# Resilient Organisations in the Cloud

*Research in Progress*

Andrea Herrera
Business School
University of Auckland
Auckland, New Zealand
Email: a.herrera@auckland.ac.nz

Fernando Beltrán
Business School
University of Auckland
Auckland, New Zealand
Email: f.beltran@auckland.ac.nz

Lech Janczewski
Business School
University of Auckland
Auckland, New Zealand
Email: l.janczewski@auckland.ac.nz

## 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

## 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; IDC 2013; Ried and 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 et al. 2013; Winkler and 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). 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 and Hogben 2009; Cloud Security Alliance 2011; Hancock and 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 and 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 and Wachtendorf 2003), disasters (Dalziell and McManus 2004; Paton and Johnston 2001; Stephenson 2010; Tierney 2003), high-reliability organisations (Weick and Sutcliffe 2001; Weick et al. 2008; Woods and Wreathall 2008) and ICT (Caralli et al. 2010). In the latter, "mainly to understand how computing systems impact organisational performance, how to assess alternative methods and how to establish essential components"(Herrera and 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. 2010).

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.

## 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 and 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" (Mingers 2001) 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 and Janczewski 2014). The framework adopts the cloud definition by the National Institute for Standards and Technology (NIST) (Mell and Grance 2009) 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. 2010; 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, Mingers' approach (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.

## 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)". 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.

### 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 (Dalziell and McManus 2004): (1) engineering resilience that aims to maximise "the efficiency of systems and processes to return and maintain the system at its desired state" and (2) ecological resilience that aims to design "flexible systems and processes that continue to function in the face of disturbances". From an organisational perspective, "increasing the ecological resilience would increase the magnitude of consequences that an organisation could withstand before suffering irreparable damage" (Dalziell and McManus 2004) 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 1.

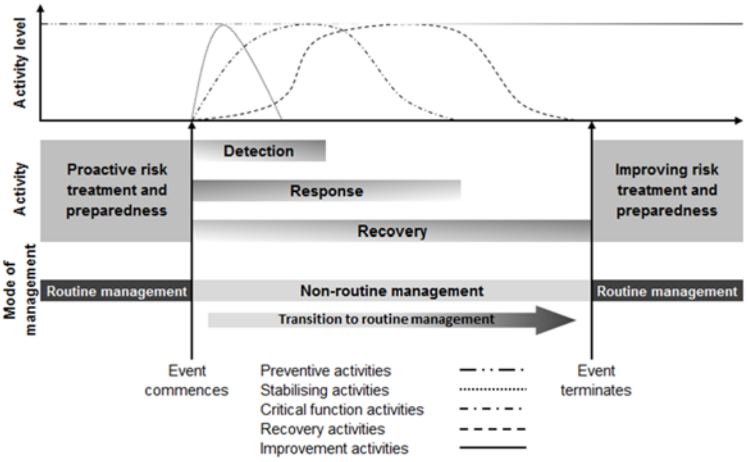

Figure 1: Activities vs. Incident Stages adapted from "Relationship of treatments for disruption-related risk"(Standards Australia/Standards New Zealand 2010)

The first type of activities, preventive activities, deals with strategies designed to minimize an asset's exposure to sources of disruption; 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's (1994) 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 and Crowston 1990). 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 Table 1) (Caralli et al. 2010). It also defines six levels of maturity: incomplete, preferred, managed, defined, quantitatively managed, and optimised.

Based on the research framework (Herrera and 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 & 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 and Zhan 2011). (2) The "operational risk & 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 and 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.

Table 1. RMM processes by high-level categories

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

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. 2010), as shown in Figure 2. Therefore, this last foundation narrow down the scope of this research focusing on core activities and mechanisms 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).

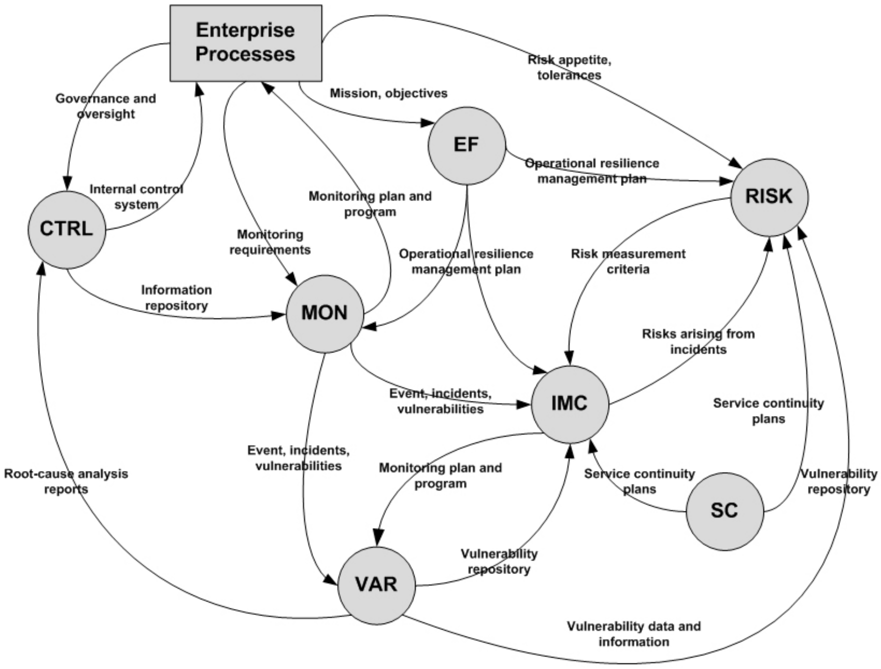
Enterprise Processes
Governance and oversight
Internal control system
Mission, objectives
Risk appetite, tolerances
EF
Operational resilience management plan
RISK
CTRL
Monitoring plan and program
Monitoring requirements
Operational resilience management plan
Risk measurement criteria
Information repository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

Figure 2: Relationship that drive incident management (Caralli et al. 2010)

### 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 et al. 2011; Grobauer and Schreck 2010; Kaliski Jr and Pauley 2010; Wahlgren and 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 2.

Table 2. OR challenges by CC characteristics

| 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 |

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.

### High-level Conceptual Model

The high-level graphical representation of the conceptual model is presented in Figure 3. 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 before starting with the model itself, as briefly discussed in the final section of this paper. This preliminary assessment is considered part of the third stage,

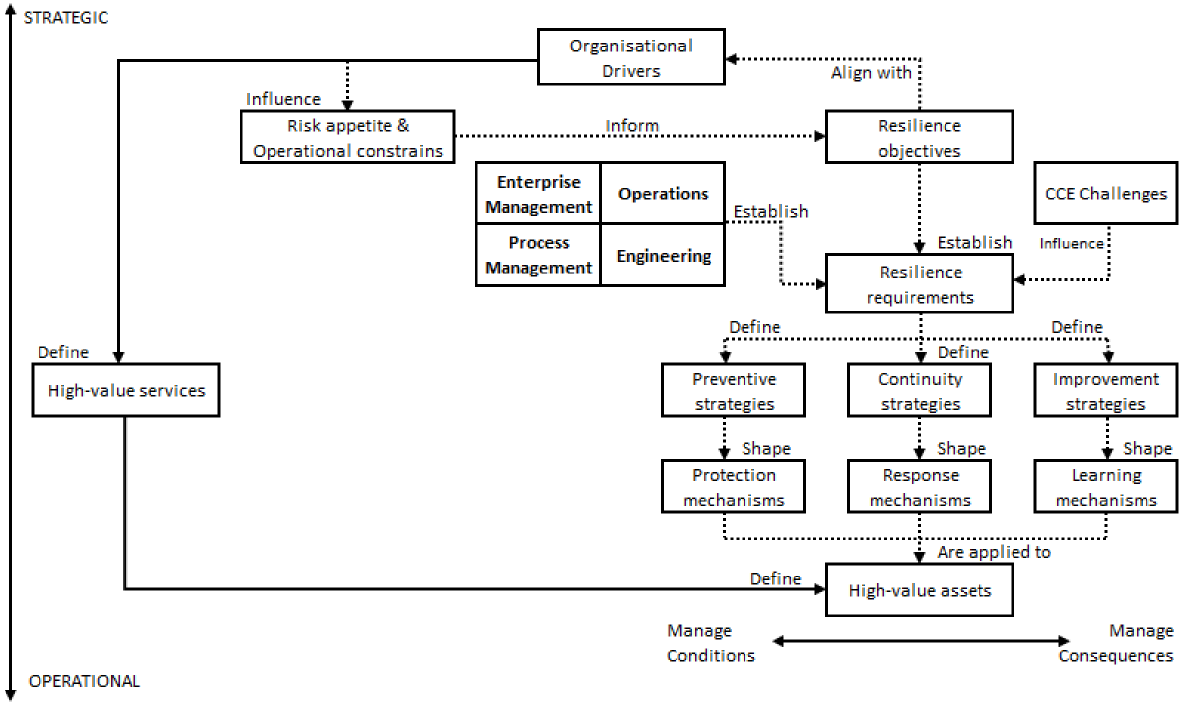

Figure 3: Model's baseline

## 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 foundations and challenges, 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.

## REFERENCES

Adams, L. A., and Courtney, J. F. Year. "Achieving relevance in IS research via the DAGS framework," System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on System Sciences2004, p. 10 pp.

Almorsy, M., Grundy, J., and Ibrahim, A. S. Year. "Collaboration-based cloud computing security management framework," Cloud Computing (CLOUD), 2011 IEEE International Conference on, IEEE2011, pp. 364-371.

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), pp 5-7.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. 2010. "A view of cloud computing," *Commununications of the ACM* (53:4), pp 50-58.

Badger, L., Grance, T., Patt-Corner, R., and 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., and 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., and Calheiros, R. 2010. "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services," in *Algorithms and Architectures for Parallel Processing*, C.-H. Hsu, L. Yang, J. Park and S.-S. Yeo (eds.), Springer Berlin / Heidelberg, pp. 13-31.

Cao, C., and Zhan, Z. Year. "Incident management process for the cloud computing environments," Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on, IEEE2011, pp. 225-229.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., and Young, L. R. 2010. "CERT® Resilience Management Model v1.0: Improving Operational Resilience Processes," CMU/SEI-2010-TR-012 / ESC-TR-2010-012, Carnegie Mellon.

Catteddu, D., and Hogben, G. 2009. "Cloud Computing: Benefits, risks and recommendations for information security," European Network and Information Security Agency.

Chen, Y., Paxson, V., and Katz, R. H. 2010. "What's New About Cloud Computing Security?," UCB/EECS-2010-5, 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., and McManus, S. 2004. "Resilience, Vulnerability and Adaptive Capacity: Implications for System Performance," in *International Forum for Engineering Decision Making*.

Dekker, M. 2012. "Critical Cloud Computing: A CIIP perspective on cloud computing services," ENISA.

Dekker, M., Liveri, D., and Lakka, M. 2013. "Cloud Security Incident Reporting: Framework for reporting about major cloud security incidents," ENISA.

Dutta, A., Peng, G. c. a., and 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."

Grobauer, B., and Schreck, T. 2010. "Towards incident handling in the cloud: challenges and approaches," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, ACM: Chicago, Illinois, USA, pp. 77-86.

Hancock, I., and Hutley, N. 2012. "Modelling the Economic Impact of Cloud Computing," KPMG and Australian Information Industry Association (AIIA).

Herrera, A., and Janczewski, L. Year. "Modelling Organizational Resilience in the Cloud," PACIS 2013 Proceedings. Paper 275.2013.

Herrera, A., and Janczewski, L. Year. "Issues in the study of organisational resilience in cloud computing environments," To be presented at CENTERIS 2014 - Conference on ENTERprise Information Systems, Troia, Portugal, 2014.

IDC 2013. "Worldwide and Regional Public IT Cloud Services 2013–2017 Forecast," IDC.

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

Kaliski Jr, B. S., and Pauley, W. Year. "Toward risk assessment as a service in cloud environments," Proceedings of the 2nd USENIX conference on Hot topics in cloud computing, USENIX Association2010, pp. 13-13.

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

Khasnabish, B., Chu, J., Ma, S., So, N., Unbehagen, P., Morrow, M., Hasan, M., Demchenko, Y., and Meng, Y. 2013. "Cloud Reference Framework," Internet Engineering Task Force.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., and Leaf, D. 2011. "SP 500-292: NIST Cloud Computing Reference Architecture," NIST - Information Technology Laboratory, Gaithersburg, MD.

Malone, T., and Crowston, K. Year. "What is coordination theory and how can it help design cooperative work systems?," Proceedings of the 1990 ACM conference on Computer-supported cooperative work, ACM1990, pp. 357-370.

Malone, T. W., and Crowston, K. 1994. "The interdisciplinary study of coordination," *ACM Comput. Surv.* (26:1), pp 87-119.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. 2011. "Cloud computing — The business perspective," *Decision Support Systems* (51:1), pp 176-189.

Mell, P., and Grance, T. 2009. "SP 800-145: The NIST Definition of Cloud Computing," NIST - Information Technology Laboratory, Gaithersburg, MD.

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

National Fire Protection Association 2004. "NFPA 1600 standard on disaster/emergency management and business continuity programs," NFPA - Technical Committee on Disaster Management.

Nunamaker, J., Chen, M., and Purdin, T. D. M. 1991. "Systems Development in Information Systems Research," *Journal of Management Information Systems* (7:3), pp 89-106.

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

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

Ried, S., and Kisker, H. 2011. "Sizing The Cloud: Understanding And Quantifying The Future Of Cloud Computing," Forrester.

Rimal, B. P., Jukan, A., Katsaros, D., and Goeleven, Y. 2011. "Architectural requirements for cloud computing systems: an enterprise cloud approach," *Journal of Grid Computing* (9:1), pp 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*, 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., and Kowalski, S. Year. "IT Security Risk Management Model for Cloud Computing: A Need for a New Escalation Approach," The International Conference on Digital Information Processing, E-Business and Cloud Computing (DIPECC2013), The Society of Digital Information and Wireless Communication2013, pp. 56-68.

Wand, Y., and Weber, R. 2002. "Research commentary: information systems and conceptual modeling—a research agenda," *Information Systems Research* (13:4), pp 363-376.

Weick, K. E., and 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., and Obstfeld, D. 2008. "Organizing for high reliability: Processes of collective mindfulness," *Crisis management* (3), pp 81-123.

Wilson, R. L. 2010. *Organizational Resilience Models Applied to Companies in Bankruptcy*, University of Maryland University College, United States -- Maryland.

Winkler, U., and Gilani, W. 2011. "Model-Driven Framework for Business Continuity Management," in *Service Level Agreements for Cloud Computing*, Springer, pp. 227-250.

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

## INTELLECTUAL PROPERTY