Towards Modelling a Cloud Application's Life Cycle

Reginald Butterfield[1,2], Silia Maksuti[2,3], Markus Tauber[2,3], Christian Wagner[3] and Ani Bicaku[2,3]
[1]*Management Resource Centre, Vienna, Austria*
[2]*University of Applied Sciences Burgenland, Eisenstadt, Austria*
[3]*Austrian Institute of Technology, Vienna, Austria*

Keywords: Cloud Application Life Cycle, Security Software Development Life Cycle, Security, Business Requirements, Risk, Governance, Decision-making.

Abstract: The success of any cloud-based application depends on appropriate decisions being taken at each phase of the life cycle of that application coupled with the stage of the organisation's business strategy at any given time. Throughout the life cycle of a cloud-based project, various stakeholders are involved. This requires a consistent definition of organizational, legal and governance issues regardless of the role of the stakeholder. We proffer that currently the models and frameworks that offer to support these stakeholders are predominantly IT focused and as such lack a sufficient focus on the business and its operating environment for the decision-makers to make strategic cloud related decisions that benefit their individual business model. We propose an emerging framework that provides a stronger platform on which to base cloud business decisions. We also illustrate the importance of this approach through extrapolating the subject of security from the initial Business Case definition phase, through the Decision Making phase and into the Application Development phase to strengthen the case for a comprehensive Business-based framework for cloud-based application decision-making. We envisage that this emerging framework will then be further developed around all phases of the Application Life Cycle as a means of ensuring consistency.

1 INTRODUCTION

The cloud features (Mell and Grance, 2011) on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service makes cloud computing an attractive infrastructure aid for modern day applications. Whilst a lot of work has been invested in engineering issues the overall processes defining the life cycle of cloud based applications have not been looked at in great detail. Such processes or phases involve Business Case-Definition, Decision Phase, Design Phase, Test-driven Development Phase, Deployment, Operations including monitoring, updates, and resource adaptations until Decommissioning the application. In this position paper we investigate two major parts of the life cycle of cloud based applications, as a starting point: (i) business strategy related phases, and (ii) secure software development.

We explain details to show the need and how a framework for guiding the phases of the life cycle could be supported. This includes, e.g. modelling issues, which should be dealt with in a consistent way throughout the life cycle.

Regarding business strategy related phases we argue that there needs to be a wider business case for discussion and understanding before any decision is made whether to move into the cloud environment. Our argument is based on the notion that the very promises made about the cloud are, in themselves, sufficient to bring about unforeseen change in the whole organisation system. If those changes are not understood or recognised before entering into any contractual cloud arrangement, then business owners and shareholders may rue their decision. Our aim is to provide a high-level framework to assist decision makers in coming to terms with the potential impact of the cloud on their business. The starting point for our framework is that of the TOE (Technological, Organizational, and Environmental) framework researched and developed by Rocco DePietra, et al (DePietro, et al., 1990). Their framework is explained in more detail in Section IV through an overview of the definitions of the TOE framework constructs. The definitions demonstrate the absence of the important general business issues that need to be considered and as such reinforces the need for further development to be of real assistance to management in their adoption decision process. In order to identify and define the additional constructs

Butterfield, R., Maksuti, S., Tauber, M., Wagner, C. and Bicaku, A.
Towards Modelling a Cloud Application's Life Cycle.
In *Proceedings of the 6th International Conference on Cloud Computing and Services Science (CLOSER 2016) - Volume 1*, pages 310-319
ISBN: 978-989-758-182-3

of the business model we discuss some of the key lements of any successful business. This discussion is followed by a revised TOE framework that we believe will add further resilience to organisational decisions about moving to the cloud. Additionally, we investigate how we can model individual issues in the individual phases to support creating, operating and decommission the application.

Regarding secure software development we show the Cloudification Security Development Life Cycle (CloudSDL) (Wagner, et al., Aug 2015) based on common security development life cycles (Howard and Lipner, 2009), (Kissel, et al., 2008), and (Chandra, 2009). The CloudSDL approach is built around the security requirements relevant to the cloudified product. Our approach specifically considers the software development phase and allows an integration with the Production / Maintenance phase.

Our contribution is to show in a discussion of the two novel approaches how they can be interlinked with each other, which issues persist in the individual phases of the life cycle and discuss how they could be modelled in future work.

The reminder of this paper is as follows: in Section II, we present the current state of the art. In Section III, we discuss details about our novel framework supporting the business strategy related phase and in Section IV, we provide details about the CloudSDL. In Section V, we compare both approaches, discuss how a common approach could be modelled and give an outlook to our future work.

2 RELATED WORK

2.1 Development Life Cycles for Cloud-based Applications

Many of the development life cycles only address technical issues and no such early stages like business strategy and development are considered, even though these earlier stages actually define what should be modelled.

As part of the process-oriented security guideline in the SECCRIT project (Wagner, et al., Aug 2015), a Cloudification Security Development Life cycle (CloudSDL) together with a mapping of security relevant issues to current best practice guidelines and standards was developed. At first, to emphasize the differences between industry and critical infrastructure providers concerning information security requirements, two extensive surveys among regular industry and critical infrastructure provider experts have been conducted. Based on the result of the survey analysis a set of 29 relevant security topics, which have been further mapped to current best practice guidelines and standards, including NIST, ENISA, CSA, OPENSAMM, etc. have been selected. To use such a taxonomy in an effective way, it has been incorporated into a process (CloudSDL) that gives attention to the information security aspects of cloudification. The approach for CloudSDL has been built around the security requirements relevant to the cloudified product. The following use cases for CloudSDL have been considered: (i) software development for cloud environment from scratch, (ii) software migration from legacy system to cloud, and (iii) software migration from private to public cloud and vice versa. CloudSDL is composed of five phases: Analysis, Design, Implementation, Verification and Deployment. Business strategy has been considered as a preliminary phase, and so, not detailed in this work.

With the Cloud Controls Matrix (CCM) (Cloud Security Alliance (CSA), 2015), CSA provides a set of fundamental security principles to guide cloud vendors and assist cloud customers in assessing the overall security risk of a cloud provider. The matrix provides a framework in 16 domains that are cross-walked to other industry-accepted security standards, regulations, and control frameworks. In support of this framework, the Consensus Assessments Initiative Questionnaire (CAIQ) (Cloud Security Alliance (CSA), s.d.) provides a series of »yes or no« control assertion questions which can then be tailored to suit each unique cloud customer's requirements. Together, CCM and CAIQ constitute a comprehensive cloud security control framework. The library provided by CSA covers different domains, but does not go into the level of detail we presented. It also does not explicitly consider a critical infrastructure use case. Open Security Architecture (OSA) is a non-profit organization supported by volunteers for the benefit of the security community. The main OSA artefacts are assembled in the OSA Library (Open Security Architecture (OSA), s.d.). The library contains security architecture patterns, security controls (based on NIST SP 800-53) needed to create security solutions, and a catalogue of related security threats. Among others, the OSA Library also contains the Cloud Computing Pattern SP-011, which comprises a list of applicable security controls for cloud computing. A complete catalogue of OSAcontrols is available on-line.

2.2 Cloud and Organisational Forms

The impact of cloud computing technologies on management practices and business strategies is not only an area for investigation, but little research has been conducted into the extent to which it impacts on the organisation's strategy, business model, structure or management processes.

The business case for organisations moving more into the cloud is predominantly based on the financial gains (Armbrust et al., 2009); competitive advantage (Truong, 2010); flexibility through on-demand and self-service (Bias, 2010) and reduced purchasing risks (Leavitt, 2009). At the same time many risks are identified predominantly around security and accountability (Greenwood and Khajeh-Hosseni, 2010), technical business failures (Bisong and Rahman, 2011) and lack of standards (Leavitt, 2009).

Cloud literature and marketing emphasis tends to be geared towards technical and financial factors in the deployment of the technology with limited reference to the organisation's supply chain strategy or the impact on the organisation itself.

In order for a resource to add value to an organisation and develop its competitive advantage it must add value, be rare, inimitable and it cannot be substitutable (Wright and McMahan, 1992). Equally, the resource based view suggests that new technologies are more likely to provide a unique competitive advantage if they are firm specific and cannot easily be copied by competitors. Cloud computing models are in many ways the antithesis of the resource view.

Irrespective of the organizational size, the cloud arguably permits the purchase of relatively high-level ICT services from specialist external providers. Cloud providers will generally supply ICT services to a number of firms as generic ''off the shelf'' products and services, rather than firm-specific ICT services (Ryan and Loeffler, 2010).

The increasing commoditisation of ICT is seen as ''the twenty-first century vision of computing'', as cloud-based ICT providers increasingly mirror utilities with customers buying ICT services as required (Buyya et al., 2009). If this is the case, how does an organisation gain competitive advantage if everybody is buying cloud technology off-the-shelf at relatively cheap prices? It is our view, supported by Ross and Blumenstein that " Cloud computing business models therefore require ICT sections to play a more strategic role within firms, as opposed to the more isolated ''cost centre'' role that many ICT departments have played in the past " (Ross and Blumenstein, 2013, p.42). A high risk for business is that the commoditisation of the cloud will have a similar impact as the quality and efficiency programs that organisations follow; they end up as efficient as one another because they use similar processes and equipment. The only realistic outcome is price as the major differentiator. It has long been understood that the 'DNA' of an organisation is the only real way of having a strategic advantage over competitors; it is the one thing that they cannot copy. Most literature relating to business cases for cloud implementation alludes to the need to consider the organisation itself, albeit most is focused on the IT section of the organisation (Ross and Blumenstein, 2013, p.5). We found none that discussed in detail the impact on organisations overall.

2.3 Business Strategy

2.3.1 Organisational Strategy

Business growth is arguably the main objective of any enterprise and 'resource management' is one parameter of business growth. This is epitomised by the need to focus on containing costs and increasing efficiencies in order to generate profits and maintain competitiveness. Supply chain management (SCM) and its optimisation is a critical aspect of enterprises and the IT department plays a major role in this process of optimisation. The convergence of business units and the IT department using state-of-art cloud technology is seen as a solution to optimise complicated supply chains (Manuel, et al., 2013).

Cloud providers' publications and journal articles push for organisations to use their public cloud facilities as part of their business strategy. They focus on the argument that public cloud is a better choice from the perspective of resource management since it provides the least elasticity.

Whilst resource management is one of the parameters of the growth business objective and even though public cloud is an optimal model from the perspective of resource management, the question remains if the public cloud is the most suitable from a business strategy perspective.

Manuel, et al provide a good argument for adopting the community cloud as the optimal model in the case of supply driven enterprises (Manuel et al., 2013, pp. 209-302). According to their study, and Google and Amazon marketing, it is true that the public cloud is the choice for optimisation of resource management; yet business growth is optimised through community cloud application.

This important study indicates that when organisations decide on the type of cloud services to adopt, it is essential to consider the strategy and objectives of the business before commitment. We have included the strategic parameters in our emerging framework.

2.3.2 Business Model

The deployment of cloud facilities in an organisation is a strategic decision and as such requires a clear understanding of its impact or potential impact on the pertaining or future business model. The cloud can be seen as a "New Market" disruptive innovation that has led to the servitization of the IT industry and most importantly, implementing this innovation is likely to require a fundamental and cultural change in how organisations view their IT resources, conduct their business, and prepare for the future (Sultan, 2014, pp. 375, 385).

The potential opportunities or impact on the business is clearly set out in a white paper "Above the Clouds" (Armbrust et al., 2009, pp. 1, 2, 4) as follows:

- Avoid missed business opportunities from under-provisioning and over-provisioning
- Responsive service to variable demand
- Pursue emergent and explorative new business market opportunities hitherto unforecast or predicted
- Perform cost associative tasks fast and at lower cost
- Decouple utility services and brokering from business front end (the "fab-less" chip foundries example)
- Make more money from amortizing economies of scale
- Leverage existing investments through hybrid means
- "Anywhere" services, "border-less" delivery

The opportunities offered through the developments of the cloud mean that the introduction of the cloud can have a disruptive potential on an organisation's business model. Current discussions around the business cases to introduce the cloud seldom indicate that such a strategic understanding is of importance and benefit to consider before moving to the cloud. Discussions are predominantly around the strategic case for the IT element as opposed to the whole business model. We contend that this is an important omission and our emerging framework includes this critical aspect. The relationship between business model and strategy has been a matter of debate among strategy and organisation scholars (Achtenhagen et al., 2013) and the longitudinal case study of Saeed Khanagha et al., sought to understand why and how strategy and business models are interrelated (Khanagha et al., 2014). Their study indicates that it can be inferred that, irrespective of the degree of uncertainty, the design and implementation of a new business model is a function of an organisation's strategy at a given period in time.

It is our contention that any organisation that is moving to the Cloud needs to be aware of the impact on the strategy, business model and the effect that this will have on the structure of that organisation.

2.3.3 Organisational Structure

When contemplating significant changes to an organisation's strategy and business model it is important to identify the implications of such changes on the structure of the organisation itself.

Tarabanis et al., state that the organisational structure consists of values, visions and power, which influence the development of strategic processes (Tarabanis et al., 2001). According to Iyamu, some factors that influence the institutionalisation of the EA include organisational structure, economic investment, administrative processes and politics evident within the organisation's structure, technical capabilities and business buy-in (Iyamu and Mphahlele, 2014).

Morton and Hu (Morton and Hu, 2008, p. 399) also have identified the importance of considering the organisational structure and have linked their findings to five forces:

- the pull exerted by the strategic apex to centralize and to coordinate by direct supervision in order to retain control over decision making
- the pull exerted by the techno-structure to coordinate by standardization
- the pull exerted by the operators to professionalize
- the pull exerted by middle managers to Balkanize, or to divide the structure into market-based units
- the pull exerted by the support staff (and by the operators as well in the operating adhocracy) for collaboration in decision-making.

In their case study approach to Enterprise Architecture (EA) implementation, Iyamu and Mphahlele identified that "…organisational structure influences and has impact on the deployment of EA in the organisation." (Iyamu and Mphahlele, 2014, p.18).

Cámara et al., "…highlight the importance of

aligning IT-enabled capabilities and supply chain integration to improve the operational performance of supply chain members. The results specifically suggest that technological breakthroughs like cloud computing enable supply chain integration, which in turn yields greater operational performance." (Cámara et al., 2015, p. 443).

It is important to note that cloud computing has a positive and significant effect on the company's operational performance only when it contributes to greater supply chain integration (Cámara et al., 2015, p. 446). This reinforces the need for a more strategic view of the introduction and management of cloud computing and the associated structural changes of the organisation because of the potential to affect the whole organisation and its operations. The introduction of cross-functional teams is one way to introduce this strategic role for ITC.

As the product and service markets become more internet based and/or supported the more important developing cross-functional teams becomes in order to link and coordinate the operations side with the ICT colleagues. Such changes require a new form of organisation that moves away from the often-found 'silo' mind-set and structure. The development and implementation of resource-based changes requires a strategic input from the Human Resources (HR) section. The study by Iyamu and Mphahlele reinforces the need for HR to align and deliver appropriate policies, "…In conclusion, the people, processes and technology are considered important agents in the deployment of the EA.Without proper policies, the synchronisation of effort and focus among the factors (people, processes and technology) could not be achieved. This could deter and further disintegrate the strategic alignment (IT and business) and the EA deployment as a whole." (Iyamu and Mphahlele, 2014, p. 17).

2.3.4 Governance

Governance is a critical aspect of organisational management and responsibility. When considering change in the technological map of an organisation it is argued that governance of the IT is becoming a more difficult aspect to resolve and as such needs specific attention during any decision-making phase.

Peterson (Peterson, 2004) defined information technology governance as "…the distribution of IT decision-making rights and responsibilities among different stakeholders in the enterprise, and defines the procedures and mechanisms for making and monitoring strategic IT decisions."

Until the beginning of the 21st Century, governance was more about standards and centralised management. It then moved from centralised to federated technology governance models and then to a more participatory form of models (Andriole, 2015). Andriole's analysis indicates that governance now involves more stakeholders than ever before with many of them outside of the organisation itself. It also suggests that participatory governance is emerging as the predominant model for the 21st Century and is accelerating amongst those companies who adopt cloud computing (Andriole, 2015, p. 50).

Governance is also linked to the legal responsibilities of an organisation in areas such as data protection and industry and regulation compliance. This, coupled with the need to protect confidential business data, reinforces the need to include governance as one of the elements of our emerging framework.

2.3.5 Business Security

Moving IT services to the cloud creates additional security challenges that need to be considered as part of the business case for moving to the cloud. A survey of industry experts by the Cloud Security Alliance identified nine major areas considered the most vulnerable (Cloud Security Alliance, 2013). These are data breaches, account & service hijacking, insecure interfaces & APIs, denial of service, malicious insiders, abuse of cloud services, insufficient due diligence, and shared technology vulnerabilities. Whilst many of these will be catered for during the 'Design phase' of the Cloud Application Life-Cycle and discussed later in this paper, it is important for these areas to be given consideration at the higher level as part of the 'Decision phase'. In addition to these nine specific areas, we propose that corporate decision makers also need to consider three major business areas specifically associated with their business operations and industry when making decisions:

- **Data Residency** - In many countries there is legislation that requires specific forms of data to be located within defined geographical areas; these may be dictated by the location of the company itself or the location at which it operates.
- **Data Privacy** - Business data is often so sensitive to the business' operations and survival that it requires very specific protection than is required by the less sensitive data.
- **Industry and Regulation Compliance** - Many organisations have access to and are responsible for data that is highly regulated and restricted. In gaining access to this data, the organisations are

required to follow defined standards in order to safeguard the private and business data as well as comply with relevant laws.

An often overlooked aspect of cloud services is the ease with which staff in organisations are able to implement their own activities and cloud storage without authorisation. An example of this is in a recent article by Joe Mont (Mont, 2016, p. 49) where a company of 150,000 employees found out that the employees were using nearly 900 cloud-based applications and programmes that relied upon some form of online storage. The company authorized only 20 of these applications. The security issues around such a situation are significant and it is unlikely that this company is an exception to what is currently happening across the business world.

We argue that it is absolutely imperative that the governance issues are discussed and agreed before a decision to move to the cloud is made and as such is included in our emerging framework.

2.4 State-of-the-Art TOE Framework

The TOE framework is an organisation-level theory that represents one segment of the innovation process, i.e. how the firm context influences the adoption and implementation of innovations (Baker, 2011). Based on this framework, the technology innovation adoption process is influenced by three aspects of an enterprise's context: Technological, Organisational and Environmental (Alshamaila and Papagiannidis, 2013, p. 253).

The TOE framework, shown below in figure 1, is almost entirely designed from an IT organisational perspective and as such does not, in its current format, assist readers to identify the fundamental issues around the wider organisational business systems. Limited exceptions to this are the subject of complexity and, competitive pressure.

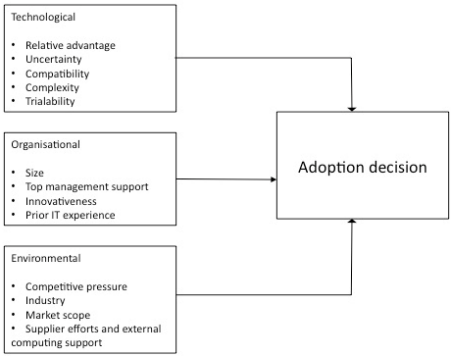

Figure 1: TOE framework for SME adaption of on-demand computing services (DePietro et al., 1990).

Without going into the finite detail of the TOE framework here, Table 1 provides an overview of the definitions of the TOE framework construct. The definitions demonstrate the absence of any of the important general business issues that need to be considered and as such reinforces the need for some further development if it is to be of real assistance to management in their adoption decision process.

Table 1: Definitions of the TOE framework constructs (Alshamaila and Papagiannidis, 2013, p. 256).

		Refers to
Technological	Relative advantage	The degree to which an innovation is perceived as being better than the idea it supersedes (Rogers, 2003)
	Uncertainty	The extent to which the results of using an innovation are insecure (Ostlund, 1974); (Fuchs, 2005).
	Compatibility	The degree to which an innovation is perceived as consistent with the existing values, past experiences, and needs of potential adopters (Rogers, 2003)
	Complexity	The degree to which an innovation is perceived as relatively difficult to understand and use (Rogers, 2003)
	Trialability	The degree to which an innovation may be experimented with on a limited basis (Rogers, 2003)
Organisational	Size	The size of the company
	Top management support	Devoting time to ICT programme in proportion to its cost and potential, reviewing plans, following up on results and facilitating the management problems involved with integrating ICT with the management process of the business (Young and Jordan, 2008)
	Innovativeness	The extent to which a client adopts innovations earlier than other members of the same social context (Rogers and Shoemaker, 1971)
	Prior technology experience	The extent of a user's experience with previous similar technologies (Heide and Weiss, 1995)
Environmental	Competitive pressure	The degree of pressure felt by the firm from competitors within the industry (Oliveira and Martins, 2010)
	Industry	The sector to which the business belonged (Yap, 1990); (Goode and Stevens, 2000)
	Market scope	The horizontal extent of a company's operations
	Supplier computing support	The supplier activities that can significantly influence the probability that an innovation will be adopted (Frambach et al., 1998)

3 AN EXAMPLE USE CASE AND A MODEL/FRAMEWORK PROTOTYPE

This paper is not an exhaustive study of organisations and change. It has sought to demonstrate that whilst the adoption of the cloud may be a perfect IT solution for many companies it is also important to take into account the wider aspects of the business and the reason for its existence. Operating a successful business is a continuing struggle to motivate and maintain the cooperation of the many actors within the organisation as well as those who are outside, such as providers, suppliers and customers. The role of IT in organisations is no longer a standalone function of supply and maintenance; it is now a strategic partner enmeshed in the business as a whole at all levels.

Table 2: Definitions of the Adapted Construct of the TOE framework constructs.

Business Strategy	Strategy	Refers to: the mission, vision and strategy of the mission, vision and strategy of the company or organisation – its direction.
	Business model	Refers to: the rationale of how the organisation creates, delivers, and captures value in economic, social, cultural or other contexts.
	Governance	Refers to: the distribution of decision-making rights and responsibilities among different stakeholders in the enterprise and its providers, suppliers and customers.
	Structure	Refers to: how activities such as task allocation, coordination and supervision are directed toward the achievement of organisational aims. It can also be considered as how individuals see their organisation and its environment.
	Security	Refers to: identifying the risks involved around the areas of data residency, data privacy and industry & regulation compliance.
	Culture	Refers to: the collective values, beliefs, behaviours and principles of organisational members.
	Power structure	Refers to: the way in which power or authority is distributed between people within groups: government, institution, organisation, or a society.
	Unique DNA	Refers to: the combination of formal and informal traits that determine your company's identity and performance.
	HRM	Refers to: a function in organisations designed to maximise employee performance in the service of an employer's strategic objectives

We have extended the TOE framework and included the following elements that we have shown are important contributors to the decision to adopt the cloud or not. These constructs are now described in the style of the original TOE framework:

Figure 2 adds the additional aspect of Business Strategy to the original TOE framework. In doing so, we believe that the framework is emerging towards a suitable set of constructs for management to use when making the important decisions around the adoption of cloud technology.

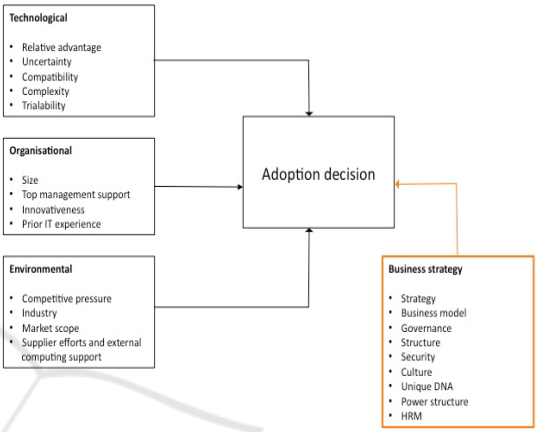

Figure 2: TOE framework for SME adaption of on-demand computing services – adapted (DePietro et al 1990).

Figure 3 provides a high-level overview of the Cloud Service Life Cycle including a Change Management Cycle with the addition of the Business Strategy construct in location.

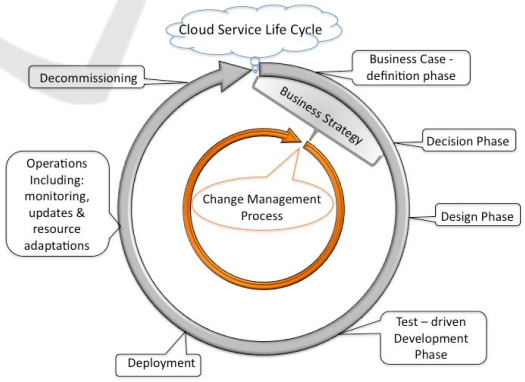

Figure 3: The Cloud Application Life Cycle.

4 CloudSDL

Based on literature research and two extensive surveys among critical infrastructure providers and regular industry we have built a list of security controls and

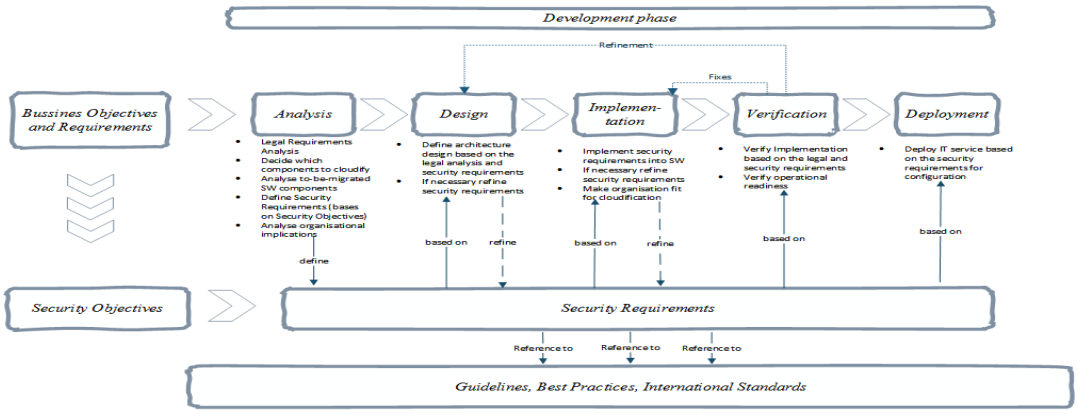

Figure 4: Cloudification Security Development Life Cycle (Wagner, et al., Aug 2015).

linked it to relevant best-practice guidelines and international standards, in which the topic is addressed. This security taxonomy can be consulted during the process of migrating IT systems to the cloud (Wagner et al., Aug 2015). According to our literature review there is currently no security development life cycle that explicitly takes into account a cloud migration scenario, so we used this taxonomy as a starting point to build a process around it, which we named the Cloudification Security Development Life Cycle (CloudSDL).

As shown in Figure 4 the CloudSDL contains five phases (Analysis, Design, Implementation, Verification, and Deployment) with two preliminary phases: (1) Business Objectives and Requirements, and (2) Security Objectives.

The CloudSDL is based on well-known security development life cycles (Howard and Lipner, 2009), (Kissel et al., 2008), and (Chandra, 2009) for the secure development of software applications.

During the Analysis phase, a decision is made upon which service or which part of a service is to be migrated to cloud. The IT service that is to be cloudified is analysed for cloud fitness (e.g., risk assessment), and an initial set of security requirements relevant for the service is specified. In this phase, we also suggest an analysis of the implications that the cloudification of the IT service has on the organization and the business. In the Design phase, the software architecture for the to-be-migrated IT service is constructed based on the security requirements specified in the analysis phase. If necessary, refinements to the security requirements are made. Based on the design, the software is implemented in the Implementation phase. Additionally in this phase, the organization is, where necessary, prepared for the use of the cloudified IT service. In the Verification phase, the software is tested against the specified security requirements. In addition, the readiness of the organization for the cloudified IT service shall be verified (e.g., special disaster recovery strategies, trainings, or revisions of SLAs might be required). If the verification does not succeed, either further implementation effort needs to be taken and/or the design needs to be revised. In the final phase of the CloudSDL, the IT service is deployed on the cloud environment, taking into account the security requirements related to platform configuration.

5 DISCUSSION

The extensive marketing of cloud services adoption focusses on the IT benefits and that as a result those services become more cost effective and technically flexible than traditional solutions. The IT and management literature and journals show that this has led to significant discussion amongst the IT professionals and other organisational stakeholders.

The cloud provider market has expanded significantly and it makes an overwhelmingly wide range of technologies available. This is causing confusion amongst corporate level stakeholders (Hernandez, 2015). This confusion has led to a lot of industry effort into explaining the various terminologies and methodologies of their products and services; focusing primarily on IT with emphasis on flexibility, scaling, availability and associated IT infrastructure cost reduction. Using this information, the business decision makers are encouraged to move to the cloud some or all of their IT. However, there is much more to a business than the IT infrastructure alone.

We argue that it is critical for the organisational decision makers to be very clear of their business case for moving to the cloud and, given the sense of

confusion amongst the corporate decision makers, a high-level framework is important to help focus on the non-IT related aspects as well as the IT itself. Porter and Heppelmann reinforce this with their discussion about the wide ranging impact that the connected technology is starting to have on the way that businesses are organised and managed, both internally and externally (Porter and Heppelmann, 2015). We have shown in this paper that the operational business side of the equation is often alluded to and yet gets lost amongst the plethora of cloud providers' technical marketing reasons for changing the IT infrastructure.

We have used the TOE framework as the basis for an emerging framework that includes the crucial, yet often neglected, business elements that we argue need to be considered when deciding whether or not to move to the cloud. In doing so, we are supporting the recognised IT elements of the decision making process and reinforcing these with the overall business model and operational strategy; we have labelled this as the Business Strategy element of the framework.

Whilst we have included nine new items into the extended TOE framework, it is important to demonstrate that these additional items are not solely confined to the 'Decision making phase' of the Cloud Application Life Cycle (CALC). Given the impact of the cloud across the whole organisation, each of these is to be considered in different ways during the remainder of the CALC. To illustrate this, we have taken the issue of Security as an example of how it links from the 'Business case definition phase' through the 'Decision phase' to the 'Design phase'. In doing so we show the key aspects of security that need to be considered from the business side of the equation as well as those from an IT perspective. We then use our primary research results (Wagner et al., Aug 2015) to provide process based guidelines for critical infrastructure providers focussing on information security. In doing so, it supports the critical infrastructure providers in migrating their services to the cloud.

6 CONCLUSIONS

In this paper we have identified the need for the decision making process to opt for transition of IT services to the cloud in some form or another to include the whole business as opposed to predominantly the IT case. In response to this need, we have extended the TOE framework.

Whilst we have extended the TOE framework, we are aware that it is not exhaustive and will require further development. For example, we have not included the Customer. Currently there is limited research in customer impact, satisfaction and quality around the provision of cloud services. We suggest that this is the next important stage of the framework development. In addition, it is necessary to further elaborate on the interconnection between the Decision-making process in the TOE framework and the technological development of the cloudified IT system. A first step towards that goal has been made by introducing the preliminary activities Business Objectives and Requirements, and Security Objectives. Also in the Analysis phase of the CloudSDL, organisational aspects are taken into account. Nevertheless, a more coherent approach should be investigated as part of our future work.

ACKNOWLEDGEMENTS

The research presented in this paper has been funded by the European Union (FP7 project SECCRIT, Grant No. 312758).

REFERENCES

Achtenhagen, L., Melin, L. & Naldi, L., 2013. Dynamics of business models – strategizing, critical capabilities and activities for sustained value creation. *Long Range Planning,* 46(6), pp. 427-442.

Alshamaila, Y. & Papagiannidis, S., 2013. Cloud computing adoption by SMEs in the northeast of England. *Journal of Enterprise Information Management,* 26(3), pp. 250-275.

Andriole, S. J., 2015. Who Owns It?. *Communications of the ACM,* 58(3), pp. 50-57.

Armbrust, M. et al., 2009. *Above the Clouds: A Berkeley View of Cloud Computing,* Berkeley: s.n.

Baker, J., 2011. The technology-organization-environment framework. In: *Information Systems Theory: Explaining and Predicting Our Digital Society.* New York (NY): Springer, pp. 231-246.

Bias, R., 2010. The Cloud is not outsourcing. *Cloudbook,* 1(2), pp. 11-13.

Bisong A & Rahman S, 2011. An Overview of the Security Concerns in Enterprise Cloud Computing. *International Journal of Network Security & Its Applications (IJNSA),* 3(1).

Buyya, R. et al., 2009. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), pp. 599-616.

Cámara, S. B., Fuentes, J. M. & Marín, J. M. M., 2015. Cloud computing, Web 2.0, and operational

performance - The mediating role of supply - chain integration. *The International Journal of Logistics Management,* 26(3), pp. 426-458.

Chandra, P., 2009. *The Software Assurance Maturity Model - A guide to building security into software development,* s.l.: s.n.

Cloud Security Alliance (CSA), 2015. *Cloud Controls Matrix,* s.l.: s.n.

Cloud Security Alliance (CSA), s.d. *Consensus Assessments Initiative Questionnaire,* s.l.: s.n.

Cloud Security Alliance, 2013. *The Notorious Nine Cloud Computing Top Threats in 2013,* s.l.: Cloud Security Alliance.

DePietro, R., Wiarda, E. & Fleischer, M., 1990. *The context for change: organization, technology and environment, in Tornatzky, L.G. and Fleischer, M. (Eds), The Process of Technological Innovation.* Lexington(MA): Lexington Books.

Frambach, R., Barkema, H., Nooteboom, B. & Wedel, M., 1998. Adoption of a service innovation in the business market: an empirical test of supply-side variables. *Journal of Business Research,* 41(2), pp. 161-174.

Fuchs, S., 2005. *Organizational Adoption Models for Early ASP Technology Stages: Adoption and Diffusion of Application Service Providing (ASP) in the Electric Utility Sector,* Vienna: s.n.

Goode, S. & Stevens, K., 2000. An analysis of the business characteristics of adopters and non-adopters of World Wide Web technology. *Information Technology and Management,* 11(2), pp. 129-154.

Greenwood, D. & Khajeh-Hosseni, A., 2010. *The Cloud Adoption Toolkit: Addressing the Challenges of Cloud Adoption in Enterprise,* s.l.: s.n.

Heide, J. & Weiss, A., 1995. Vendor consideration and switching behavior for buyers in high technology markets. *The Journal of Marketing,* 59(3), pp. 30-43.

Hernandez, P., 2015. Path to Digital Business Transformation Gets Cloudy. *eWeek,* 11 April.p. 1.

Howard, M. & Lipner, S., 2009. *The Security Development Life Cycle,* s.l.: O'Reilly Media.

Iyamu, T. & Mphahlele, L., 2014. The impact of organisational structure on enterprise architecture deployment. *Journal of Systems and Information Technology,* 16(1), pp. 2-19.

Khanagha, S., Volberda, H. & Oshri, I., 2014. Business model renewal and ambidexterity: structural alteration and strategy formation process during transition to a Cloud business model. *R&D Management,* 44(3).

Kissel, R. et al., 2008. *SP 800-64 Security considerations in the System Development Life Cycle,* s.l.: s.n.

Leavitt, N., 2009. Is Cloud Computing Really Ready for Prime Time?. *Computer*, 42(1), pp. 15-20.

Manuel, P., Al-Hamadi, H. & Qureshi, K., 2013. Challenges, strategies and metrics for supply-driven enterprises. *Annals of Operations Research.,* March.pp. 293-303.

Mell, P. & Grance, T., 2011. *The NIST definition of cloud computing,* s.l.: NIST.

Mont, J., 2016. Cloud Security is a Challenge for Users and Providers. *Compliance Week,* January, 13(144), pp. 49-65.

Morton, N. A. & Hu, Q., 2008. Implications of the fit between organizational structure and ERP: A structural contingency theory perspective. *International Journal of Information Management,* Volume 28, pp. 391-402.

Oliveira, T. & Martins, M., 2010. Understanding e-business adoption across industries in European countries. *Industrial Management & Data Systems,* 110(9), pp. 1337-1354.

Open Security Architecture (OSA), s.d. *OSA Library,* s.l.: s.n.

Ostlund, L., 1974. Perceived innovation attributes as predictors of innovativeness. *The Journal of Consumer Research,* 1(2).

Peterson, R., 2004. Crafting information technology governance. *EDPACS: The EDP Audit, Control, and Security Newsletter,* 32(6), pp. 1-24.

Porter, M. E. & Heppelmann, J. E., 2015. How Smart connected products are transforming companies. *Harvard Business Review,* October, 93(10), pp. 96-114.

Rogers, E., 2003. *Diffusion of Innovations.* New York (NY): Free Press.

Rogers, E. & Shoemaker, F., 1971. *Communication of Innovations: A Cross-Cultural Approach.* New York (NY): Free Press.

Ross, P. & Blumenstein, M., 2013. Cloud computing: the nexus of strategy and technology. *Journal of Business Strategy,* 34(4), pp. 39-47.

Ryan, W. & Loeffler, C., 2010. Insights into cloud computing. *Intellectual Property & Technology Law Journal,* 22(11).

Sultan, N., 2014. Servitization of the IT Industry: The Cloud Phenomenon. *Strategic Change: Briefi ngs in Entrepreneurial Finance,* Volume 23, pp. 375-388.

Tarabanis, K., Peristeras, V. & Fragidis, G., 2001. *Building an enterprise architecture for public administration: a high level data model for strategic planning.* Bled, s.n.

Truong, D., 2010. How Cloud computing Enhances Competitive Advantages: A Research Model for Small Businesses. *The Business Review*, 15(1), pp. 59-65.

Wagner, C. et al., Aug 2015. *Impact of critical infrastructure requirements on service migration guidelines to the cloud,* s.l.: Future Internet of Things and Cloud (FiCloud).

Wright, P. & McMahan, G., 1992. Theoretical perspectives for strategic human resource management. *Journal of Management,* 18(2), pp. 295-320.

Yap, S., 1990. Distinguishing characteristics of organizations using computers. *Information and Management,* 18(2), pp. 97-107.

Young, R. & Jordan, E., 2008. Top management support: mantra or necessity?. *International Journal of Project Managemen,* 26(7), pp. 713-725.