and techniques Vulnerabilities repository - resolution status	*Control mechanisms* Evidence retention Evidence preservation	*Embedment mechanisms* Policies and guidelines enforcement Compliance report analysis Risk procedures assessment Remediation plans definition Corrective actions tracking to closure

	External/internal audits		
Agility	*Visibility mechanisms* Resilience awareness and training needs definition OR awareness / training material repository Resilience exercises schedule	*Velocity mechanisms* Potential non-compliance risk analysis Restoration procedures Exercises documentation	*Innovation mechanisms* Awareness/training activities assessment Update awareness/training requirements Exercises assessment

SUMMARY INCIDENT 5 - I5

A. Organisation overview Organisation: IT Security firm (Medium size – niche player) Type of Industry: IT serving private and public sectors (highly regulated sectors) Role in the CSC: Cloud broker Deployed resilience frameworks and models: Not a particular resilience framework. Best practices in our industry, +25 experience and specific customers regulation requirements Length of time deployed frameworks in place: +5 specifically for cloud solutions
B. Business service info Type of service: External users Seasonal service?: Not really High-value business service (1-10): 6 RTO/RPO: It does depend in our customers, actually we manage different SLAs and partner up with different IaaS providers according to their requirements
C. ICT Service info Service model: SaaS Deployment model: public cloud, however we have local/overseas IaaS providers according to our customers' data jurisdiction and other legislation requirements Service dimension: some customers are in the few dozens of users while other in few thousands. Concurrently, we manage hundred thousand users CSC structure: Triad relationship mainly, even though there are multiple entities directly involved in the upstream and downstream of the service. Particular, our "overseas IaaS provider" solution customers do know who is our IaaS provider but we do all the intermediations and our customers only have an agreement with us so actually it could be seen as a dyadic relationship in practice
D. Event info Summary: A SSL certificate expired - IaaS provider Duration: +24 hours Source of the event: Scheduled maintenance was not done Consequences: Our customers still had access to our service, however, when they were trying to get access to it, they were getting a "this connection is untrusted" type of error … being a security company is an acceptable message (lose confidence)
E. Lessons learnt In term of our relationship with the provider side – Monitoring our agreements, I guess. Well, not directly related with the described incident but in general with this cloud service, latency is a major concern in our organisation and we have not found a practical solution yet

I5: INCIDENT RECONSTRUCTION - Coordination Mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Service delivery architecture baseline RTO/RPO Resilient services design guidelines Asset profiles definition Replication, backups and retention procedures	*Flexibility mechanisms* Incident detection and reporting procedures Incident escalation procedures	*Learning mechanisms* Root-cause analysis report
Collaboration	*Situational awareness mechanisms* Communication tools and techniques Communication guidelines and standards Base and derived measures	*Synchronisation mechanisms* Incident status report Incident closure criteria Incident escalation criteria	*Alignment mechanisms* Post-incident analysis report Disputes resolution procedures
Risk Management Culture	*Vulnerability assessment mechanisms* Frameworks/certification/codes of conduct Resilience policy Compliance guidelines and standards	*Control mechanisms* Incident documentation Requirements tracking Evidence recording	*Embedment mechanisms* None
Agility	*Visibility mechanisms* Vital records, contracts and SLA repository Monitoring scope definition	*Velocity mechanisms* Incident analysis report Real-time monitoring	*Innovation mechanisms* None

	Monitoring requirements definition Collection, organisation and distribution of data Governance scorecard repository		

I5: TABLETOP EXERCISE – Coordination mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	Architectural mechanisms Assets discovery tools	Flexibility mechanisms Incident knowledgebase	Learning mechanisms Design guidelines assessment Change procedures assessment Updating plans Updating incident knowledgebase
Collaboration	Situational awareness mechanisms Contextual information for interpreting results Stakeholders list	Synchronisation mechanisms	Alignment mechanisms
Risk Management Culture	Vulnerability assessment mechanisms Operational risk sources (taxonomy) Compliance knowledgebase Vulnerabilities identification tools and techniques	Control mechanisms Evidence retention Evidence preservation	Embedment mechanisms Policies and guidelines enforcement Compliance report analysis Risk procedures assessment Remediation plans definition

	Vulnerabilities repository - resolution status External/internal audits		Corrective actions tracking to closure
Agility	Visibility mechanisms Resilience awareness and training needs definition OR awareness / training material repository Resilience exercises schedule	Velocity mechanisms Potential non-compliance risk analysis Restoration procedures Exercises documentation	Innovation mechanisms Awareness/training activities assessment Update awareness/training requirements Exercises assessment

SUMMARY INCIDENT 6 – I6

A. Organisation overview

Organisation: Cloud Provider (Medium size local player)

Type of Industry: IT Services

Role in the CSC: Provider (IaaS and SaaS)

Deployed resilience frameworks and models: Best practices developed by ourselves and our experience. (Also vendors recommendations where applicable)

Length of time deployed frameworks in place: Always

B. Business service info

Type of service: External users

Seasonal service? N/A

High-value business service (1-10): 9 (Core to our business)

RTO/RPO: It does really depend in our customers and I don't know on the top of my head the best RTO/RPO we offer to be honest … With our vendor the RTO is 4 hours

C. ICT Service info

Service model: Not a specific service … technical issue affecting maybe both of our service models

Deployment model: public cloud / private cloud

Service dimension: N/A – more than 30% customers were affected

CSC structure: Different structures, mainly dyadic/triad relationships (main actors) + entities involved in the upstream of the service. Usually the customers sign the agreements with us directly (the third entity would play more like a reseller kind of role).

D. Event info

Summary: All the data in a volume in one of ours SANs was lost – That particular SAN was providing a lot of virtual machines (of course they stopped operating affecting many different services depending on what virtual machines were on)

Duration: The whole environment was recovered in about 20hours however some customers were back in about 30mins. The incident started around midday and next morning all our customers were back.

Source of the event: a series of hardware faults that affected one of ours SANs (3 disks failed all at the same time)

Consequences: Basically some of our customers could not access their services until we started restoring our backups in another site (we had enough capacity to recover but of course it took some time). Our last backup was from the night before. Only in one case, this fact was a problem (large SQL server). They had to rebuild some transactions, fortunately, their systems was developed in such way that they were able to do it by themselves (they did not require any input from us). The recovery process was driven by impact priorities

At the same time we opened a case with our hardware provider (they did some investigation and at the end of the day 75% of the original volume was restored … well, anyway we managed to recover from our own backups)

E. Lessons learnt

It does not matter how much redundancy you got, things can anyway go wrong (importance of testing last level contingencies … backups/restoring, things like that)

Make sure we apply our "minimum" backup regime to all our customers even if they are not live with us yet (one migration project was affected and we were not able to restore that from our backups) … one thing that we have changed is that now we start backing up anything that is added to our environment regardless if it has gone to production or not … at the end we managed to recovered that environment too with our vendor's help but you know better like this

We wanted to have something in place that allows us to more regularly know what was running where, I mean we do have that information but it may have taken us 10-15 minutes to sort of get it all lined out … so we wanted to know exactly who was affected straight away (we do quite a bit of monitoring and we can see all our appliances and all the services and whether they are working or not but we did not necessarily immediately know what services where on that particular volume … that is one thing we wanted to be able more efficient … we do know!

I6: INCIDENT RECONSTRUCTION - Coordination Mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Service delivery architecture baseline Resilient services design guidelines Change schedule Change control procedures Replication, backups and retention procedures Asset profiles definition	*Flexibility mechanisms* Incident detection and reporting procedures Incident escalation procedures Incident knowledgebase	*Learning mechanisms* Root-cause analysis report Change procedures assessment Updating plans Updating incident knowledgebase
Collaboration	*Situational awareness mechanisms* Communication tools and techniques Communication guidelines and standards Base and derived measures Stakeholders list	*Synchronisation mechanisms* Incident status report Incident closure criteria Incident escalation criteria Communication channels deployment	*Alignment mechanisms* Communication channels assessment Post-incident analysis report Updating guidelines Disputes resolution procedures
Risk Management Culture	*Vulnerability assessment mechanisms* Frameworks/certification/codes of conduct Resilience policy Compliance guidelines and standards Operational risk sources (taxonomy)	*Control mechanisms* Incident documentation Evidence recording Requirements tracking	*Embedment mechanisms* Policies and guidelines enforcement Remediation plans definition Corrective actions tracking to closure Resilience promotion

	Vulnerabilities identification tools and techniques External/internal audits		
Agility	*Visibility mechanisms* Vital records, contracts and SLA repository Monitoring scope definition Monitoring requirements definition Collection, organisation and distribution of data Governance scorecard repository Resilience awareness and training needs definition OR awareness / training material repository OR plans repository Resilience exercises schedule	*Velocity mechanisms* Incident analysis report Real-time monitoring Restoration procedures Exercises documentation	*Innovation mechanisms* Update awareness/training requirements Exercises assessment

TABLETOP EXERCISE – Coordination mechanisms

	Protection	**Response**	**Adaptation**
(Re)engineering	*Architectural mechanisms* Assets discovery tools Collaborative capacity forecasting	*Flexibility mechanisms*	*Learning mechanisms* Design guidelines assessment

	RTO/RPO		
Collaboration	*Situational awareness mechanisms*	*Synchronisation mechanisms*	*Alignment mechanisms*
Risk Management Culture	*Vulnerability assessment mechanisms* Vulnerabilities repository - resolution status Compliance knowledgebase	*Control mechanisms* Evidence retention Evidence preservation	*Embedment mechanisms* Compliance report analyses Risk procedures assessment
Agility	*Visibility mechanisms* OR plans repository with updates Awareness / training activities schedule	*Velocity mechanisms* Potential non-compliance risk analysis	*Innovation mechanisms* Assessment awareness/training activities

Master Reference List

Adams, L. A., & Courtney, J. F. (2004, 5-8 Jan. 2004). *Achieving relevance in IS research via the DAGS framework.* Paper presented at the System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on System Sciences.

Alberts, C. J., Dorofee, A. J., Creel, R., Ellison, R. J., & Woody, C. (2011). *A systemic approach for assessing software supply-chain risk.* Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference on.

Almorsy, M., Grundy, J., & Ibrahim, A. S. (2011). *Collaboration-based cloud computing security management framework.* Paper presented at the Cloud Computing (CLOUD), 2011 IEEE International Conference on.

American National Standards Institute, I. (2009). Organisational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use – ASIS SPC. 1-2009.

Arean, O. (2013). Disaster recovery in the cloud. *Network Security, 2013*(9), 5-7.

Argote, L. (1982). Input uncertainty and organizational coordination in hospital emergency units. *Administrative science quarterly,* 420-434.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Commununications of the ACM, 53*(4), 50-58. doi: 10.1145/1721654.1721672

Arshinder, K., Kanda, A., & Deshmukh, S. (2011). A review on supply chain coordination: coordination mechanisms, managing uncertainty and research directions *Supply chain coordination under uncertainty* (pp. 39-82): Springer.

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). SP 800-146: Cloud Computing Synopsis and Recommendations: US National Institute of Standards and Technology (NIST).

Bartoletti, D., Nelson, L. E., Cser, A., Rymer, J. R., Kindness, A., Martorelli, W., O'Donnell, G., Koetzle, L., Chhabra, N., Herbert, L., Liu, F., Miller, P., Vargas, S. I., & Caputo, M. (2016). Predictions 2016: The cloud accelerates: Eleven key developments for cloud and what I&O pros should do about them: Forrester.

Baxter, L. F., & Simmons, J. E. (2001). *The software supply chain for manufactured products: reassessing partnership sourcing.* Paper presented at the Management of Engineering and Technology, 2001. PICMET'01. Portland International Conference on.

Behrendt, M., Glasner, B., Kopp, P., Dieckmann, R., Breiter, G., Pappe, S., Kreger, H., & Arsanjani, A. (2011). Cloud Computing Reference Architecture v2.0: IBM.

Bevere, L., Enz, R., Menhlhorn, J., & Tamura, T. (2012). Natural catastrophes and man-made disasters in 2011: historic losses surface from record earthquakes and floods.

Bhatia, G., Lane, C., & Wain, A. (2013). Building Resilience in Supply Chains: World Economic Forum.

Boin, A., & Lagadec, P. (2000). Preparing for the Future: Critical Challenges in Crisis Management. *Journal of Contingencies and Crisis Management, 8*(4), 185-191. doi: 10.1111/1468-5973.00138

British Standards Institute. (2011). BS ISO/IEC 27031:2011 Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity.

British Standards Institute. (2014). BS 65000:2014 Guidance on organizational resilience.

Burstein, F., & Gregor, S. (1999). *The systems development or engineering approach to research in information systems: an action research perspective.*, 10th Australasian Conference on Information Systems.

Bursztein, E., & Goubault-Larrecq, J. (2007). A logical framework for evaluating network resilience against faults and attacks. *Advances in Computer Science–ASIAN 2007. Computer and Network Security*, 212-227.

Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. *MIS Quarterly, 30*(2), 211-224.

Buyya, R., Ranjan, R., & Calheiros, R. (2010). InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services. In C.-H. Hsu, L. Yang, J. Park & S.-S. Yeo (Eds.), *Algorithms and Architectures for Parallel Processing* (Vol. 6081, pp. 13-31): Springer Berlin / Heidelberg.

Cadzow, S., Giannopoulos, G., Merle, A., Storch, T., Vishik, C., Gorniak, S., & Ikonomou, D. (2015). Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward (2015) (Version 1.1 ed.): Enisa.

Campbell, A. J. (1997). What Affects Expectations of Mutuality in Business Relationships? *Journal of Marketing Theory and Practice, 5*(4), 1-11.

Cao, C., & Zhan, Z. (2011). *Incident management process for the cloud computing environments.* Paper presented at the Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010a). CERT® Resilience Management Model v1.0: External Dependencies Management (EXD) (S. E. Institute, Trans.): Carnegie Mellon.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010b). CERT® Resilience Management Model v1.0: Improving Operational Resilience Processes (S. E. Institute, Trans.): Carnegie Mellon.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010c). CERT® Resilience Management Model v1.0: Monitoring (MON) (S. E. Institute, Trans.): Carnegie Mellon.

Carpenter, S., Walker, B., Anderies, J. M., & Abel, N. (2001). From metaphor to measurement: resilience of what to what? *Ecosystems, 4*(8), 765-781.

Carroll, J. M., & Swatman, P. A. (2000). Structured-case: a methodological framework for building theory in information systems research. *European journal of information systems, 9*(4), 235-242.

Catteddu, D., & Hogben, G. (2009). Cloud Computing: Benefits, risks and recommendations for information security: European Network and Information Security Agency.

Centre for Economics and Business Research ltd. (2011). The cloud dividend: Part Two - The economic benefits of cloud computing to business and the wider EMEA economy (Comparative analysis of the impact on aggregated industry sectors). London: Cebr.

Chen, R., Sharman, R., Rao, H. R., & Upadhyaya, S. J. (2008). Coordination in emergency response management. *Communications of the ACM, 51*(5), 66-73.

Chen, Y., Paxson, V., & Katz, R. H. (2010). What’s New About Cloud Computing Security? : University of California at Berkeley - Electrical Engineering and Computer Sciences.

Chou, M., Ye, H.-Q., & Yuan, X.-M. (2005). *Analysis of a software focused products and service supply chain.* Paper presented at the Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on.

Christopher, M. (2004). Creating resilient supply chains. *Logistics Europe, 11*.

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The international journal of logistics management, 15*(2), 1-14.

Cisco Systems. (2011). Cloud: What an Enterprise Must Know.

Clemons, E. K., & Chen, Y. (2011). *Making the decision to contract for cloud services: managing the risk of an extreme form of IT outsourcing.* Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference on.

Cloud Security Alliance. (2010). Top threats to cloud computing, version 1.0.

Cloud Security Alliance. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.

Cloud Security Alliance. (2013). Enterprise Architecture v2.0.

Cockram, D. (2012). Organisational Resilience. In T. B. W. Group (Ed.), *A BCI Working Group White Paper*: Business Continuity Institute.

Comfort, L. K., & Kapucu, N. (2006). Inter-organizational coordination in extreme events: The World Trade Center attacks, September 11, 2001. *Natural Hazards, 39*(2), 309-327.

Coutu, D. L. (2002). How resilience works. *Harvard Business Review, 80*(5), 46-56.

Crowston, K. (1994). *A taxonomy of organizational dependencies and coordination mechanisms*: Center for Coordination Science, Alfred P. Sloan School of Management, Massachusetts Institute of Technology.

Crowston, K., & Osborn, C. S. (2003). A coordination theory approach to process description and redesign. In T. W. Malone, K. Crowston & G. A. Herman (Eds.), *Organizing business knowledge: the MIT process handbook*: MIT press.

Cumbie, B. (2007). *The Essential Components of Disaster Recovery Methods: A Delphi Study Among Small Businesses*. Paper presented at the AMCIS 2007 Proceedings. Paper 115.

Czarniawska, B. (1998). *A narrative approach to organization studies* (Vol. 43): Sage.

Da Rold, C., Heiser, J., & Morency, J. P. (2011). The Realities of Cloud Services Downtime: What You Must Know and Do.

Dalziell, E., & McManus, S. (2004). *Resilience, Vulnerability and Adaptive Capacity: Implications for System Performance*. Paper presented at the International Forum for Engineering Decision Making.

Dekker, M. (2012). Critical Cloud Computing: A CIIP perspective on cloud computing services: European Network and Information Security Agency (ENISA).

Dekker, M., Liveri, D., & Lakka, M. (2013). Cloud Security Incident Reporting: Framework for reporting about major cloud security incidents: European Network and Information Security Agency (ENISA).

Demirkan, H., Cheng, H. K., & Bandyopadhyay, S. (2010). Coordination strategies in an SaaS supply chain. *Journal of Management Information Systems, 26*(4), 119-143.

DMTF - Open Cloud Standards Incubator. (2010). Architecture for Managing Clouds: Distributed Management Task Force.

Du, S., Lu, T., Zhao, L., Xu, B., Guo, X., & Yang, H. (2013). *Towards An Analysis of Software Supply Chain Risk Management.* Paper presented at the Proceedings of the World Congress on Engineering and Computer Science.

Dutta, A., Peng, G. c. a., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of its experts *Journal of Computer Information Systems, 53*(4).

European Commision. (2012). *Unleashing the Potential of Cloud Computing in Europe*. Brussels: Retrieved from http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf.

Faraj, S., & Xiao, Y. (2006). Coordination in fast-response organizations. *Management Science, 52*(8), 1155-1169.

Fischer, F., & Turner, F. (2009). Cloud computing as a supply chain. *Walden University*.

Franke, J., Charoy, F., & El Khoury, P. (2013). Framework for coordination of activities in dynamic situations. *Enterprise Information Systems, 7*(1), 33-60.

Fugate, B., Sahin, F., & Mentzer, J. T. (2006). Supply chain management coordination mechanisms. *Journal of Business Logistics, 27*(2), 129-161.

Galbraith, J. R. (1973). *Designing complex organizations*: Addison-Wesley Pub. Co.

Gartner. (2012). Gartner Says Worldwide Cloud Services Market to Surpass $109 Billion in 2012 [Press release]. Retrieved from http://www.gartner.com/newsroom/id/2163616

Gartner. (2013). Forecast: IT Services, 2011-2017, 4Q13 Update: Gartner.

Gens, F. (2010). IDC IT Cloud Services Survey, 2Q10.

Gibson, C. A., & Tarrant, M. (2010). A 'conceptual models' approach to organisational resilience. *The Australian Journal of Emergency Management, 25*(02), 6-12.

Gilson, R. J., Sabel, C. F., & Scott, R. E. (2009). Contracting for Innovation: Vertical Disintegration and Interfirm Collaboration. *Columbia Law Review, 109*(3), 431-502. doi: 10.2307/40380356

Gittell, J. H., & Weiss, L. (2004). Coordination Networks Within and Across Organizations: A Multi‐level Framework*. *Journal of Management Studies, 41*(1), 127-153.

Gosain, S., Malhotra, A., & El Sawy, O. A. (2004). Coordinating for flexibility in e-business supply chains. *Journal of Management Information Systems, 21*(3), 7-45.

Grivas, S. G., Kumar, T. U., & Wache, H. (2010). *Cloud broker: Bringing intelligence into the cloud.* Paper presented at the Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on.

Grobauer, B., & Schreck, T. (2010). *Towards incident handling in the cloud: challenges and approaches*. Paper presented at the Proceedings of the 2010 ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA.

Hancock, I., & Hutley, N. (2012). Modelling the Economic Impact of Cloud Computing: KPMG and Australian Information Industry Association (AIIA).

Hawes, C., & Reed, C. (2006). Theoretical steps towards modelling resilience in complex systems. *Computational Science and Its Applications-ICCSA 2006*, 644-653.

Herrera, A., Beltran, F., & Janczewski, L. (2014). *Resilient Organisations in the Cloud.* Paper presented at the The 25th Australasian Conference on Information Systems, Auckland, New Zealand.

Herrera, A., & Janczewski, L. (2013). *Modelling Organisational Resilience in the Cloud.* Paper presented at the PACIS 2013 Proceedings. Paper 275.

Herrera, A., & Janczewski, L. (2014). Issues in the Study of Organisational Resilience in Cloud Computing Environments. *Procedia Technology, 16*(0), 32-41. doi: http://dx.doi.org/10.1016/j.protcy.2014.10.065

Herrera, A., & Janczewski, L. (2015). *Cloud Supply Chain Resilience: A Coordination Approach.* Paper presented at the 14th International Information Security South Africa Conference (ISSA), Johannesburg.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105.

Hoberg, P., Wollersheim, J., & Krcmar, H. (2012). *The Business Perspective on Cloud Computing - A Literature Review of Research on Cloud Computing*. Paper presented at the AMCIS 2012 Proceedings. Paper 5.

Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics, 4*(ArticleType: research-article / Full publication date: 1973 / Copyright © 1973 Annual Reviews), 1-23. doi: 10.2307/2096802

Holling, C. S. (2010). Engineering resilience versus ecological resilience. In L. H. Gunderson, C. R. Allen & C. S. Holling (Eds.), *Foundations of ecological resilience* Washington : Island Press, c2010.

Hon, W. K., Millard, C., & Walden, I. (2012). Negotiating Cloud Contracts-Looking at Clouds from Both Sides Now. *Stanford Technology Law Review, 16*(1), 79-128.

Hossain, L., & Kuti, M. (2010). Disaster response preparedness coordination through social networks. *Disasters, 34*(3), 755-786.

Houtman, L., Kotlarsky, J., & Van den Hooff, B. (2014). *Understanding Knowledge Coordination Dynamics in Traditional and Fast-Response IT Organizations.* Paper presented at the International Conference on Infomration Systems.

Iansiti, M., & Richards, G. L. (2011). *Economic Impact of Cloud Computing White Paper*. Working papers series. Retrieved from http://ssrn.com.ezproxy.auckland.ac.nz/abstract=1875893

IBM Global Technology Services. (2014). Resilience in the era of enterprise cloud computing *Thought leadership white paper*.

Intelligence and National Security Alliance. (2012). Cloud Computing: Risk, Benefits, and Mission Enhancement for the Intelligence Community: Intelligence and National Security Alliance - INSA, Cloud Computing task force.

International Data Corporation. (2013). Worldwide and Regional Public IT Cloud Services 2013–2017 Forecast [Press release]. Retrieved from http://www.idc.com/getdoc.jsp?containerId=242464

International Data Corporation. (2014). IDC FutureScape: Worldwide Cloud 2015 Predictions [Press release]. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS25350114

International Organization for Standardization. (2012). 22301: Societal security - Business continuity management systems - Requirements *Terms and Definitions*. Switzerland.

ISACA. (2012). Guiding Principles for Cloud Computing Adoption and Use *Cloud Computing Vision Series*.

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security, 20*(5), 332-349.

Jarzabkowski, P. A., Lê, J. K., & Feldman, M. S. (2012). Toward a theory of coordinating: Creating coordinating mechanisms in practice. *Organization science, 23*(4), 907-927.

Julisch, K., & Hall, M. (2010). Security and control in the cloud. *Information Security Journal: A Global Perspective, 19*(6), 299-309.

Kaliski Jr, B. S., & Pauley, W. (2010). *Toward risk assessment as a service in cloud environments.* Paper presented at the Proceedings of the 2nd USENIX Workshop on Hot Topics in Cloud Computing.

Kellogg, K. C., Orlikowski, W. J., & Yates, J. (2006). Life in the trading zone: Structuring coordination across boundaries in postbureaucratic organizations. *Organization science, 17*(1), 22-44.

Kendra, J. M., & Wachtendorf, T. (2003). Elements of resilience after the world trade center disaster: reconstituting New York City's Emergency Operations Centre. *Disasters, 27*(1), 37-53.

Kern, T., Lacity, M. C., & Willcocks, L. P. (2002). *Netsourcing: Renting Business Applications and Services Over a Network*: Financial Times Prentice Hall.

Kern, T., Willcocks, L. P., & Lacity, M. C. (2002). Application service provision: Risk assessment and mitigation. *MIS Quarterly Executive, 1*(2), 113-126.

Khasnabish, B., Chu, J., Ma, S., So, N., Unbehagen, P., Morrow, M., Hasan, M., Demchenko, Y., & Meng, Y. (2013). Cloud Reference Framework: Internet Engineering Task Force.

Klein, H., & Myers, M. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, 67-93.

Klein, R. J. T., Nicholls, R. J., & Thomalla, F. (2003). Resilience to natural hazards: How useful is this concept? *Global Environmental Change Part B: Environmental Hazards, 5*(1–2), 35-45. doi: 10.1016/j.hazards.2004.02.001

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and operations management*, *14*(1), 53-68.

Kobialka, D. (2014). 10 Worst Cloud Outages of 2014 (So Far). Retrieved October 10, 2015, from http://mspmentor.net/cloud-computing/112114/lights-out-10-cloud-outages-you-need-know-about#slide-0-field_images-45571

Kounev, S., Reinecke, P., Brosig, F., Bradley, J., Joshi, K., Babka, V., Stefanek, A., & Gilmore, S. (2012). Providing Dependability and Resilience in the Cloud: Challenges and Opportunities. In K. Wolter (Ed.), *Resilience assessment and evaluation of computing systems*: Berlin ; London : Springer, 2012.

Labaka, L., Hernantes, J., Rich, E., & Sarriegi, J. M. (2013). Resilience Building Policies and their Influence in Crisis Prevention, Absorption and Recovery. *Journal of Homeland Security and Emergency Management, 10*(1), 289-317.

Legner, C., & Schemm, J. (2008). Toward the Inter-organizational Product Information Supply Chain-Evidence from the Retail and Consumer Goods Industries*. *Journal of the Association for Information Systems*, *9*(3/4), 119.

Lindner, M., Galán, F., Chapman, C., Clayman, S., Henriksson, D., & Elmroth, E. (2010). *The cloud supply chain: A framework for information, monitoring, accounting and billing.* Paper presented at the 2nd International ICST Conference on Cloud Computing (CloudComp 2010).

Lindner, M., McDonald, F., Conway, G., & Curry, E. (2011). *Understanding Cloud Requirements-A Supply Chain Lifecycle Approach.* Paper presented at the Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization CLOUD COMPUTING 2011.

Lindner, M., McDonald, F., McLarnon, B., & Robinson, P. (2011). *Towards automated business-driven indication and mitigation of VM sprawl in Cloud supply chains.* Paper presented at the Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on.

Lindner, M., Robinson, P., McLarnon, B., & McDonald, F. (2011). *The bullwhip effect and VM sprawl in the cloud supply chain.* Paper presented at the Towards a Service-Based Internet. ServiceWave 2010 Workshops.

Linstone, H. A., & Turoff, M. (2002). *The Delphi Method: Techniques and applications* (Vol. 53): Addison-Wesley.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). SP 500-292: NIST Cloud Computing Reference Architecture. Gaithersburg, MD: US National Institute of Standards and Technology (NIST) - Information Technology Laboratory.

Liu, J., Zhang, L.-J., Hu, B., & He, K. (2012). *CCRA: Cloud Computing Reference Architecture.* Paper presented at the Services Computing (SCC), 2012 IEEE Ninth International Conference.

Mahowald, R. P., & Sullivan, C. G. (2012). Worldwide SaaS and Cloud Software 2012–2016 Forecast and 2011 Vendor Shares: International Data Corporation.

Malone, T., & Crowston, K. (1990). *What is coordination theory and how can it help design cooperative work systems?* Paper presented at the Proceedings of the 1990 ACM conference on Computer-supported cooperative work.

Malone, T., & Crowston, K. (1994). The interdisciplinary study of coordination. *ACM Computing Surveys*, *26*(1), 87-119. doi: 10.1145/174666.174668

Malone, T., Crowston, K., Lee, J., Pentland, B., Dellarocas, C., Wyner, G., Quimby, J., Osborn, C. S., Bernstein, A., & Herman, G. (1999). Tools for inventing organizations: Toward a handbook of organizational processes. *Management Science*, *45*(3), 425-443.

March, J. G., & Simon, H. A. (1958). *Organizations*. Oxford, England: Wiley Organizations.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. *Decision Support Systems, 51*(1), 176-189. doi: http://dx.doi.org/10.1016/j.dss.2010.12.006

Martens, B., & Teuteberg, F. (2011). *Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model*. Paper presented at the AMCIS.

Maurer, F., & Lechner, U. (2014). *From Disaster Response Planning to e-Resilience: A Literature Review*. Paper presented at the BLED 2014 Proceedings. Paper 32.

McCracken, G. (1988). *The long interview* (Vol. 13): Sage.

McManus, S., Seville, E., Brunsdon, D., & Vargo, J. (2007). Resilience Management: A Framework for Assessing and Improving the Resilience of Organisations.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing *Special Publication (SP) 800-145*. Gaithersburg, MD: US National Institute of Standards and Technology (NIST).

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*: Sage.

Mingers, J. (2001). Combining IS research methods: towards a pluralist methodology. *Information systems research, 12*(3), 240-259.

Mintzberg, H. (1980). Structure in 5's: A Synthesis of the Research on Organization Design. *Management Science, 26*(3), 322-341.

Morisse, M., & Prigge, C. (2014). *Business Continuity in Network Organizations–A Literature Review*. Paper presented at the Twentieth Americas Conference on Information Systems, Savannah.

Mousavi, P., Marjanovic, O., & Hallikainen, P. (2012). *Disaster Recovery – The Process Management Perspective*. Paper presented at the PACIS 2012 Proceedings. Paper 67.

Myers, M. D. (2009). *Qualitative Research in Business and Management*. London, UK: SAGE Publications.

Najjar, W., & Gaudiot, J. L. (1990). Network resilience: A measure of network fault tolerance. *Computers, IEEE Transactions on, 39*(2), 174-181.

National Fire Protection Association. (2004). NFPA 1600 standard on disaster/emergency management and business continuity programs (2013 ed.): NFPA - Technical Committee on Disaster Management.

Nunamaker, J., Chen, M., & Purdin, T. D. M. (1991). Systems Development in Information Systems Research. *Journal of Management Information Systems, 7*(3), 89-106.

Nurmi, A. (2009). Coordination of Multi-Organizational Information Systems Development Projects-Evidence from Two Cases. *JITTA: Journal of Information Technology Theory and Application, 10*(3), 4.

Oberhauser, R., & Schmidt, R. (2007). *Improving the integration of the software supply chain via the semantic web*. Paper presented at the Software Engineering Advances, 2007. ICSEA 2007. International Conference on.

Oh, L. B., & Teo, H. H. (2006). The Impacts of Information Technology and Managerial Proactiveness in Building Net-Enabled Organizational Resilience. *The Transfer and Diffusion of Information Technology for Organizational Resilience*, 33-50.

Okhuysen, G. A., & Bechky, B. A. (2009). 10 Coordination in Organizations: An Integrative Perspective. *The Academy of Management Annals, 3*(1), 463-502.

Oppenheimer, D., Ganapathi, A., & Patterson, D. A. (2003). *Why do Internet services fail, and what can be done about it?* Paper presented at the USENIX Symposium on Internet Technologies and Systems.

Oracle Corporation. (2012). Cloud Reference Architecture.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research, 2*(1), 1-28.

Paton, D., & Johnston, D. (2001). Disasters and communities: vulnerability, resilience and preparedness. *Disaster Prevention and Management*, *10*(4), 270-277.

Peiris, C., Sharma, D., & Balachandran, B. (2011). C2TP: a service model for cloud. *International Journal of Cloud Computing, 1*(1), 3-22.

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: development of a conceptual framework. *Journal of Business Logistics*, *31*(1), 1-21.

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The international journal of logistics management, 20*(1), 124-143.

Post, G. V., & Diltz, J. D. (1986). A Stochastic Dominance Approach to Risk Analysis of Computer Systems. *MIS Quarterly, 10*(4), 363-375.

Ried, S., & Kisker, H. (2011). Sizing The Cloud: Understanding And Quantifying The Future Of Cloud Computing: Forrester.

Riessman, C. K. (2008). *Narrative methods for the human sciences*: Sage.

Rimal, B. P., Jukan, A., Katsaros, D., & Goeleven, Y. (2011). Architectural requirements for cloud computing systems: an enterprise cloud approach. *Journal of Grid Computing, 9*(1), 3-26.

Riolli, L., & Savicki, V. (2003). Information system organizational resilience. *Omega, 31*(3), 227-233.

Sabherwal, R. (2003). The evolution of coordination in outsourced software development projects: a comparison of client and vendor perspectives. *Information and organization, 13*(3), 153-202.

Saripalli, P., & Walters, B. (2010). *QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security.* Paper presented at the Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on.

Saya, S., Pee, L. G., & Kankanhalli, A. (2010). *The impact of institutional influences on perceived technological characteristics and real options in cloud computing adoption.* Paper presented at the International Conference On Information Systems (ICIS).

Schrödl, H., & Bensch, S. (2013). *E-Procurement of Cloud-based Information Systems–a Product-Service System Approach.* Paper presented at the Thirty Fourth International Conference on Information Systems, Milan.

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

Sheffi, Y. (2001). Supply Chain Management under the Threat of International Terrorism. *The international journal of logistics management, 12*(2), 1-11. doi: doi:10.1108/09574090110806262

Sheffi, Y. (2005). *The resilient enterprise: overcoming vulnerability for competitive advantage* (Vol. 1): MIT Press Books.

Shim, J., & Lim, Y. (2013). Implementation of Real Time Alert System over Cloud Computing. *International Journal of Energy, Information & Communications, 4*(3).

Shropshire, J. (2015). *Strategies for Ensuring High Availability Cloud Services.* Paper presented at the Twenty-first Americas Conference on Information Systems, San Juan.

Simatupang, T. M., & Sridharan, R. (2008). Design for supply chain collaboration. *Business Process Management Journal, 14*(3), 401-418.

Simatupang, T. M., Victoria Sandroto, I., & Hari Lubis, S. (2004). Supply chain coordination in a fashion firm. *Supply Chain Management: An International Journal, 9*(3), 256-268.

Simmonds, D., Collins, R. W., & Berndt, D. (2010). *Coordinating the Relationship between IT Services Providers and Clients: The Case of Cloud Computing.* Paper presented at the Proceedings of SIGSVC Workshop.

Soni, U., Jain, V., & Kumar, S. (2014). Measuring supply chain resilience using a deterministic modeling approach. *Computers & Industrial Engineering, 74*, 11-25.

Spring, J. (2011a). Monitoring cloud computing by layer, part 1. *Security & Privacy, IEEE, 9*(2), 66-68.

Spring, J. (2011b). Monitoring cloud computing by layer, part 2. *Security & Privacy, IEEE, 9*(3), 52-55.

Standards Australia/Standards New Zealand. (2010). Business continuity - Managing disruption-related risk (AS/NZS 5050:2010). Sydney & Wellington.

Staten, J., Nelson, L., Bartoletti, D., Herbert, L., Martorelli, W., Baltazar, H., O'Donnell, G., & Caputo, M. (2014). Predictions 2015: The Days Of Fighting The Cloud Are Over.

Stephenson, A. V. (2010). *Benchmarking the Resilience of Organisations.* (Doctoral thesis), University of Canterbury, Christchurch.

Sutcliffe, K. M., & Vogus, T. (2003). Organizing for resilience. In J. Dutton, R. Quinn & K. Cameron (Eds.), *Positive Organizational Scholarship: Foundations of a New Discipline*: Berrett-Koehler Publishers.

Tan, C., & Sia, S. K. (2006). Managing flexibility in outsourcing. *Journal of the Association for Information Systems, 7*(1), 10.

The Open Group. (2011). TOGAF 9.1 *37. Building Blocks*: Van Haren Pub.

The Resilience Alliance. (2012). Key concepts. Retrieved November 2012, from http://www.resalliance.org/index.php/key_concepts

Thompson, J. D. (1967). *Organizations in action: social science bases of administrative theory*: McGraw-Hill.

Tierney, K. J. (2003). Conceptualizing and measuring organizational and community resilience: lessons from the emergency response following the September 11, 2001 attack on the World Trade Center.

Toomer, L. G. D. (2011). *FISMA compliance and cloud computing*. Paper presented at the Proceedings of the 2011 Information Security Curriculum Development Conference, Kennesaw, Georgia.

Troshani, G. R., & Wickramasinghe, N. (2011). *Cloud Nine? An Integrative Risk Management Framework for Cloud Computing.* Paper presented at the Proceedings of Bled Conference.

Tsidulko, J. (2014). The 10 Biggest Cloud Outages Of 2014. Retrieved October 10, 2015, from http://www.crn.com/slide-shows/cloud/300075204/the-10-biggest-cloud-outages-of-2014.htm

Tsidulko, J. (2015). The 10 Biggest Cloud Outages Of 2015 (So Far). Retrieved October 10, 2015, from http://www.crn.com/slide-shows/cloud/300077635/the-10-biggest-cloud-outages-of-2015-so-far.htm

U.S. Department of Homeland Security. (2011). Communications-Specific Tabletop Exercise Methodology (pp. 110): SAFECOM.

Undheim, A., Chilwan, A., & Heegaard, P. (2011). *Differentiated Availability in Cloud Computing SLAs.* Paper presented at the 2011 12th IEEE/ACM International Conference on Grid Computing (GRID)

United Nations. (2015). The Global Assessment Report on Disaster Risk Reduction (GAR) 2015.

Van de Ven, A. H., Delbecq, A. L., & Koenig Jr, R. (1976). Determinants of coordination modes within organizations. *American sociological review*, 322-338.

Van de Walle, B., & Rutkowski, A.-F. (2006). A fuzzy decision support system for IT Service Continuity threat assessment. *Decision Support Systems, 42*(3), 1931-1943. doi: 10.1016/j.dss.2006.05.002

van der Vegt, G. S., Essens, P., Wahlström, M., & George, G. (2015). Managing Risk and Resilience. *Academy of Management Journal, 58*(4), 971-980. doi: 10.5465/amj.2015.4004

van Fenema, P. C., Pentland, B., & Kumar, K. (2004). *Paradigm shifts in coordination theory.* Paper presented at the Academy of Management Annual Meeting, New Orleans.

Wahlgren, G., & Kowalski, S. (2013). *IT Security Risk Management Model for Cloud Computing: A Need for a New Escalation Approach.* Paper presented at the The International Conference on Digital Information Processing, E-Business and Cloud Computing (DIPECC2013).

Walsham, G. (1993). *Interpreting information systems in organizations*: John Wiley & Sons, Inc.

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *Eur J Inf Syst, 4*(2), 74-81.

Wand, Y., & Weber, R. (2002). Research commentary: information systems and conceptual modeling—a research agenda. *Information systems research, 13*(4), 363-376.

Weick, K., Sutcliffe, K., & Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. *Research in organizational behavior, 21*, 23-81.

Weick, K. E., & Sutcliffe, K. M. (2001). Managing the Unexpected: Assuring high performance in an age of complexity. 2001. *University of Michigan Business School Management Series*.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. *Crisis management, 3*, 81-123.

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stößer, J. (2009). Cloud Computing – A Classification, Business Models, and Research Directions. *Business & Information Systems Engineering, 1*(5), 391-399. doi: 10.1007/s12599-009-0071-2

Willcocks, L. P., Venters, W., & Whitley, E. A. (2013a). Cloud sourcing and innovation: slow train coming? A composite research study. *Strategic Outsourcing: An International Journal, 6*(2), 184-202.

Willcocks, L. P., Venters, W., & Whitley, E. A. (2013b). *Moving to the Cloud Corporation: How to face the challenges and harness the potential of cloud computing*: Palgrave Macmillan.

Wilson, R. L. (2010). *Organizational Resilience Models Applied to Companies in Bankruptcy.* (Doctor of Management), University of Maryland University College, United States -- Maryland.

Winkler, U., & Gilani, W. (2011). Model-Driven Framework for Business Continuity Management *Service Level Agreements for Cloud Computing* (pp. 227-250): Springer.

Witty, R. J., & Morency, J. P. (2014). Hype Cycle for Business Continuity Management and IT Disaster Recovery Management: Gartner.

Woods, D. D., & Wreathall, J. (2008). Stress-strain plots as a basis for assessing system resilience. *Resilience Engineering: Remaining Sensitive to the Possibility of Failure,* 143-158.

World Economic Forum, & INSEAD. (2012). The Global information Technology Report 2012: Living in a Hyperconnected World.

Xiaohui, L., Jingsha, H., & Ting, Z. (2013). A Service-oriented Identity Authentication Privacy Protection Method in Cloud Computing. *International Journal of Grid & Distributed Computing, 6*(1), 77-86.

Xu, L., & Beamon, B. M. (2006). Supply chain coordination and cooperation mechanisms: an attribute‐based approach. *Journal of Supply Chain Management, 42*(1), 4-12.

Yan, J., Guo, Y., & Schatzberg, L. (2012). Coordination mechanism of IT service supply chain: an economic perspective. *Electronic Markets, 22*(2), 95-103.

Yang, H., & Tate, M. (2012). A Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for Information Systems, 31*(1), 2.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), 7-18. doi: 10.1007/s13174-010-0007-6

Zhao, W., Melliar-Smith, P., & Moser, L. E. (2010). *Fault tolerance middleware for cloud computing.* Paper presented at the Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on.

Zobel, C. W. (2011). Representing perceived tradeoffs in defining disaster resilience. *Decision Support Systems, 50*(2), 394-403. doi: 10.1016/j.dss.2010.10.001

Zobel, C. W., & Khansa, L. (2012). Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks. *Decision Sciences, 43*(4), 687-710. doi: 10.1111/j.1540-5915.2012.00364.x