

MANAGING CLOUD COMPUTING: A LIFE CYCLE APPROACH

Gerard Conway¹ and Edward Curry²

¹*Innovation Value Institute, National University of Ireland, Maynooth*

²*Digital Enterprise Research Institute, National University of Ireland, Galway*
gerard.conway@nuim.ie, ed.curry@deri.org

Keywords: Cloud Computing, Project Management, Outsourcing, Life Cycle

Abstract: Cloud computing has the promise of significant benefits that include reduced costs, improved service provisioning, and a move to a pay-per-use model. However, there also are many challenges to successfully delivering cloud-based services; including security, data ownership, interoperability, service maturity and return on investment. These challenges need to be understood and managed before attempting to take advantage of what the cloud has to offer. In this paper we introduce a nine-step cloud life cycle that can be used for both the migration and the ongoing management of public, cloud-based services. A consortium of organizations using an open-innovation approach developed the life cycle. This paper describes each step of the life cycle in terms of the key challenges faced, and the recommended activities, with resultant outputs, needed to overcome them.

1. INTRODUCTION

The move to a cloud computing environment has started in earnest with the complete spectrum of businesses, from large multinationals to smaller organizations, moving their IT services to cloud computing platforms. There are many drivers for this, with reduced costs being the most commonly cited reason (Harms and Yamartino, 2010). Cloud services may be provided in a pay-per-use model that allows companies to pay only for what they actually need, with the flexibility of increasing or reducing capacity in line with business demand. In effect, cloud computing offers the advantage of switching from a Capital Expense (CapEx) to an Operational Expense (OpEx) cost model whilst promising to deliver a reduced Total Cost of Ownership (TCO). Cloud computing also provides greater flexibility and agility as new applications and services can be deployed in less time.

A major driver of cloud computing is the pressure on IT departments to deliver more and enhanced services with reduced budgets, whilst responding to ever-increasing and ever-changing business requirements. Cloud computing is also seen as a way to free up IT resources to concentrate on core activities, by outsourcing non-core activities such as management of e-mail systems. An internal IT department running cloud-based services can focus

its energy on services that offer core business value to the business, whilst letting the cloud service provider deal with the non-core services. While cloud computing promises significant benefits, there are many challenges to successfully delivering cloud-based services. These challenges need to be understood and managed before attempting to take advantage of what the cloud has to offer. In this paper, a cloud life cycle approach is introduced and it is shown how such an approach can be used for both the migration and the ongoing management of public, cloud-based services.

2. CHALLENGES WITH MANAGING CLOUD PROJECTS

Despite all of the claims made on behalf of cloud computing, it is not a panacea for all the problems faced by companies and their IT departments. Bitter experience has shown that if an IT department is struggling to deliver services, a move to cloud computing will either leave them in the same mess or potentially make it far worse (Brooks, 2010). Before we delve into the key challenges to managing cloud projects, it is important to understand that cloud computing comes in four primary deployment models: public, community, private, and hybrid.

- **Public Cloud:** Public cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group. Two examples are Amazon Web Services (AWS) and Microsoft Azure.
- **Community Cloud:** Community cloud infrastructure is shared by several organizations and supports a specific community that has a shared mission and shared goals, security requirements, policies, and compliance considerations. An example is Google Gov.
- **Private Cloud:** Private cloud infrastructure is owned or leased by a single organization and it is operated solely for that organization. Intel, Hewlett Packard (HP) and Microsoft have their own internal private clouds.
- **Hybrid Cloud:** Hybrid cloud infrastructure consists of two or more clouds (public, community, or private) that remain unique entities but are bound together by standardized or proprietary technology that enables data or application portability.

Within this work we have initially targetted the adoption challenges of migrating to a public cloud. There are a number of key challenges faced by companies that want to move to a public cloud. These challenges include:

- **Security:** With cloud computing, you are heavily dependent on the service provider for security. Cloud service providers can claim to provide complete security for access, compliance, data segregation, backup, recovery, etc. With so many new players in the market how do you know if you can trust the supplier? Do you know what their security policies are (Armbrust et al., 2010) (Heiser and Nicolett, 2008) (Grossman, 2009) (Kaufman, 2009)?
- **Data Ownership:** What happens to your data when it leaves your organization to reside in the cloud? Companies who move to the cloud probably will not completely lose track of their data but they are likely to lose some level of ownership and, in particular, control. It is important to understand who can access the data and for what purpose (Armbrust et al., 2010) (Buyya et al., 2009) (Kaufman, 2009) (Curry et al., 2010).
- **Lock-in and Interoperability:** Today each service offering provides its own unique way for the cloud to interact with applications, data and clients. It can be very difficult to use multiple vendors and to seamlessly integrate legacy and cloud services. Do you have a plan to integrate

your cloud services or to move to another cloud supplier in the future (Armbrust et al., 2010) (Dillon et al., 2010) (Grossman, 2009)?

- **Standard Architecture:** There is no standard open architecture being used for cloud services. Each of the major cloud providers (Amazon Web Services, Salesforce Force, Google App Engine, and Microsoft Azure) imposes different architectures that are dissimilar to the common architectures currently used for enterprise apps (Buyya et al., 2009). Although a customer's functional and technical requirements may be satisfied, the lack of standards will compromise the customer's ability to seamlessly migrate from one service provider to another and may need a complete re-write of their software to do so.
- **Enterprise Support and Service Maturity:** Cloud computing services may not provide the levels of reliability, manageability, and support required by large enterprises. Is the cloud supplier mature enough for your needs (Li et al., 2009) (Armbrust et al., 2010)?
- **Loss of Data:** Data stored in the cloud can be replicated across multiple machines and backed up. However, not all cloud services have the same redundancy for disaster recovery. Does the cloud supplier have an appropriate disaster recovery strategy? (Kaufman, 2009)
- **Return on Investment:** The expectation is that external cloud computing can reduce costs. However, the cost advantages for large enterprises may not be as clear as for SMEs. Currently, many large enterprises can reap the benefits of significant economies of scale in their own internal IT operations. What is the real TCO of the cloud service (Li et al., 2009)?
- **Requirement for online connectivity:** Cloud computing is impossible if you cannot connect to the Internet. A dead Internet connection means it is not possible to work, and in areas where Internet connections are few or inherently unreliable, this could be a problem. What network redundancy exists between you and the cloud supplier (Armbrust et al., 2010) (Curry, 2004)?

In order to overcome these challenges, organisations need a systematic means of reviewing their business needs and weighing up the potential gains and opportunities against the risks, so that the transition to cloud computing is strategically planned and understood.

3. DEFINING THE LIFE CYCLE

In order to deliver the advantages and overcome the challenges faced by organizations that want to migrate to cloud computing, there is now a need to define a management framework for how a cloud migration project can be successfully managed. However, because the field is new and evolving, few guidelines and best practices are available. To address this shortcoming, a consortium of leading organizations from industry, (including: Microsoft, Intel, SAP, Chevron, Cisco, The Boston Consulting Group, Ernst & Young, and Fujitsu) the not-for-profit sector, and academia have developed and tested a life cycle for systematically managing cloud migration projects. This section outlines the design process for the cloud life cycle, how the cloud life cycle aligns with the IT-Capability Maturity Framework (IT-CMF), and why a life cycle approach was taken.

3.1 Design Methodology

The Innovation Value Institute (IVI; <http://ivi.nuim.ie>) consortium uses an open innovation model of collaboration that engages academia and industry in scholarly work to amalgamate leading academic theory with the best of corporate experience – in order to advance practices for managing information technology for business value and innovation.

The development of the life cycle was undertaken using a design process with defined review stages and development activities that were based on the Design Science Research (DSR) guidelines advocated by Hevner et al. 2004. The approach followed a similar design process used to develop a maturity model for Sustainable ICT (Donnellan et al., 2011) within the IT-CMF.

Within this work we have initially targetted the adoption challenges of migrating to a Public Cloud. This lead us to leverage the work by Cullen et al., 2005 into the management of IT outsourcing projects using a life cycle. The Cullen life cycle is an in-depth piece of research on IT outsourcing that is backed up by many years of practical experience. We have adapted Cullen's work and applied the resulting life cycle to the problems of managing a public cloud migration and then running the cloud services on an ongoing basis. In particular, we examined the requirements of a public cloud project from both the life cycle and supply chain perspectives (Linder et al., 2011).

During the design process, researchers participated together with practitioners within research teams to research and develop the life cycle. The research team interviewed multiple cloud stakeholders to capture the views of key domain experts and to understand current practice and barriers to managing public cloud projects. The team widely consulted the relevant literature, both industrial and academic, on cloud computing.

Once the life cycle was developed, it was validated within a number of organizations – with learning and feedback incorporated into subsequent versions. Cloud projects were studied within 11 organizations in order to validate the life cycle. These included organizations that had successfully delivered public cloud-based projects, and also organizations that have failed cloud projects. The research approach involved a qualitative approach to data collection. Empirical evidence was collected via semi-structured interviews with representatives of the 11 companies. From this perspective, the use of the interview was an appropriate research method, as it enabled depth, nuance and complexity in data to be captured (Mason, 2002).

3.2 The IT-Capability Maturity Framework

IVI has developed an IT Capability Maturity Framework (IT-CMF) that is an innovative and systematic framework, enabling CIOs/CEOs to understand and improve their organization's maturity and enable optimal business value realization from IT investments (Curley 2004). IT-CMF provides a high-level process capability maturity framework for managing the IT function within an organization to deliver greater value from IT by assessing and improving a broad range of management practices. The framework identifies 33 critical IT processes and defines maturity models for each process. A core function of the IT-CMF is to act as an assessment tool and a management system.

Within this work we utilize a combination of the life cycle approach and the use of IT-CMF to establish the key areas a customer must identify for it to ensure it has the required level of maturity before migrating to the cloud. The resulting cloud life cycle can be applied to both the migration and the ongoing management of public cloud services.

3.3 Why does the Life Cycle Work?

The cloud life cycle applies proven and documented project management principles that are known by most IT and business managers. It breaks down the project into discrete manageable stages that allows the company to gather the correct information to make a decision before moving to the next stage. The life cycle ensures appropriate pre-planning so that the correct partners are chosen and that the impacts on the business are properly understood, managed, and controlled. For example it allows a company to identify the correct services to move to the cloud and to create plans for the impact on staff directly and indirectly impacted. It also provides a mechanism of building up a repository of knowledge and best practices to fill the current void created by this new use of technology, with its lack of standards and best practice.

4. THE CLOUD LIFE CYCLE

The cloud life cycle is broken down into four phases that are further divided into 9 steps as illustrated in Figure 1. Each step prepares the way for the following step, so the sequence is important and must be followed for a successful outcome. The reason for such an approach is it allows a company to break down its planning and workload to suit its requirements. The basic premise is that a company only commits resources one step at a time – so, as each step is completed, there is the option to stop without losing the initial investment. This incremental approach reduces the risk associated with cloud projects.

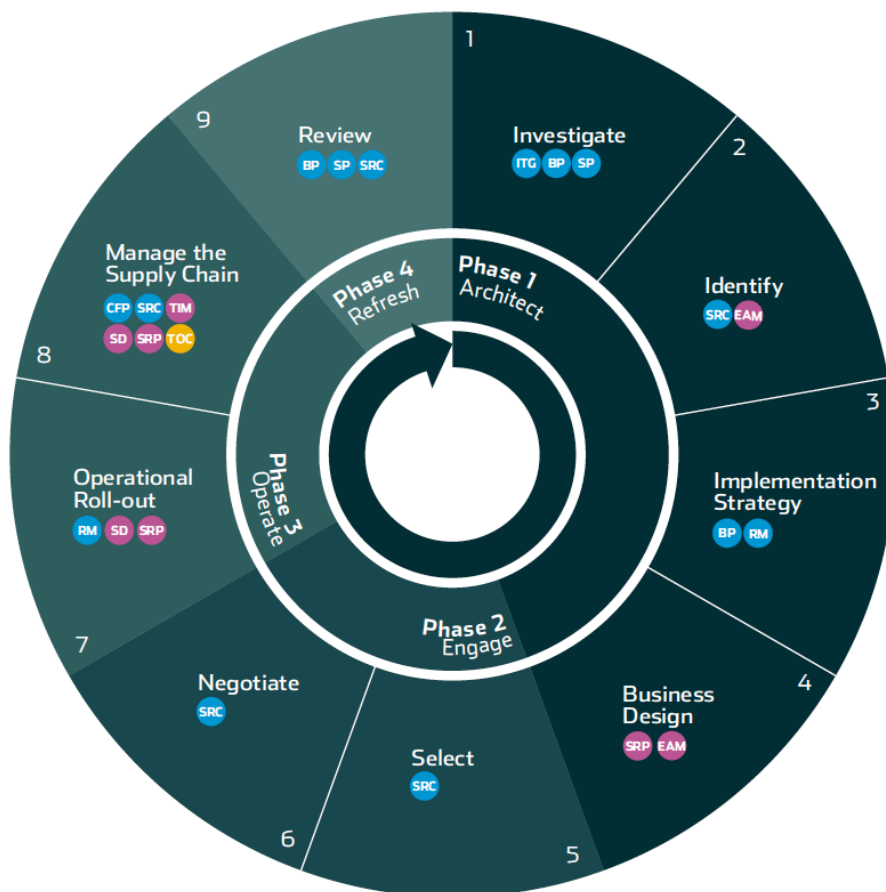


Figure 1 The Cloud Life Cycle

The four stages of the cloud life cycle are:

- **Architect:** The first phase starts with the investigation and planning of the cloud project. Typically an organization will only commit a small number of high-level resources in order to decide if they should go ahead with a full-scale project.
- **Engage:** The second phase selects a service provider that can deliver the required cloud service. Many organizations decide to stop at this stage because the appropriate cloud services are not available, or because there is no cloud provider that they have confidence in to deliver the required cloud services.
- **Operate:** The third phase is the implementation and the day-to-day management of the cloud service.
- **Refresh:** The fourth phase is the ongoing review of cloud services.

In line with all well-managed projects, this structure maintains control and allows a company to stop at any step in the project and re-start when external and or internal circumstances allow, without losing the value and investment of the work done in the preceding steps.

The steps in the cloud life cycle were surveyed among 11 organizations to determine their importance. The results of this survey are available in the appendix at the end of this paper.

The following sections describe in detail the objectives, activities, outputs and challenges for the cloud life cycle.

4.1 Phase 1: Architect

Step 1: Investigate

This step provides an insight into and an understanding of what an organization wants to achieve by moving to the cloud, and what goals and expectations are to be met. This will be based on an analysis of the appropriate industrial segment, with insights from experts and experiences from peer organizations, together with knowledge of potential suppliers.

The key challenges faced in the *investigate* step are:

- To satisfy new requirements within an existing or a reduced budget.

- To provide a clear cost-benefit analysis of cloud services using limited or no historical cost data.
- To clearly articulate the benefits of a move from CapEx to OpEx. This may need to consider the current CapEx investment of decommissioning existing services (depending on where the service is in its life cycle).
- Resistance by a perceived lack of financial control using the pay-as-you go model.
- The need for seed funding to investigate cloud options.

The critical capabilities used in the *investigate* step are IT Leadership and Governance (ITG), Strategic Planning (SP), and Business Planning (BP). The key activities and outputs of the *investigate* step are described in Table 1.

Table 1: Key Activities and Outputs for Step 1: Investigate

Activities	Outputs
<ul style="list-style-type: none"> • Determine the organization's IT objectives and its alignment with the business. • Determine what role cloud computing will play within the IT strategy. • Gather intelligence on cloud service offerings. • Validate with cloud subject matter experts. 	<ul style="list-style-type: none"> • IT strategy for cloud computing. • Strategic intent of moving to the cloud and how it progresses the business objectives. • Intelligence document on cloud service offerings and providers. • Documented understanding of what will be achieved by comparing the strategic requirements with the available services and providers.

Within the organizations we studied it was clearly shown that having a clear vision and strategy of what can be achieved by moving to cloud computing was a distinct advantage. Once the strategy and vision was clearly defined and communicated, it was a much easier task to see what services were available and what service providers could deliver. Organizations that lacked this vision experienced resistance – particularly from the user community, who were not active participants as they failed to see the strategic and financial benefits.

Step 2: Identify

Objectively assess what areas of the business are appropriate to outsource to the cloud and what impact this will have on the current delivery model. This will require an understanding of the

current state, so that it can be compared to the desired future state. At a minimum, the impact on the service, people, cost, infrastructure, stakeholders and how the impact will be managed should be considered.

The key challenges faced in the *identify* step are:

- To define the Enterprise Architecture. This can be particularly time-consuming if none is already in place.
- To objectively choose the appropriate service to outsource.
- To engage with both users and IT personnel who will be impacted, particularly if their job is being altered or removed.

The critical capabilities used in the *identify* step include Enterprise Architecture Management (EAM) and Sourcing (SRC). The key activities and outputs of the *identify* step are described in Table 2.

Table 2: Key Activities and Outputs for Step 2: Identify

Activities	Outputs
<ul style="list-style-type: none"> • Determine what services will be outsourced to the cloud, and consider impacts on the service, people, cost, infrastructure, and stakeholders. • Decide what type of cloud outsourcing model will be used, and why it is suitable. • Document the current and future states of the IT infrastructure. 	<ul style="list-style-type: none"> • A List of services to be outsourced to the cloud, with documented understanding on impacts to service, people, cost, infrastructure, and stakeholders. • A Cloud outsourcing model, with documented justification. • Documented current and future states of the IT structure.

Choosing the correct service to outsource was influenced by the maturity of the service and the desired functionality. Organizations that successfully migrated to the cloud: had a well-defined Enterprise Architecture, engaged both users and suppliers at an early stage, and recruited external expertise in areas not covered by internal resources. Organizations that attempted to correct problems with their existing services by simply moving them to the cloud, failed, as they just moved the problem to the new environment.

Step 3: Implementation Strategy

Define at a strategic level how the cloud services that are to be outsourced will be rolled out. This will document how key decisions will be made later on, by defining strategies on: staffing,

communication, program roll-out, organizational rules, and risk assessment.

The key challenges faced in the *implementation strategy* step are:

- To get the commitment and support to make key resources available.
- To clearly define business and technical requirements.
- To fully engage key stakeholders and users.
- To agree a formal decision-making / sign-off process with stakeholders.

The critical capabilities used in the *implementation strategy* step are Business Planning (BP) and Risk Management (RM). The key activities and outputs of the *implementation strategy* step are described in Table 3.

Table 3: Key Activities and Outputs for Step 3: Implementation Strategy

Activities	Outputs
<ul style="list-style-type: none"> • Determine the roll-out approach and how the program will be managed. • Detail how the program will be staffed and reported. • Decide how cloud suppliers will be engaged, selected and managed. • Determine how risks will be assessed and managed, including data recovery and in-sourcing. 	<ul style="list-style-type: none"> • A program roll-out strategy. • A Communication strategy. • A strategy to manage staff impacted by the migration to cloud. • A Cloud risk management strategy. • A Cloud supplier management strategy.

One of the key findings of our research was that organizations that wanted to move to the cloud needed to fully understand the impact of the migration on the user community, and on IT support staff. Those organizations that did not understand this impact and that failed to plan accordingly either lost key resources or experienced resistance from the IT and user community – both during and after the migration.

Step 4: Business Design

Design what is to be outsourced to the cloud and what the future state will look like. This will detail the new service, how it will be managed, how it interfaces to the existing / remaining systems, and how it will be monitored and reported. To provide requirements with sufficient detail to have a meaningful conversation with suppliers so that they can be objectively compared, based on cost and quality of service.

The key challenges faced in the *business design* step are:

- To provide a clear definition of the existing and desired interfaces.
- To clearly define what is negotiable / non-negotiable.
- To engage and build a relationship with the stakeholders that is based on trust.

The critical capabilities used in the *business design* step are Enterprise Architecture (EAM) and Service Provisioning (SRP). The key activities and outputs of the *business design* step are described in Table 4.

Table 4: Key Activities and Outputs for Step 4: Business Design.

Activities	Outputs
<ul style="list-style-type: none"> • Detail the service offering you wish to tender for. • Clearly define negotiable / non-negotiable issues around contracts, service-level agreements (SLA), and pricing model 	<ul style="list-style-type: none"> • Detailed and clear tender documents for cloud suppliers.

The research demonstrated that organizations that developed clear and concise tender documentation had improved discussions with suppliers without placing undue limitations and constraints on what could be provided. Conversely, those organizations that had poorly-defined requirements spent a lot of time in discussions with suppliers and were driven by the supplier’s agenda.

4.2 Phase 2: Engage

Step 5: Select

Based on the requirements and the other criteria defined by the Architect phase this step will *select* the best supplier based on value, sustainability, and quality.

The key challenges faced in the *selection* step are:

- In a lot of cases it was found that the cloud supplier provided the Contract, Service Level Agreement (SLA) and pricing as a standard offering. The challenge was to ensure all business and user requirements were still satisfied.
- To balance requirements between what functionality is available now, with what will be available in the future.
- To retain objectivity and do a thorough background check on all suppliers.
- To have a back-out / alternatives strategy if things change or go wrong.
- To retain the overall strategic intent and core requirements; that is, do not compromise to get a particular service up and running.

The critical capability used in the *select* step is Sourcing (SRC). The key activities and outputs of the *select* step are described in Table 5.

Table 5: Key Activities and Outputs for Step 5: Selection

Activities	Outputs
<ul style="list-style-type: none"> • Define the tender/bid process. • Select and staff an evaluation team. • Invite bids/tenders. • Evaluate suppliers against the defined criteria. • Shortlist the supplier(s). • Carry out due diligence. 	<ul style="list-style-type: none"> • A tender process. • Evaluation criteria. • A shortlist of suitable suppliers with caveats. • A Due diligence report.

The organizations that were successful were characterised by:

- Only accepting solutions that had the required functionality.
- The active involvement of the user community via surveys and by validation of the proposed solution.
- Choosing suppliers that were prepared to work and resolve issues prior to the migration.

Organizations that compromised by accepting partial functionality with the promise of enhanced functionality at a later stage, or that skipped proper validation to meet deadlines, ended up with problems that led to failure of the cloud services, or were very expensive to rectify.

Step 6: Negotiate

This step is to complete the final negotiation, pick the preferred supplier, get internal approval and sign the contract(s).

The key challenges faced in the *negotiate* step are:

- To maintain control and objectivity by resisting any major last-minute changes in order to achieve sign-off; in other words be prepared to walk away.
- To have clearly defined and agreed contingency plans for disaster and change scenarios.
- To understand the cloud supplier get-out clauses and to make sure there is enough time to move cloud services in-house, or to an alternative cloud supplier.

The critical capability used in the *negotiate* step is Sourcing (SRC). The key activities and outputs of the *negotiate* step are described in Table 6.

Table 6: Key Activities and Outputs for Step 6: Negotiate

Activities	Outputs
<ul style="list-style-type: none"> • Define the negotiation strategy. • Select and staff the negotiation team. • Carry out negotiations. • Select the preferred cloud supplier. • Get internal approvals and sign the contract. 	<ul style="list-style-type: none"> • A negotiation strategy. • Results of the negotiation. • Signed final documents: Contract, SLA and Pricing document.

Our research showed significant variations in the attitude of cloud suppliers to accommodate client requirements. Some suppliers would only offer their default service offering and standard SLA, while other cloud suppliers invested significant time and effort to ensure they delivered on all major requirements. Those organizations that had invested time in the earlier steps of the life cycle, particularly the engagement of users, had a smooth sign-off with no major, last-minute problems.

Problems were found with a number of organizations when they treated this final step as a rubber-stamping exercise. One example showed that although the preceding step highlighted issues around due diligence, the promise of a cost reduction resulted in a binding contract being signed. As a result, major problems occurred during implementation that lead to a contractual dispute with the supplier.

4.3 Phase 3: Operate

Step 7: Operational Roll-out

To put together a project team that will manage the transition of the agreed services to the new cloud service. This will require the transition of the service itself, the management of staff impacted, communication to all stakeholders, knowledge retention / transition, and acceptance sign-off.

The key challenges faced in the *operational roll-out* step are:

- To keep to the desired timelines, particularly for dates that cannot be changed.
- To get access to appropriate case studies of previous successful roll-outs of similar services.
- To resist the temptation to compromise on quality in order to maintain the schedule.
- To get formal user and technical sign-off.

The critical capabilities used in the *operational roll-out* step are Service Provisioning (SRP), Solution Delivery (SD), and Risk Management (RM). The key activities and outputs of the *operational roll-out* step are described in Table 7.

Table 7: Key Activities and Outputs for Step 7: Operational Roll-out

Activities	Outputs
<ul style="list-style-type: none"> • Finalize and publish transition plans. • Select and staff the transition team. • Agree and publish acceptance criteria. • Carry out the transition. • Communicate progress. • Conduct knowledge transfer. • Manage staff (directly and indirectly) impacted. 	<ul style="list-style-type: none"> • A roll-out plan. • Progress updates. • A signed acceptance document.

The research has shown that many of the organizations had a very smooth transition due to: good planning, the full engagement of users, and a strong partnership with the supplier. The research highlighted that using a phased approach that allowed the option to roll back to an in-house version at any stage significantly reduced the risk and exposure to the business. Organizations that experienced difficulties in the transition to cloud computing missed vital steps in their planning. Examples included: not having the system validated and tested by end users, or reducing the time required for testing to meet deadlines.

Step 8: Manage the Supply Chain

It is important to manage the new cloud service as efficiently and effectively as possible. The organization will need to adapt to the new setup, particularly at IT management level – because rather than directly managing internal resources, the requirement will be to manage the cloud supplier and in particular the supplier relationship. This will require effective monitoring and control so that issue, variations and disputes can be resolved to the satisfaction of both parties.

The key challenges faced in the *manage the supply chain* step are:

- The integration of the cloud service with existing support and reporting structures.
- That IT management make a smooth transition from managing their own internal staff to managing the cloud supplier and the interfaces.
- The control, communication and coordination of internal and external changes.

The critical capabilities used in the *manage the supply chain* step include Capacity Forecasting and Planning (CFP), Sourcing (SRC), Technical Infrastructure Management (TIM), Solution Delivery (SD), Service Provisioning (SRP), and Total Cost of Ownership (TCO). The key activities and outputs are described in Table 8.

Table 8: Key Activities and Outputs for Step 8 Manage the Supply Chain

Activities	Outputs
<ul style="list-style-type: none"> • Manage and report at cloud service operational level. • Capture and manage issues, variations and disputes. • Manage the supplier relationship. • Change management. • Continuous improvement. • Assess and validate how the cloud service is performing. 	<ul style="list-style-type: none"> • Day-to-day cloud service performance metrics. • Status on issues, problems, variations, and disputes. • Supplier meeting minutes. • A change management report. • Audit reports.

Building a relationship with the cloud supplier was the key to success in many of the projects we studied. Some companies have gone further and built a strategic partnership with their suppliers, which further increased their success. The research highlighted that the risk to the business can be significantly reduced if you retain the flexibility to move the service back in-house or to an alternative supplier within an agreed notice period.

Where problems arose, they were mainly around the management of the supplier. There were examples where the supplier did not deliver as per the signed agreement and in one instance the supplier went out of business, highlighting the need for adequate risk assessment and mitigation.

4.4 Phase 4: Refresh

Step 9: Review

To review the cloud service requirements based on: the cloud service itself, other changes within the business, changes within the supplier organization, or the need to change the supplier.

The key challenges faced in the *review* step are:

- To prioritise and get approval to start a new cloud service project cycle.

The critical capabilities used in the *review* step are Strategic Planning (SP), Business Planning (BP), and Sourcing (SRC). The key activities and outputs of the *review* step are described in Table 9.

Table 9: Key Activities and Outputs for Step 9: Review

Activities	Outputs
<ul style="list-style-type: none"> • Gather intelligence on the relevant market segment, cloud service technology trends, and supplier offerings. • Audit cloud supplier performance and compare to alternatives. • Understand and assess how other changes in the organization impact on the existing cloud service arrangement. • Based on the above inputs, regularly reassess and review requirements. • Make and present a business case for any significant change to the current cloud service arrangement in order to get approval to start a new cycle. 	<ul style="list-style-type: none"> • An intelligence report for next generation cloud service offerings. • Cloud supplier audit results. • A business case for any proposed changes.

Some of the organizations researched had a clear vision of the future that provided them with an understanding of how cloud service offerings could be enhanced by the use of common standards, the use of cloud brokers and a standard integrated architecture. Other organizations

struggled to integrate their services due to vendor lock-in and not investing sufficient resources with the correct skills to decide what was needed for the future. In one instance it was found that cloud services were being purchased without any central control, leading to a mixture of solutions that was very difficult to integrate.

5. CONCLUSION

The use of a cloud life cycle has been shown to be a very good mechanism for organizations to control and manage not only their migration but also the ongoing, day-to-day management of their public cloud environment. The research for each of the nine steps described above clearly demonstrates the value of using a cloud life cycle to control and manage the move to cloud. The cloud life cycle provides an organization with a management structure to assess the following:

- The readiness/maturity of an organization to move to the public cloud.
- How the organisation is managing the new environment on a day-to-day basis after it is migrated.
- What new services can be moved to a public cloud environment.

Future research on the cloud computing life cycle will focus on the development of a cloud vendor assessment that uses both IT-CMF and the cloud life cycle to help the consumer determine the correct cloud computing service offerin for their needs.

6. ACKNOWLEDGEMENTS

We would like to recognize the contribution of the members of the Innovative Value Institute's Cloud Computing working group. Enterprise Ireland funded part of the work presented in this chapter under Grant CC/2009/0801.

7. REFERENCES

Armbrust, B., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., et al. 2010. A

- view of cloud computing. *Communications of the ACM*, 53(4), 50-58. ACM.
- Brooks, C., 2010. Heroku learns the hard way from Amazon EC2 outage, SearchCloudComputing.com
- Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), 599-616. Elsevier B.V.
- Cullen, S., Seddon, P., & Wilcox, L., 2005. *Managing Outsourcing, The Life Cycle Imperative*. MIS Quarterly Executive, pp.229-256.
- Curry, E. 2004. *Message-Oriented Middleware*. In Q. H. Mahmoud (Ed.), *Middleware for Communications* (pp. 1-28). Chichester, England: John Wiley and Sons.
- Curry, E., Freitas, A., & O'Riain, S. 2010. *The Role of Community-Driven Data Curation for Enterprises*. In D. Wood (Ed.), *Linking Enterprise Data* (pp. 25-47). Boston, MA: Springer US.
- Curley, M. 2004. *Managing Information Technology for Business Value: Practical Strategies for IT and Business Managers*. Intel Press.
- Dillon, T., Chen Wu., & Chang, E., 2010. *Cloud Computing: Issues and Challenges*, 2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), pp.27-33.
- Donnellan, B., Sheridan, C., & Curry, E. 2011. *A Capability Maturity Framework for Sustainable Information and Communication Technology*. *IEEE IT Professional*, 13(1), 33-40.
- Grossman, R.L., 2009. *The Case for Cloud Computing*, *IT Professional*, vol.11, no.2, pp.23-27
- Harms, R., and Yamartino, M., 2010. *The Economics of the Cloud*, White Paper, Microsoft.
- Heiser, J., and Nicolett, M., 2008. *Assessing the Security Risks of Cloud Computing*, Gartner
- Hevner, A. R. March, S. T. Park, J. & Ram, S. 2004. *Design Science in Information Systems Research*, *MIS Quarterly*, vol. 28, no. 1, pp. 75-105.
- Kaufman, L. M., 2009. *Data Security in the World of Cloud Computing*, *IEEE Security and Privacy*, vol. 7, no. 4, pp. 61-64.
- Li, H., Sedayao, J., Hahn-Steichen, J., Jimison, E., Spence, C., & Chahal, S., 2009. *Developing an Enterprise Cloud Computing Strategy*, Intel White Paper
- Lindner, M. A., McDonald, F., Conway, G., & Curry, E. 2011. *Understanding Cloud Requirements – A Supply Chain Life Cycle Approach*. Second International Conference on Cloud Computing, GRIDs, and Virtualization (Cloud Computing 2011), (pp. 20-25). Rome, Italy: IARIA.
- Mason, J., 2002. *Qualitative Researching*, London, Sage Press.