Cloud Supply Chain Resilience

A Coordination Approach

Andrea Herrera
Business School – Information Systems and Operations
Management Department
University of Auckland
Auckland, New Zealand
a.herrera@auckland.ac.nz

Lech Janczewski
Business School – Information Systems and Operations
Management Department
University of Auckland
Auckland, New Zealand
l.janczewski@auckland.ac.nz

***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 (CCE); organisational resilience (OR); ICT operational resilience; cloud supply chain (CSC) resilience; coordination mechanisms

I. 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 [1–3]. 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 [4]. 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 [5, 6]. 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 [7]. Such environments represent more risks to consumers [8, 9], 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 [4]. 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 [10, 11].

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" [12]. 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 [13]. 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 [14], 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" [15], 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" [16]. From this perspective, this paper understands coordination as "the essence of supply chain management" [17, 18] and sees coordination mechanisms as tools for effectively managing dependencies among supply chain members [19].

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

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 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.

II. 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.

A. 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 [20] 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 [21–23]. 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 [24].

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 [25, 26]; or operational risks such as equipment malfunctions and discontinuities in supply [27] 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" [28] 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" [28] 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 [29–31]. 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 [30]. 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 [14], the need for novel concepts for ICT and OR planning when using new ICT sourcing models such as cloud computing has been recognized [14, 30, 31]. From the management perspective, some resilience-related issues of CCE have been studied such as incident management [32, 33], risk management [34-38], real-time monitoring [39-40], and the mechanisms that organisations are using to enhance OR among interorganisational ICT relationships [41]. 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.

B. 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 [42] 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 [43]; approaches to improve the coordination of software life cycle processes across the supply chain [44]; and a systemic risk management approach across software supply chains [45, 46]. 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 [47, 48]. 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 [49]. 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 [50] 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 [15] 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 [51].

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 [52, 53] and that Linder et al. [7] first formally defined CSC as "two or more parties linked by the provision of cloud services, related information and funds" (**Error! Reference source not found.**). 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 [54]; discussed well-known concepts in supply chain theory such as the "bullwhip effect" [55, 56] and the procurement process [57]; and identified the major coordination strategies used by both cloud service providers and consumers in ensuring successful design and performance of the supply chain [58]. These studies all use known problems in traditional supply chains to identify problem areas and mitigation techniques in the context of CCE.

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 [27, 59–64] 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.

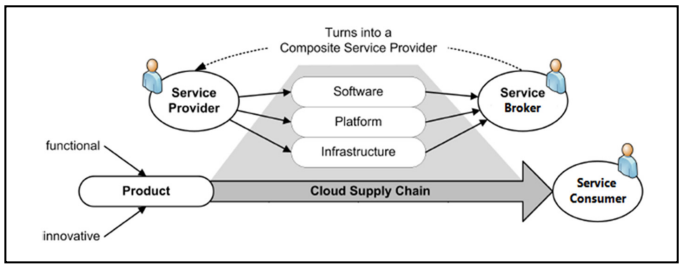

Figure 1. Cloud supply chain definition, from [7]

C. *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. Malone and Crowston [16] define coordination as managing dependencies and introduce coordination theory [65] 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" [66] 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 [67, 68]. 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" [19] 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 [27, 59–62, 64]. 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" [59]. A range of terms have been used to describe the elements that facilitate the attainment of resilience in a supply chain [27, 59–62, 64]. Specifically, Christopher and Peck [60] 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 [64]; allowing for flexible and redundant strategies [62, 64]; and organisational learning [59, 61, 62, 64].

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 [60] 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 [60] 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 [61, 64].
4. Agility: according to Christopher [63], "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 [59].

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.

III. OR 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 (Figure 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 [30], and then 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 [67]. 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 [15]. The conceptual model is focused on coordination mechanisms, which main goal is to manage dependencies among these activities in a CSC [65].

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 [64] collaboration includes an organisation's willingness to share even sensitive information, which is known as event management [60] or situational awareness [62]. 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 [62]. The second element, "synchronisation", enables effective information-sharing channels for CSC members that support decision-making processes particularly, during disruption responses [64, 69]. Finally, [70] 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 [27, 62] and report is added to a new element: "control and measure", capturing

the essential wisdom of "you cannot manage what you do not measure" [27]. 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 [62] 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 [59], 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.

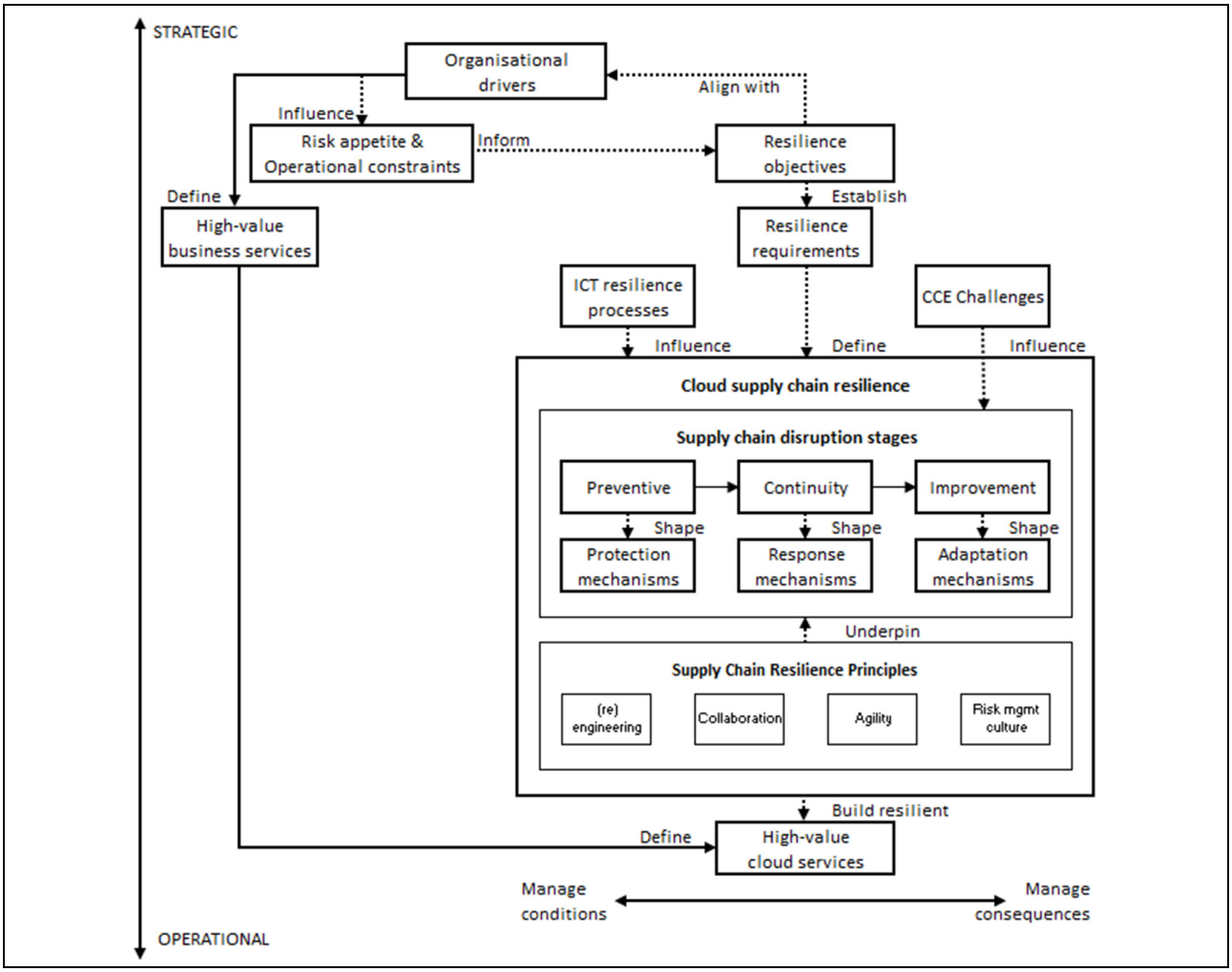

Figure 2. Resilient organisations in the cloud – conceptual model

TABLE I CATEGORIES OF OPERATIONAL RESILIENCE COORDINATION MECHANISMS FOR CSC

	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	Velocity mechanisms	Innovation mechanisms

	- Governance scorecard repository	- Real-time monitoring	- Trends analysis

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 I. This table can be seen as a more detailed description of this part of the model and is discussed next.

A. 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 [15]. 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 [30] and the identified OR challenges [50], 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. [67]. 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.

   a. Dynamically establish the CSC architecture and understand its nature (members, relationships, characteristics, among others) – Architectural mechanisms

   b. Identify information and valuable mechanisms that allow CSC members to know what is going on around them in the supply chain – Situational awareness mechanisms

   c. Identify and analyse vulnerabilities in the CSC according to the level o\f control over the specific cloud service – Vulnerability assessment mechanisms

   d. 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

   a. Provide alternatives to meet the CSC expected level of resilience – Flexibility mechanisms

   b. Provide effective channels to share information, particularly to support decision-making activities – Synchronisation mechanisms

   c. 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

   d. 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.

   a. Assess the CSC resilience ability maturity and implement improvement actions – Learning mechanisms

   b. Build CSC knowledge based on shared-experiences maintaining OR efforts aligned – Alignment mechanism

   c. Ensure that resilience activities and coordination mechanisms are embedded in the CSC daily operations – Embedment mechanisms

   d. 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.

IV. 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 a 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.

REFERENCES

[1] Gartner, "Gartner says worldwide cloud services market to surpass $109 billion in 2012," Gartner 2012.

[2] IDC, "Worldwide and regional public it cloud services 2013–2017 forecast," IDC 2013.

[3] S. Ried and H. Kisker, "Sizing the cloud: understanding and quantifying the future of cloud computing," Forrester 2011.

[4] M. Dekker, "Critical cloud computing: a CIIP perspective on cloud computing services," ENISA 2012.

[5] H. Yang and M. Tate, "A descriptive literature review and classification of cloud computing research," Communications of the Association for Information Systems, vol. 31, pp. 35–60, 2012.

[6] L. P. Willcocks, W. Venters, and E. A. Whitley, Moving to the Cloud Corporation: How to Face the Challenges and Harness the Potential of Cloud Computing. Palgrave Macmillan, 2013.

[7] M. Lindner, F. Galán, C. Chapman, S. Clayman, D. Henriksson, and E. Elmroth, "The cloud supply chain: A framework for information, monitoring, accounting and billing," in 2nd International ICST Conference on Cloud Computing, CloudComp 2010.

[8] M. Dekker, D. Liveri, and M. Lakka, "Cloud security incident reporting: framework for reporting about major cloud security incidents," ENISA 2013.

[9] U. Winkler and W. Gilani, "Model-driven framework for business continuity management," in Service Level Agreements for Cloud Computing, Springer, 2011, pp. 227–250.

[10] IBM Global Technology Services, "Resilience in the era of enterprise cloud computing," IBM 2014.

[11] O. Arean, "Disaster recovery in the cloud," Network Security, vol. 2013, pp. 5–7, 2013.

[12] British Standards Institute, "BS 65000:2014 Guidance on organizational resilience," BSI 2014.

[13] D. Cockram, "Organisational resilience," Business Continuity Institute 2012.

[14] M. Morisse and C. Prigge, "Business continuity in network organizations–a literature review," in Twentieth Americas Conference on Information Systems, 2014.

[15] A. Herrera and L. Janczewski, "Issues in the study of organisational resilience in cloud computing environments," Procedia Technology, vol. 16, pp. 32–41, November, 2014.

[16] T. W. Malone and K. Crowston, "The interdisciplinary study of coordination," ACM Comput. Surv., vol. 26, pp. 87–119, 1994.

[17] B. Fugate, F. Sahin, and J. T. Mentzer, "Supply chain management coordination mechanisms," Journal of Business Logistics, vol. 27, pp. 129–161, 2006.

[18] K. Arshinder, A. Kanda, and S. Deshmukh, "A review on supply chain coordination: coordination mechanisms, managing uncertainty and research directions," in Supply Chain Coordination under Uncertainty, Springer, 2011, pp. 39–82.

[19] L. Xu and B. M. Beamon, "Supply chain coordination and cooperation mechanisms: an attribute-based approach," Journal of Supply Chain Management, vol. 42, pp. 4–12, 2006.

[20] C. S. Holling, "Resilience and stability of ecological systems," Annual Review of Ecology and Systematics, vol. 4, pp. 1–23, 1973.

[21] R. J. T. Klein, R. J. Nicholls, and F. Thomalla, "Resilience to natural hazards: how useful is this concept?", Global Environmental Change Part B: Environmental Hazards, vol. 5, pp. 35–45, 2003.

[22] S. Carpenter, B. Walker, J. M. Anderies, and N. Abel, "From metaphor to measurement: resilience of what to what?", Ecosystems, vol. 4, pp. 765–781, 2001.

[23] The Resilience Alliance. "Key concepts". Available: http://www.resalliance.org/index.php/key_concepts. November 2012.

[24] C. S. Holling, "Engineering resilience versus ecological resilience," in Foundations of Ecological Resilience, L. H. Gunderson, C. R. Allen, and C. S. Holling, Eds. Washington, DC: Island Press, 2010, pp. 51–66.

[25] R. L. Wilson, "Organizational resilience models applied to companies in bankruptcy," unpublished doctoral dissertation, University of Maryland University College, Maryland, 2010.

[26] K. Weick, K. Sutcliffe, and D. Obstfeld, "Organizing for high reliability: processes of collective mindfulness," Research in Organizational Behavior, vol. 21, pp. 23–81, 1999.

[27] P. R. Kleindorfer and G. H. Saad, "Managing disruption risks in supply chains," Production and Operations Management, vol. 14, pp. 53–68, 2005.

[28] E. Dalziell and S. McManus, "Resilience, vulnerability and adaptive capacity: implications for system performance," presented at the International Forum for Engineering Decision Making, 2004.

[29] British Standards Institute, "BS ISO/IEC 27031:2011 Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity,"BSI 2011.

[30] R. A. Caralli, J. H. Allen, P. D. Curtis, D. W. White, and L. R. Young, "CERT® Resilience Management Model v1.0: improving operational resilience processes," Carnegie Mellon CMU/SEI–2010-TR-012 / ESC-TR-2010-012, 2010.

[31] F. Maurer and U. Lechner, "From disaster response planning to e-resilience: a literature review," in BLED 2014 Proceedings. Paper 32, 2014.

[32] C. Cao and Z. Zhan, "Incident Management Process for the Cloud Computing Environments," IEEE International Conference on Cloud Computing and Intelligence Systems, pp. 225-229, 2011.
[33] B. Grobauer and T. Schreck, "Towards Incident Handling in the Cloud: Challenges and Approaches," ACM Workshop on Cloud computing security, 2010.
[34] A. Dutta, G. Peng, and A. Choudhary, "Risks in Enterprise Cloud Computing: The Perspective of its Experts" Journal of Computer Information Systems, vol.53, pp.39-48, 2013.
[35] B. Kaliski Jr and W. Pauley, "Toward Risk Assessment as a Service in Cloud Environments," 2nd Conference on Hot Topics in Cloud Computing, 2010.
[36] B. Martens and F. Teuteberg, "Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model," 17th Americas Conference on Information Systems, 2011.
[37] P. Saripalli and B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security," IEEE 3rd International Conference on Cloud Computing, 2010.
[38] G. Troshani and N. Wickramasinghe, "Cloud Nine? An Integrative Risk Management Framework for Cloud Computing," BLED Conference, 2011.
[39] J. Shim and Y. Lim, "Implementation of Real Time Alert System over Cloud Computing," International Journal of Energy, Information & Communications, vol. 4, 2013.
[40] J. Spring, "Monitoring Cloud Computing by Layer, Part 1," IEEE Security & Privacy, vol. 9, pp. 66-68, 2011.
[41] J. Järveläinen, "Information Security and Business Continuity Management in Interorganizational IT Relationships," *Information Management & Computer Security,* vol. 20, pp. 332-349, 2012.
[42] L. F. Baxter and J. E. Simmons, "The software supply chain for manufactured products: reassessing partnership sourcing," in Management of Engineering and Technology, 2001, p. 468 vol. 1.
[43] M. Chou, H.-Q. Ye, and X.-M. Yuan, "Analysis of a software focused products and service supply chain," in Industrial Informatics, 2005, pp. 198–203.
[44] R. Oberhauser and R. Schmidt, "Improving the integration of the software supply chain via the semantic web," in Software Engineering Advances, ICSEA 2007, pp. 79–86.
[45] S. Du, T. Lu, L. Zhao, B. Xu, X. Guo, and H. Yang, "Towards an analysis of software supply chain risk management," in Proceedings of the World Congress on Engineering and Computer Science, 2013.
[46] C. J. Alberts, A. J. Dorofee, R. Creel, R. J. Ellison, and C. Woody, "A systemic approach for assessing software supply-chain risk," in System Sciences (HICSS) 2011, pp. 1–8.
[47] J. Yan, Y. Guo, and L. Schatzberg, "Coordination mechanism of IT service supply chain: an economic perspective," Electronic Markets, vol. 22, pp. 95–103, 2012.
[48] H. Demirkan, H. K. Cheng, and S. Bandyopadhyay, "Coordination strategies in an SaaS supply chain," Journal of Management Information Systems, vol. 26, pp. 119–143, 2010.
[49] P. Mell and T. Grance, "The NIST definition of cloud computing," US National Institute of Standards and Technology, 2011.
[50] A. Herrera, F. Beltran, and L. Janczewski, "Resilient organisations in the cloud," in The 25th Australasian Conference on Information Systems, 2014.
[51] D. Oppenheimer, A. Ganapathi, and D. A. Patterson, "Why do Internet services fail, and what can be done about it?," in USENIX Symposium on Internet Technologies and Systems, 2003.
[52] F. Fischer and F. Turner, "Cloud computing as a supply chain," Walden University, 2009.
[53] ISACA, "Guiding principles for cloud computing adoption and use," 2012.
[54] M. Lindner, F. McDonald, G. Conway, and E. Curry, "Understanding cloud requirements-a supply chain lifecycle approach," in Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization, 2011.
[55] M. Lindner, P. Robinson, B. McLarnon, and F. McDonald, "The bullwhip effect and VM sprawl in the cloud supply chain," in Towards a Service-Based Internet. ServiceWave 2010 Workshops, pp. 26–37.
[56] M. Lindner, F. McDonald, B. McLarnon, and P. Robinson, "Towards automated business-driven indication and mitigation of VM sprawl in cloud supply chains," in Integrated Network Management, 2011, pp. 1062–1065.
[57] H. Schrödl and S. Bensch, "E-Procurement of cloud-based information systems – a product-service system approach," in Thirty Fourth International Conference on Information Systems, 2013.
[58] D. Simmonds, R. W. Collins, and D. Berndt, "Coordinating the relationship between it services providers and clients: the case of cloud computing," in Proceedings of SIGSVC Workshop, 2010.
[59] S. Y. Ponomarov and M. C. Holcomb, "Understanding the concept of supply chain resilience," International Journal of Logistics Management, vol. 20, pp. 124–143, 2009.
[60] M. Christopher and H. Peck, "Building the resilient supply chain," International Journal Of Logistics Management, vol. 15, pp. 1–14, 2004.
[61] T. J. Pettit, J. Fiksel, and K. L. Croxton, "Ensuring supply chain resilience: development of a conceptual framework," Journal of Business Logistics, vol. 31, pp. 1–21, 2010.
[62] Y. Sheffi, "The resilient enterprise: overcoming vulnerability for competitive advantage," MIT Press, vol. 1, 2005.
[63] M. Christopher, "Creating resilient supply chains," Logistics Europe, vol. 11, 2004.
[64] U. Soni, V. Jain, and S. Kumar, "Measuring supply chain resilience using a deterministic modeling approach," Computers & Industrial Engineering, vol. 74, pp. 11–25, 2014.
[65] K. Crowston and C. S. Osborn, "A coordination theory approach to process description and redesign," in Organizing Business Knowledge: the MIT process handbook, T. W. Malone, K. Crowston, and G. A. Herman, MIT Press, 2003.
[66] T. M. Simatupang, I. Victoria Sandroto, and S. Hari Lubis, "Supply chain coordination in a fashion firm," Supply Chain Management: An International Journal, vol. 9, pp. 256–268, 2004.
[67] R. Chen, R. Sharman, H. R. Rao, and S. J. Upadhyaya, "Coordination in emergency response management," Communications of the ACM, vol. 51, pp. 66–73, 2008.
[68] J. Franke, F. Charoy, and P. El Khoury, "Framework for coordination of activities in dynamic situations," Enterprise Information Systems, vol. 7, pp. 33–60, 2013.
[69] T. M. Simatupang and R. Sridharan, "Design for supply chain collaboration," Business Process Management Journal, vol. 14, pp. 401–418, 2008.
[70] Y. Sheffi, "Supply chain management under the threat of international terrorism," International Journal of Logistics Management, vol. 12, pp. 1–11, 2001.