Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2013 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-18-2013

Towards a Consumer Cloud Computing Maturity Model - Proposition of Development Guidelines, Maturity Domains and Maturity Levels

Daniel Weiss
Technical University of Berlin, weiss@ikm.tu-berlin.de

Jonas Repschlaeger
Technical University of Berlin, j.repschlaeger@tu-berlin.de

Rüdiger Zarnekow
Technical University of Berlin, zarnekow@ikm.tu-berlin.de

Holger Schroedl
Otto-von-Guericke-University Magdeburg, holger.schroedl@ovgu.de

Follow this and additional works at: http://aisel.aisnet.org/pacis2013

Recommended Citation
Weiss, Daniel; Repschlaeger, Jonas; Zarnekow, Rüdiger; and Schroedl, Holger, "Towards a Consumer Cloud Computing Maturity Model - Proposition of Development Guidelines, Maturity Domains and Maturity Levels" (2013). *PACIS 2013 Proceedings*. 211.
http://aisel.aisnet.org/pacis2013/211

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2013 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

TOWARDS A CONSUMER CLOUD COMPUTING MATURITY MODEL - PROPOSITION OF DEVELOPMENT GUIDELINES, MATURITY DOMAINS AND MATURITY LEVELS

Weiss, Daniel, Institute for Information and Communication management, Technical University of Berlin, Berlin, Germany, weiss@ikm.tu-berlin.de

Repschläger, Jonas, Institute for Information and Communication management, Technical University of Berlin, Berlin, Germany, repschläger@ikm.tu-berlin.de

Zarnekow, Rüdiger, Institute for Information and Communication management, Technical University of Berlin, Berlin, Germany, zarnekow@ikm.tu-berlin.de

Schroedl, Holger, Institute of Business Information Systems, Otto-von-Guericke-University Magdeburg, holger.schroedl@ovgu.de

Abstract

In recent years, Cloud Computing (CC) has transformed from a new trend to IT management reality. Its potential promises to significantly change computing and benefit many organisations but at the same time uncertainty and the need for managerial guidance prevail. To benefit from the opportunities that CC promises, organisations need to adapt to the new circumstances that this phenomenon triggers and develop new capabilities. Maturity models have shown to be an excellent and easily applicable tool for the assessment and improvement of capabilities. However, there is no fully developed and universally accepted CC maturity model (CCMM) so far. Through the execution of a maturity model development process, this contribution is aiming at deriving development guidelines for the future development of a holistic consumer CCMM. Additionally, content and structure in the form of maturity domains and maturity levels are proposed throughout the development process, the combination of which represents the first steps towards a holistic consumer CCMM.

Keywords: *Cloud Computing, Maturity Model, Guidelines, Maturity Domains, Maturity Levels*

1 INTRODUCTION

Over the last years, Cloud Computing (CC) has emerged as a potential game-changing phenomenon in information technology (IT), raising massive interest in IT professionals. Many scholars link it with various benefits including the decrease of IT infrastructure and operational costs, increased flexibility as well as easy and fast scalability (Martens et al., 2011). Naturally, there are inherent risks such as the protection of sensible data, security and availability that lead to a high level of uncertainty and hesitance from adopting organisations (Nuseibeh, 2011). New paradigms such as CC force organisations to develop and improve on new skills and capabilities in order to prevail in the new economic and technological environment. Maturity models (MMs) have seen a steady and strong surge, especially in IT, as an approach "[…] for continuous improvement or as a means of benchmarking or self-assessment" (Mettler et al., 2010). It then comes as a surprise to see only a few MM approaches that are trying to aid organisations in the assessment and improvement of CC competencies.

A Cloud Computing Maturity Model (CCMM) can assist organisations that want to implement CC, by assessing the present capabilities and exposing a path for continuous improvement of those capabilities. It leads to the following research question: *How can the characteristics of CC be adequately integrated into the development process of a CCMM and consequently, how can CC maturity be expressed through maturity domains and maturity levels?*

The goals of this paper therefore are to derive development guidelines for a future CCMM and to propose tangible content for a CCMM in the form of maturity domains and maturity levels. It can be seen as taking the first steps towards a consumer-centric service CCMM. The paper will be structured as follows: First, necessary theoretical background is presented in order to introduce the subject matter adequately. Second, the research methodology used to derive the guidelines and the content is explained. In chapter four, a procedure model for the development of IT MMs is executed and lastly, chapter five will conclude the findings.

2 THEORETICAL BACKGROUND

2.1 Cloud Computing

CC is the result of many intertwining aspects and despite being a relatively new paradigm, CC in its entirety and the individual features have already seen many definitions. However, the five essential characteristics and the definition proposed by the National Institute of Standards and Technology (NIST) are increasingly accepted amongst researcher and practitioners (Che et al., 2011). The five essentials are: On-demand self-service, broad network access, resource pooling, rapid elasticity as well as measured service (Badger et al., 2012). To put it into a comprehensive sentence, CC represents the ability for a consumer to unilaterally increase (or decrease) ones computing resources, through a network, at any given moment and to a seemingly unlimited scale whilst only paying for as many resources as are actually being used, (ideally) without the need to interact with the cloud provider.

Additionally to the five essentials, there are four deployment models (private, public, hybrid and community clouds) and three service models that have been established (Che et al., 2011). The three service models are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) and they all follow the same basic idea, namely to access software and/or computing resources provided by the provider's cloud infrastructure. IaaS offers the biggest range of resource of the three models, while SaaS is the most widespread model and has already existed before CC.

However, in neither service model does the customer have control over the underlying, physical infrastructure (Dillon et al., 2010).

Lastly, there are numerous benefits and risks that are associated with CC. As for benefits, in particular the decrease of IT infrastructure and operational costs, increased flexibility, faster deployment of services and products as well as refocusing on core competencies are often named as the most significant ones (Sarkar and Young, 2011). Typically named risks are data related concerns (e.g. data loss and data security), governance and security issues, managerial and alignment challenges as well as limited availability (Dillon et al., 2010; Che et al., 2011; Sarkar and Young, 2011).

2.2 Maturity Models

MMs have long been applied in many different fields of information systems (IS), representing a versatile tool for multiple purposes within the areas of improvement of capabilities and benchmarking or self-assessment (Mettler et al., 2010). Especially Nolan's work (Nolan, 1979) had significant influences on MMs in IS, his proposed basic structure is still often used today. Crosby (1979) developed the Quality Management Maturity Grid (QMMG), which lead to the development of the most widely known MM, the Capability Maturity Model (CMM) by the Software Engineering Institute (SEI) (leading to the Capability Maturity Model Integration (CMMI)). There are several features that can be transferred from various maturity approaches, leading to the conclusion that maturity in IS can be represented through several stages of capabilities within a domain that can steadily be improved to achieve perfection, i.e. full maturity (Pöppelbuß and Röglinger, 2011). A MM consequently describes the path from the initial status quo to the state of perfection in a predictable evolutionary order. In addition to the basic components, MMs can be differentiated by their main objective, i.e. they can be descriptive (investigating the status quo of capabilities through given characteristics), prescriptive (specific actions and measures are suggested) or comparative (giving organisations the opportunity to benchmark) (Pöppelbuß and Röglinger, 2011).

2.3 Cloud Computing Maturity Models

This chapter will give a short overview of the status quo of CCMMs. Because this is also a sub-phase in the procedure model used in chapter 4, only the most significant findings will be presented here and the more detailed analysis will be presented throughout chapter 4. Several CCMMs have been proposed so far, mainly with the intention to help organisations with the adoption of CC services. Ten models could be found (seven from practitioners) during the research (see Appendix 1). Most models are not sufficiently documented and do not present necessary information to fully comprehend and validate the authors intentions. Additionally, scientific rules and requirements are mostly not being followed by the developers of the models, which is also expressed through the (mostly) non-existent definition of maturity in the context of CC. Nearly every existing model expresses cloud maturity through a combination of criteria or dimensions (from here on called domains), with the number of domains ranging from four to nine. Lastly, the models suggest that the most significant issues of CC adoption are represented through managerial and organisational challenges rather than technical. The findings strengthened the view that there is a need for scientifically validated and documented CCMM.

3 RESEARCH METHODOLOGY

The theoretical background introduced was derived through a literature review, which "[...] represents the foundation for research in IS" (Webster and Watson, 2002). Because scientific literature about CC MMs was expected to be scarce, the scope of the literature review was designed to be as broad as possible. It is common practice in IS research to identify valid literature through the search in prominent journals, online databases and conferences (Yang and Tate, 2009). Mainly online databases including EBSCOhost, IEEE Xplore, ScienceDirect and ACM Digital Library were used in the

process, covering the majority of the top IS journals and conferences. The Keywords used for the search included “cloud computing maturity model”, “cloud computing”, “cloud computing maturity”, “maturity models in IS/IT” and similar terms.

This paper is based on the research framework in IS proposed by Hevner et al. (2004). It is argued that “information systems are implemented within an organization for the purpose of improving the effectiveness and efficiency of that organization” and that design science research (DSR) poses as a problem solving paradigm, helping researcher and practitioners to contribute to the solution of IS related issues (Pöppelbuß and Röglinger, 2011). The outputs of DSR are IT artefacts, MMs representing a significant group of said artefacts. The conducted literature review functions as the knowledge base and at the same time (e.g. the overview of existing MMs) reveals the need for a CCMM. Artefacts (i.e. the proposed CCMM) are the center of IS research and ideally the outcomes of this research will have positive impacts both on the knowledge base and the business environment.

The research approach of this paper follows the procedure model for the development of MMs in IT management proposed by Becker et al. (2009). The model and the eight requirements suggested by the authors are directly influenced by the seven DSR guidelines proposed by Hevner et al., “[...] which set the de facto standard for the conduct and evaluation of Design Science Research” (Venable, 2010). The seven guidelines have been altered and adapted by Becker et al. to adequately fit into the context of MM development and include the following requirements: Comparison with existing maturity models (R1), iterative procedure (R2), evaluation (R3), multi-methodological procedure (R4), identification of problem relevance (R5), problem definition (R6), targeted presentation of results (R7) and scientific documentation (R8). Additionally, Becker et al. proposed a model that consists of eight phases, incorporating the requirements at various points. Because the evaluation part of the procedure model cannot be executed here, figure 1 shows the model altered to the necessities of this contribution. Already integrated in the figure are the guidelines (G1-G8) and the domains (D1-D6) that will be derived and explained in the next chapter.

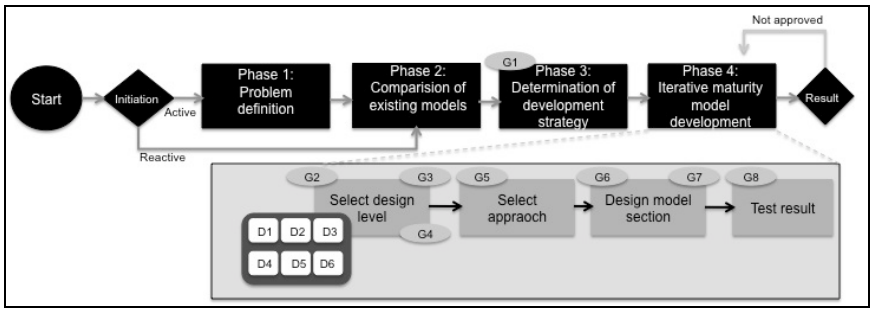

Figure 1: Altered procedure model by Becker et al. (2009).

It is important to note that the procedure model consist of four additional phases that involve transfer and evaluation. For an evaluated CCMM these phases must be carried out since they are a crucial and helpful part of the development process. The evaluation will be carried out in future contributions, however, the content proposed here and the model executed are scientifically valid and can immediately act as a helpful tool to organisations adopting CC services.

4 TOWARDS A CLOUD COMPUTING MATURITY MODEL

4.1 Phase 1: Problem definition

In compliance with requirements R5 and R6, the first phase urges the developer to show that there is indeed a need for a CCMM. The problem needs to be defined and it has to be proven that the problem is relevant for IS researchers and practitioners. Therefore, a closer look at the goal of IS research is necessary to define the problem relevance. Hevner et al. state that “the objective of research in information systems is to acquire knowledge and understanding that enable the development and

implementation of technology-based solutions to heretofore unsolved and important business problems" (Hevner et al., 2009). They define a problem as the difference between the current state and the wanted state of a system. In the context of a CCMM, the problem is that the MMs available are not sufficient to satisfy the business demands of today (the current state) and therefore a new CCMM is necessary in order to adequately answer business' CC problems (the goal state).

Organisations have to constantly improve their capabilities, decrease costs, improve quality, etc., in order to gain (or keep) a competitive advantage (De Bruin et al., 2005). Especially IT organisations see themselves in a volatile, fast paced and globalised competition. CC is a new paradigm and easily available information, best practices and helpful tools (e.g. in the form of CC MMs) are difficult to obtain. As chapter 2.3 and the following phase will show, a commonly accepted and used CCMM could not be found. As a result of these considerations, the current state of CC for service customers can safely be described as one that is dominated by uncertainty, unawareness and a lack of adequate tools to implement, assess and improve upon CC services (Martens et al., 2011). The goal state consequently is characterised by certainty of risks and benefits, structured management approaches and the availability of adequate tools to assess and improve CC. Therefore the conclusion can be drawn that there are differences between the current state for CC service customers (uncertainty, hesitation, lack of management tools and methods, etc.) and the goal state (certainty, existence of management tools and methods, etc.). The existence of differences in current and goal state leads to the decision that there exists a problem in the CC environment of service customers (Repschläger et al., 2012).

Additionally, the procedure model by Becker et al. requires the determination of the targeted domain (e.g. IT management as a whole vs. a partial discipline) and the targeted audience (e.g. external vs. internal). As for the targeted domain, CCMMs can be targeted at every level within IT and business management, depending on the goal and scope. The goal here is to assist organisations using CC services to assess and ultimately improve their CC capabilities. Therefore, the targeted domain is the business management of the organisation. The targeted audience is primarily internal, as it will help assess and improve CC capabilities within an organisation. Finally, it is necessary to show that the problem is relevant to the IS community. Moreover, the relevance of the intended solution (the CCMM) must be demonstrated for the targeted audience. Usually, MMs point out that the targeted domain is relevant and therefore a MM for that domain must be relevant. The relevance of CC can be seen through the intensive research and repeatedly high rankings of CC in IT and business studies (Gartner, 2012). MMs are widely accepted to help organisations to assess their current state of capabilities, to find potential for improvement and bring clarity and certainty to a given management field (Hevner et al., 2004; Mettler et al., 2010). Therefore, a CCMM can bring CC from the current, unsatisfactory to a preferred or targeted state, posing as a solution to the problem defined above.

4.2 Phase 2: Comparison of existing models

There are a few aspects that attract immediate attention when comparing the ten maturity model approaches that were identified (see Appendix 1). First, most of the models show a lack of documentation making it difficult to comprehend the exact intentions of the developers. Second, scientific rules and guidelines (e.g. in the form of development models) are almost completely ignored. Only one model mentioned a structured development approach (Martens et al., 2011), but most of the documentation for this model is not available at this moment. The absence of documentation is especially noticeable for the requirements 1-4 and 7-8. From a scientific point of view the status quo of CCMMs is not satisfactory and further findings are substantial. Third, it appears that the CC domains are preferably divided into organizational and technological domains, which cover all relevant aspects of CC maturity. Existing models are centred on organisational rather than technological domains, e.g. Verma et al. (2010) and Oakton (2012) propose only a single technological domain but four respectively five organisational domains.

4.3 Phase 3: Determination of development strategy

Four basic development strategies are distinguished by Becker et al.: the development of an entirely new model, the enhancement of existing models, the combination of several models into a new model and the transfer of structure or content from existing models to new application domains. Throughout phases three and four, development guidelines will be proposed by the authors, accompanying the procedure model at decision points. For a better overview, the guidelines are already summarised in Table 1 and will be explained in more detail throughout the procedure model.

Guideline	Description
G1 (development strategy)	The design strategy of a CCMM should be to develop a new model following a scientifically valid development model. Legitimate content and/or structure of existing models should be transferred, if adequate.
G2 (design level)	The basic design level of a CCMM should include multiple domains to ensure a comprehensive approach. The domains should be of technological as well as of organisational nature.
G3 (domain determination)	A CCMM should have at least six domains to ensure a holistic approach, including the organisational domains Governance, Security, Organisational readiness and Processes as well as the technological domains IT Infrastructure and Operational IT management.
G4 (model approach)	A CCMM should follow the basic structural approach introduced by the CMMI-family of maturity models.
G5 (approach selection)	The research methods used to conduct sub-phase 4.3 should consist of an extensive literature analysis and be enhanced by explorative methods if necessary and adequate.
G6 (mode approach)	A CCMM should follow a staged approach as opposed to a continuous approach.
G7 (maturity levels)	A CCMM should consist of the five maturity levels initial, assessing, determined, managed and optimised.
G8 (test results)	The results of the iterative development process of a CCMM should be iteratively evaluated. The number of evaluators should thereby be steadily increased to ensure full usefulness, plausibility, validity and problem adequacy.

Table 1: Overview of the proposed development guidelines

The comparison showed no established and accepted CCMM and that existing models often have deficits according to the requirements of the procedure model. This leads to the assumption that the strategy should be to develop an entire new model. However, most models share the CMM-like structure developed by the SEI and express CC maturity through a combination of domains, which are aspects that can reasonably be integrated into a CCMM. In general, the CMM-like structure is predominant in the world of MMs (and IT MMs) and can also be adequately used in a CCMM. A CCMM should be new to avoid the deficiencies of the existing models but at the same time transfer valid structure and content from existing models. The lack of documentation and the shortage of CCMMs that are based on scientific models strengthen this line of argumentation (leading to guideline G1 (development strategy)). The transferable content and structure will be determined in the next phase. G1 potentially needs to be revised as more CCMMs are developed and the given circumstances change.

4.4 Phase 4: Iterative maturity model development

Phase four is the central phase of Becker et al.'s procedure model where the actual content, structure and design are defined. The phase should be carried out iteratively, ensuring full validity and comprehensiveness.

Sub-phase 1: Select level design

The design level provides the architecture of the model and can be seen as the foundation of the entire artifact. Becker et al. distinguish two basic approaches: a one-dimensional sequence of discrete steps

and a multi-dimensional maturity assessment. The dimensions are to be equated with the domain term introduced earlier. Several domains should be used if the object at hand is complex and/or new, which is the case here. Given the characteristics of CC, a multi-dimensional or multi domain approach seems most adequate, leading to guideline G2 (design level). Following the basic design level, "[...] the individual dimensions and their attributes must be devised to flesh out the model architecture" (Becker et al., 2009). There are several domains that the existing CCMMs agree upon (despite differences in the terminology) and based on the comparison, the literature review in chapter 2 and CCMM adjacent models (e.g. SOA, SaaS or IT Outsourcing MMs), maturity domains are now proposed. In addition to the theoretical side of the input, a group of CC experts from the authors' university validated the results of the domains and of maturity levels through an intensive discussion session. Table 2 shows the proposed domains:

Organisational	D1 (Governance): Capabilities necessary for an organisation's governance structure, processes and best practices including auditing capabilities, legal compliance, SLA management, data storage compliance, auditing and management policies, etc..
	Sources: Kolovuo (2009), Guo, Song and Song (2010), Martens et al. (2011), Verma et al. (2011), Oracle (2012), Oakton (2012)
	D2 (Security): Capabilities necessary to guard an organisation's security and privacy. The main goal is to ensure internal and external security and privacy of ones data. CC intensifies security problems through its characteristics and represents, together with governance issues, a dominant concern in CC.
	Sources: Koehler et al. (2010), Bisong and Rahman (2011), Martens et al. (2011), Badger, Grance, Patt-Corner and Voas (2012), Oakton (2012), Qaisar and Khawaja (2012)
	D3 (Organisational Readiness): Capabilities ensuring an unobstructed adoption of CC, including organisational aspects (e.g. change management, information management, organisational skill development) and employee related aspects (e.g. motivation, information, awareness).
	Sources: Pöppelbuß and Röglinger (2011), Oracle (2012)
	D4 (Processes): Capabilities necessary for the establishment of a CC process oriented IT, including process management, business process reengineering and focus on defining, optimising and documenting CC processes within the entire organisation.
	Sources: Oracle (2012), OnX (2012), Oakton (2012)
Technological	D5 (IT Infrastructure): Scope of CC related infrastructure, including standardised IT devices, thin clients, consolidation and virtualisation, shared services, fast network connections, SAN, etc. in order to support CC adoption. In addition, characteristics such as alignment of IT and business as well as IT architectural issues are included in this domain.
	Sources: Kolovuo (2009), Martens et al. (2011), Oracle (2012), Oakton (2012)
	D6 (Operational IT management): Capabilities necessary for managing deployment and post deployment of CC, include similar capabilities like D1 such as change management but also technology management, service portfolio management, innovation management and in general capabilities that ensure the efficiency and effectiveness of the CC services on the operational level.
	Sources: Oracle (2012), OnX (2012)

Table 2: Overview of the proposed maturity domains

The domains have been categorised into technological and organisational domains and the table shows the sources that either directly or indirectly support the proposed domains in the CC context. In sub-phase 3 the maturity levels will be proposed and consequently criteria for the levels will also be proposed, thereby giving the domains more substance.

The last step is to determine the actual architecture of the model. The CMMI-family approach is the most popular and used MM approach that exists at the moment (Mettler et al., 2010). It has been used for several decades, adapting to new requirements and building a steadily growing user base. The approach is sophisticated and shows a lot of documentation and the widespread application indicates its popularity amongst practitioners and researchers. Additionally, the underlying structure can be used in this context and leads to a continuous assessment and improvement cycle, resulting in guideline G4 (model approach).

Sub-phase 2: Select approach

Phase 4.2 is the first sub-phase to incorporate requirement R4, research methods have to be chosen in order to fill the potential CCMM with more content. Becker et al. indicate that the most popular research method is a literature analysis and suggest that explorative methods are also suitable. The methods chosen here have a large influence on the next sub-phase. The research methods are hereby not preclusive, meaning that they can and ideally should be combined. A literature analyses represents an excellent knowledge foundation and additive, explorative methods can fill the possible gaps that exist in the literature and leads to guideline G5 (approach selection).

Sub-phase 3: Design model section

Based on the CMMI-like structure, there are five maturity levels. In this case, the first level in the proposed maturity levels will also integrate cases of non-existing CC in organisations, which need to be accounted for. The CMMI model differentiates between two approaches for the progress in maturity levels, the staged (every domain has to be categorised into the same level for the organisation to advance to that level) and the continuous (maturity is determined through the advancement of the processes within a domain) approach. The staged approach was chosen here, its broader focus on each domain and the consequential need to improve the capabilities in every single domain is more suitable in the given situation. This may change in the future when CC has developed the granularity necessary for a comprehensive continuous approach but at this point the staged approach is more appropriate, leading to guideline G6 (mode approach). Before introducing the actual maturity levels, the purpose objective has to be determined, i.e. whether the MM should primarily be descriptive, prescriptive or comparative. The line of thought presented so far suggests a mainly descriptive model, enabling organisations to assess their individual status quo of CC usage. Additionally, several recommendations for organisations willing to advance in their CC maturity will be suggested, therefore resulting in a primarily descriptive model with prescriptive elements.

Ultimately, the goal for organisation using the CCMM is to advance in CC maturity to the desired level. In order to do that there have to be CC specific criteria and characteristics inherent to the maturity levels that describe the progressing maturity. CC maturity is a complex issue that is in need of holistic research and discussion, which cannot be conducted in this paper alone. However, one can make several assumptions and limitations that (combined with maturity domains and levels) enable a viable choice of criteria. First, it is assumed that the five NIST characteristics are always fulfilled as opposed to act as measure of maturity. This ensures a broader applicability and a CC focus as well as that the individual features do not need to be assessed for every maturity level. Second, the service models will not be coupled with maturity. Whether SaaS, PaaS or IaaS is used does not have a direct correlation to the overall maturity of CC usage in an organisation, the service models can therefore not serve as an indicator for CC maturity. Third, the same holds true for the deployment models, the usage of a more complex deployment model does not automatically indicate a higher maturity. Taking all this into consideration, the level descriptions that follow now propose suitable guiding criteria that allow for a categorisation of organisation's CC maturity.

At Level 1 (initial), CC usage is characterised by its informality and lack of organisational knowledge, it can be seen as a bottom-up approach. CC usage resembles "shadow IT", it is mainly used by individuals (or teams) who personally chose CC services over regular services without the clear knowledge of the organisation about the actual usage (e.g. someone buying Salesforce services with own credit card). Since there is little organisational knowledge about the usage, it cannot be adequately controlled and supported by the organisational IT. Therefore there is no CC related governance or security management, the regular principles of operation are extended to CC services by the users themselves. The "shadow services" are accessed through the existing IT infrastructure, CC is not embedded in the process flow and the main driver behind the usage is the personal motivation of the users. At the organisational level, CC usage is practically non-existent and is not supported due to a lack of knowledge or hesitance by top management. The authors suggest three scenarios that can take place at this level that significantly shape the progress of CC in an

organisation: the usage of CC can either be blocked (i.e. top management forbids the further usage), tolerated (employees are allowed to choose) or supported (CC usage is actively encouraged). An interesting case would emerge if management blocked CC usage while users increasingly use CC but this scenario cannot be dissected here at length and has to be discussed by future research.

Assuming one of the last two scenarios, Level 2 (assessing) is shaped by the start of organisational attention of CC due to the experiences made at the individual level. It now shifts to a top-down approach; the management is involved and introduces rules of action. The (good) experiences are one of the main drivers of CC adoption, in addition to cost reduction, flexibility and the fast deployment of services that CC offers (i.e. the benefits of CC). CC services become a component in the IT and are perceived in the organisation. There is knowledge about where and to what extent CC is used in processes within the organisation. Nonetheless, isolated solutions still exist and the organisation is faced with CC inherent issues (e.g. data integration, inter-operability, location of physical data) that need to be addressed by governance and security management. First CC related security measures such as identity management or data transmission protection integration are put into place. IT infrastructure is assessed and it is determined which necessary steps need to be taken in order to adequately integrate CC in the future. Level 2 is characterised by the start of knowledge acquisition, the organisation assesses its CC possibilities, CC providers are identified, knowledge regarding CC and its features is obtained.

Organisations that can be categorised into level 3 (determined) actively choose to adopt CC services. Based on the knowledge acquired in level 2 and as the experiences with CC increases, the organisation becomes more aware of inherent risks, advantages and opportunities. In accordance with the top-down approach, CC is tested in departments or teams. Governance regulations are determined that deal with the occurring concerns of CC usage (e.g. data location, data storage, SLA management) and responsibilities and competencies are appointed. As literature and practice have shown, especially risk and compliance management should be in the focus of the first governance steps. CC security management creates custom security measures (e.g. organisational interfaces, emergency plans) that are necessary for organisational CC usage. The focus starts to shifts from the protection of risks such as identity management, access control and firewall rules to more advanced concerns including data segregation, resource sharing or economies of failure. IT infrastructure is adopted in relation to CC needs (e.g. thin clients, fast and reliable Internet connection, redundant infrastructure). Business and IT architecture alignment is analysed, the organisation is becoming aware of issues involving organisational CC adoption, including interoperability, standardised interfaces and centralised services. IT infrastructure is adapted to enable CC. Processes involving CC are equal to regular processes and actively encouraged. Furthermore, a comparison is enabled and existing processes are examined regarding their Cloud potential. Information about CC providers is acquired and a multi-vendor strategy is pursued. Additionally, that leads to CC concerns being addressed such as data lock-in or economy of failure. Employees are receiving CC training and even though the majority of CC services are still purchased, internal solutions start to surface.

Maturity level 4 (managed) represents the definitive transition from testing scenarios to a controlled and more standardised, i.e. managed state. The main focus is to roll out CC usage organisation-wide. Therefore, issues such as integration, standardisation and comprehensive usage are the main focus. Governance policies are implemented for the whole organisation, auditing of CC services is enabled. Similar to IT Outsourcing, governance focus start to shift towards supplier relationship management. Security management is fully aware of CC inherent risks and has identified and determined accordingly measures to ensure a safe usage of CC service within the entire organisation. Security is increasingly automated and organisational focus now lies on uninterrupted service, finally shifting from technical risks to more substantial risks as CC is expanded into more strategically significant business areas. CC services represent the standard option and business processes are increasingly optimised through CC (e.g. team collaboration, data back up, online presence, resource provision). Top management and employees are actively pursuing further CC adoption and standardisation, motivated to increase efficiency, flexibility and innovation. The majority of the existing IT

infrastructure is altered to fit the requirements of CC (e.g. client devices and laptops, virtualisation) and procurement acts in accordance with the organisational goals. The organisation starts to develop best practices. Multiple providers are used and the organisation attempts to implement interoperability and data-integration to prevent data lock-in. SLA management is put into place to deal with the occurring issues of organisation wide CC usage including availability and uptime, data backup and recovery and fast scalability.

The final level of CC maturity has to be seen as an anticipation of the CC progress. An organisation with maturity level 5 (optimised) has re-engineered the suitable processes according to CC and new processes are automatically analysed for CC potential and development. Governance has shifted towards supplier relationship management issues, SLAs are customised to the organisations needs and fully automated, best practices are developed within the organisation and serve as guidelines for other organisations. The security provided by the CC providers is monitored and benchmarked, the internal computing environment is optimised regarding CC usage. Additionally, the processes are continuously monitored and evaluated. IT infrastructure consists completely of devices that enable easy CC usage, the architecture is fully aligned with business architecture, full interoperability between multiple providers exists. Internal and custom CC solutions can now be developed by the organisation and full performance management of internal and procured solution is enabled for provider evaluations.

Summarised in table 3, these descriptions illustrate the exemplary and evolutionary path an organisation follows when adopting CC services. Currently, as pointed out by a recent study (ISACA, 2012), it is safe to assume that only a small number of organisations may be able to reach level 5 (or even level 4). It is therefore difficult to suggest more tangible content for the higher levels, the experiences made in practise in the future will significantly shape the requirements of CC maturity. Nonetheless, it is important that organisations have a vision and an ultimate goal that can be reached, which is provided by the CCMM. Guideline G7 (maturity levels) is the product of these considerations.

Level \ Domain		Governance	Security	Organisational Readiness	Processes	IT Infrastructure	Operational IT management
Level 1: Initial	Description	No CC-related governance; existing structures are used informally	No CC-related security management; existing structures are used informally	Only individual CC readiness; shadow IT	No organisational CC processes	Regular IT infrastructure is used	Informal, self-regulated management due to CC as shadow IT
	Effects	The bottom-up usage as shadow IT introduces risks that are not covered by the organisation while the benefits of CC cannot unfold its potential.					
	Recommendation	Formalisation of CC usage; addressing of issues by management.					
Level 2: Assessing	Description	Awareness of CC inherent governance issues (e.g. jurisdictional compliance, SLA management) and assessment of existing structures	Integration of current CC usage into security management and introduction of basic CC-related measures (e.g. identity management, data access rules)	Organisational awareness of CC usage; motivation to adopt CC; willingness to change; assessment of organisational CC capabilities and necessities; knowledge acquisition	Knowledge about CC usage in existing processes	Assessment of existing infrastructure with regard to CC; identification of IT organisation's alignment with business	Assessment and integration of current CC usage; cost-benefit analysis; knowledge acquisition; identification of suitable CC providers; organisational and market status quo of CC is assessed
	Effects	Bottom-up shifts to top-down; organisational knowledge about CC usage exists; security and governance are adapted; organisational and market status quo of CC is assessed.					
	Recommendation	Active management involvement; increased CC usage and organisational learning; creation of CC-related structures and architecture; implementation of governance and security measures.					
Level 3: Determined	Description	Determination of responsibilities & competencies; risk & compliance management are introduced (e.g. jurisdictional compliance, data ownership); authentication & authorisation	Custom CC measures (e.g. emergency plans, data segregation, disaster recovery) are introduced through security management; contractual protection responsibilities are determined; provider security is analysed and compared	Active management support; resources are provided; change management is introduced; CC related employee trainings; communication of CC strategy, benefits & risks; determination of roll out strategy in cooperation with operational IT management	Comparison of CC vs. regular processes; CC processes are defined; potential CC involvement in additional processes is analysed	Adoption of basic CC-related infrastructure (e.g. client devices, SAN); determination of infrastructure needs to further implement CC	Providers are compared; multi-vendor strategy is considered; IT procurement is analysed with regard to CC; CC experiences are documented and processed; determination of outsourceable services and transition plans
	Effects	Organisational CC experiences are made through testing scenarios; CC awareness is created; management support ensures implementation; basis for further deployment is created; incremental improvements are triggered.					
	Recommendation	Definition of enterprise architecture and IT strategy; top-management support; clarification of responsibilities and competencies; application of test scenario in additional divisions or teams; implementation of CC-related organisational learning.					
Level 4: Managed	Description	Auditing of CC usage; policy & service management (e.g. data policies) are introduced; organisation-wide adoption of CC governance; failure insurance is acquired	Internal computing security environment is optimised regarding CC; provider security is negotiated; due diligence is performed; security management standards are developed	Full top-management support; changes in organisational culture; full information sharing; organisation-wide change management; communication of changes; integration of CC services	CC processes are defined, standardised documented; strategically more significant process are supported	Beginning of organisation-wide adoption of CC-related infrastructure, access network is adapted (e.g. bandwidth, ubiquity)	Multi-vendor strategy; IT procurement is executed in accordance to CC needs; determination of CC-related IT strategy; focus on interoperability and automation
	Effects	CC is used organisation-wide; top-down approach is implemented; increased alignment of IT and business structures; CC benefits begin to unfold their potential; governance and security can keep up with the risks of CC; increased CC reliability; increased employee collaboration.					
	Recommendation	Full organisational integration; focus continuous monitoring and benchmarking; increased standardisation efforts; shift to supplier relationship management.					
Level 5: Optimised	Description	Supplier relationship management; customised & automated SLAs; focus on continuous monitoring and evaluation	Provider security is monitored and benchmarked; security audits exist; secure internal CC environment complements external security; proactive security management	Best cases and practices are developed and exported; full organisational learning structures exist; CC culture; continuous employee training; regular assessment and review of requirement	Business process reengineering of suitable process, fully defined, standardised and repeatable CC processes	Full CC infrastructure adoption and standardisation; business-driven alignment of IT and business architecture;	Performance management is implemented; full interoperability; self-service; centralised services; continuous market research; provider benchmarking
	Effects	Optimisation of CC usage; full perception of CC benefits, minimisation of CC risks and threats; continuous monitoring and evaluation of CC usage					
	Recommendation	Perpetual optimisation efforts through monitoring and external benchmarking; cooperation with industry partners, researchers and developers; induce strong and lasting partnerships with providers;					

Table 3: Cloud Computing Maturity Model

Sub-phase 4: Test results

Despite sub-phase 4 not being carried out in this contribution, it is still necessary to shortly address the issue of testing and evaluating. This sub-phase is based on the requirement R3 and incorporates a testing and evaluation of the findings. The evaluation of the findings contains three options: full approval of the model, approval of the findings but the need for a further iteration or the rejection of

the model. The circle of evaluators should be steadily increased to ensure full validity, consistency and problem adequacy. Only vigorous testing by practitioners and researchers can fully validate the findings, leading to the formulation of guideline G8 (test results). The evaluation of the findings of this contribution will be carried out in further publications. The last part of the procedure model consists of the transfer and evaluation of the MM, two aspects that are also of significance but are not discussed in this paper for reasons explained earlier

5 CONCLUSION

This contribution has shown the need for CC management aids and tools and has provided the first steps towards a CCMM to fill the gap. Guidelines for the development of a CCMM were proposed that act as a broad framework for future users of MM procedure models but leave enough decision space for adjustments. Six domains were derived that are divided into organisational and technological capabilities thereby holistically addressing the current needs for CC adoption. The five maturity levels describe the capacity in which said capabilities are performed and act as an indicator for improvement. Assumptions regarding CC maturity were made to address the issue, e.g. service and deployment models as well, the NIST characteristics were left out of the CC maturity term in order to allow for a broad application and a strong CC focus.

There are theoretical and practical implications that this paper offers. Firstly, the literature review and the executed procedure model have shown that there are still many research gaps for future research to close including how (or if) to adequately integrate service and deployment models into a CCMM or what transfer and evaluation methods are best suited for a CCMM. Additionally, despite recent findings (a study found 80% of respondents to be maturing or close to maturity in cloud adoption (Capgemini, 2012)) the authors believe that CC maturity research needs to further mature and especially practice-related research has to provide information to fill in more specifics of CC maturity. Secondly, the research has shown that the field of CCMMs in particular is in need of a MM that fully follows scientific models. This has partially been provided by this contribution but requires more research and validation. Thirdly, the development guidelines have direct and practical implications, as do the proposed domains and maturity levels. They are based on current research and the current needs of organisations that are adopting CC and express cloud maturity accordingly. Organisations can thereby assess and ultimately improve their CC capabilities. Additionally, future researchers can build on the research presented and transfer adequate content.

Naturally, there are limitations to this contribution. First, the proposed content and guidelines were not evaluated by outside groups, leaving it to future research to validate the findings. The procedure model requires thorough evaluation for reasons of validity, plausibility and usability. Secondly, the research is mainly based on recent academic publications in major journals and conferences and certain keywords were used for the search, possibly limiting the research outcome.

Concluding, one can safely say that CCMMs will soon advance to the same importance as many of their predecessors in other fields but are still in need for extensive future research. Especially conclusions from the practical application of CC in organisations need to be integrated into such models in order to fill and specify the cloud maturity term and substantiate the proposed content and structure. However, this contribution can be seen as the first step towards a service-consumer CCMM and thereby aid organisations, in particular in implementing CC and ideally serve as a basis for future models.

References

Anstett, T., Karastoyanova, D., Leymann, F., Mietzner, R., Monakova, G., Schleicher, D. and Strauch, S. (2009). MC-Cube: Mastering Customizable Compliance in the Cloud. *Service-Oriented Computing: Lecture Notes in Computer Science*, 5900, 592-606.

Badger, M.L., Grance, T., Patt-Corner, R. and Voas, J.M. (2012). NIST Cloud Computing Synopsis and Recommendations. Retrieved June 27th, 2012, from http://www.nist.gov/.

Becker, J., Knackstedt, R. and Pöppelbuß, J. (2009). Developing Maturity Models for IT Management – a Procedure Model and its Application. *Business & Information Systems Engineering,* 1, 213-222.

Bender, D. (2012). Privacy and Security Issues in Cloud Computing. *The Computer & Internet Lawyer*, 29 (10), 1-15.

Bisong, A. and Rahman, S. M. (2010). An Overview of the Security Concerns in Enterprise Cloud Computing. *International Journal of Network Security & Its Applications*, 3 (1), 30 – 45.

Capgemini. (2012). Business Cloud: The State of Play Shifts Rapidly: Retrieved February 3rd 2013 from http://www.capgemini.com/insights-and-resources/by-publication/business-cloud-the-state-of-play-shifts-rapidly/.

Che, J., Duan, Y., Zhang, T. and Fan, J. (2011). Study on the Security Models and Strategies of Cloud Computing. *Procedia Engineering* 23, 586- 593.

Computing Technology Solutions. (2012). Cloud Maturity. Retrieved April 25th, 2012, from http://cloudmaturity.com/.

Conway, G. & Curry, E. (2012). Managing Cloud Computing: A Life Cycle Approach. Retrieved February 10th 2013 from http://edwardcurry.org/#60e/custom_plain.

Crosby, P. B. (1979). Quality is Free. McGraw Hill, New York.

De Bruin, T., Rosemann, M., Freeze, R. and Kulkarni, U. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. *Proceedings of the Australasian Conference on Information Systems (ACIS),* paper 109, available at http://aisel.aisnet.org/acis2005/109.

Dillon, T., Wu, C. and Chang, E. (2010). Cloud Computing: Issues and Challenges. *24th IEEE International Conference on Advanced Information Networking and Applications,* 27-33, IEEE press, Perth, Australia.

Gartner. (2012). Gartner Outlines Five Cloud Computing Trends That Will Affect Cloud Computing Strategy Through 2015. Retrieved May 29th 2012, from http://www.gartner.com/it/page.jsp?id=1971515.

GTSI. (2012). Cloud Computing White Paper. Retrieved April 24th 2012, from www.gtsi.com/cms/documents/White-Papers/Cloud-Computing.pdf.

Guo, Z.; Song, M. and Song, J. (2010). A Governance Model for Cloud Computing. *International Conference on Management and Service Science,* 1-6, Beijing, China.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly,* 28, 1-49.

ISACA. 2012. Cloud Computing Market Maturity Study Results, retrieved February 5th, 2013from www.isaca.org.

Koehler, P., Anandasivam, A. and Dan, M.A. (2010). Cloud Services from a Consumer Perspective. *Proceedings of the Americas Conference on Information Systems (AMCIS),* paper 329, available at http://aisel.aisnet.org/amcis2010/329.

Kolovuo, V. (2009). Junction of the iSOAMM Maturity Model for SOA with the Evaluation Framework CloudTCO for Cloud Computing Offerings. Master thesis at University Karlsruhe.

Martens, B. and Teuteberg, F. (2011). Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model. *AMCIS Proceedings,* Detroit, Michigan.

Martens, B., Poeppelbuss, J. and Teuteberg, F. (2011). Understanding the Cloud Computing Ecosystem: Results from a Quantitative Content Analysis. *Wirtschaftsinformatik Proceedings*, Zurich, Switzerland.

Martens, B., Teuteberg, F. and Gräuler, M. (2011). Design and Implementation of a Community Platform for the Evaluation and Selection of Cloud Computing Services: A Market Analyses. *Proceedings of the European Conference on Information Systems (ECIS)*, Helsinki, Finland.

Maslow, A. (1954). Motivation and Personality. Harper, New York.

Mettler, T. Rohner, P. and Winter, R. (2010). Towards a Classification of Maturity Models in Information Systems. D'Atri, A., De Marco, M., Braccini, A.M., Cabiddu, F. (eds.) *Management of the Interconnected World*, 333-340. Physica-Verlag, Heidelberg (2010).

Nolan, R. L. (1979). Managing the Crises in Data Processing. *Harvard Business Review,* 57, 115-126.

Nuseibeh, H. (2011). Adoption of Cloud Computing in Organizations. *AMCIS Proceedings*, Detroit, Michigan.

Oakton. (2012). Cloud Organisational Maturity White Paper. Retrieved April 24th 2012 from www.oakton.com.au.

OnX. (2012). The Federated Cloud Maturity Model – Charting the Path to Cloud Computing. Retrieved May 3rd 2012 from http://www.onx.com/singlecolumncontent.aspx?id=226.

Oracle. (2012). Cloud Computing Maturity Model – Guiding Success with Cloud Capabilities. Retrieved April 23rd 2012 from www.oracle.com.

Pöppelbuß, J. and Röglinger, M. (2011). What Makes a Useful Maturity Model? A Framework of General Design Principles for Maturity Models and its Demonstration in Business Process Management. *ECIS Proceedings*, Helsinki, Finland.

Qaisar, S. and Khawaja, K. F. (2012). Cloud Computing: Network/Security Threats and Countermeasures. *Interdisciplinary Journal of Contemporary Research in Business,* 3 (9), 1323-1329.

Repschläger, J., Hahn, C. and Zarnekow, R. (2012). Handlungsfelder im Cloud Computing: Relevanz und Reifegrade des Cloud Computings in typischen Prozessphasen. Forschungsumfrage, IT Operations Day, 2012.

Sarkar, P. and Young, L. (2011). Sailing the Cloud: A Case Study of Perceptions and Changing Roles in an Australian University. *ECIS Proceedings,* Helsinki, Finland.

Sorofman, J. (2012). The Cloud Computing Adoption Model. Retrieved May 4th 2012, from http://www.drdobbs.com/web-development/the-cloud-computing-adoption-model/211201818.

Urguhart, J. (2012). A Maturity Model for Cloud Computing. Retrieved May 3rd 2012 from http://news.cnet.com/8301-19413_3-10122295-240.html.

Venable, J.R. (2010). Design Science Research Post Hevner et al.: Criteria, Standards, Guidelines, and Expectations. *Proceedings of the Design Science Research in Information Systems and Technology (DESRIST),* St. Gallen, Switzerland.

Verma, M., Amardeep, S. and Vandana, S.K. (2011). A Sight into Cloud Computing. *International Journal of Computer Science and Technology,* 2, 65-68.

Webster, J. and Watson, R.T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly,* 26, 13-23.

Yang, H. and Tate, M. (2009). Where are we at with Cloud Computing? A Descriptive Literature Review. *ACIS Proceedings*, Melbourne, Australia.

Appendix 1: Comparative overview of existing Cloud Computing Maturity Models

Model (Source)	R1: Comparison with existing maturity models	R2: Iterative procedure	R3: Evaluation	R4: Multi-methodological procedure	R5: Identification of problem relevance	R6: Problem definition	R7: Targeted presentation of results	R8: Scientific documentation
Indepen dent CCMM (Kolovuo 2009)	Reference to maturity model proposed by Urquhart	No apparent iterations	Expert Interviews	Literature review on Cloud Computing and SOA	Immaturity of Cloud Computing concept and inexperience of organisations	iCCMM as an assessment tool and aid to Cloud Computing adoption	Thesis chapter (10 pages), online questionnaire. Description of model	Description of model, no description of development process
Cloud Computing Service Maturity Model (Martens et al. 2011)	Single reference to the model proposed by GTSI	Becker et al. procedure model	Expert interviews	Literature review	Quality of Cloud Computing Services can only be assessed through intense research	The model as an aid to assess service quality without intense research	Online database, 2 pages research-in-progress paper	Description of model, mentioning of the design process (Becker et al. (2009))
CMM for Cloud Computing (Verma et al. 2011)	None	No apparent iterations	No apparent evaluation	No apparent methods	Organisation have the need to evolve their capabilities	None	2 pages in a journal publication	Description of model, no description of development process
Cloud Maturity Model (Oracle 2012)	None	No apparent iterations	No apparent evaluation	Based on best practises	Technologies require substantial effort to adopt do to the impact, breadth, and complexity of the changes required for successful adoption	The model as a consistent, structured way to define and measure the progress of Cloud Computing	2 White papers (10 & 13 pages)	Partial description of model, description of domains, no description of development process
Cloud Computing Maturity Model (OnX 2012)	None	No apparent iterations	No apparent evaluation	Summary of the NIST definition and benefits and risks	Successful implementation of cloud environments	None	6 paged White Paper	Only description of model, no description of development process
Federated Cloud Maturity Model (Oakton 2012)	None	No apparent iterations	No apparent evaluation	No apparent methods	Fundamental lack of common understanding among both IT and business professionals on the components which make up cloud computing	Model as aid to provide clarity on what technology and business components make up cloud computing, and how the journey to cloud computing follows a logical progression	8 paged White Paper	Only description of model, no description of development process
Cloud Maturity Model (GTSI 2012)	None	No apparent iterations	No apparent evaluation	No apparent methods	Help senior IT professionals understand where their organisation stands with regard to cloud readiness	Model can be used to assess an organisation's level of maturity against a particular dimension of its business	19 paged White Paper	Description of model and domains, no description of development process
Cloud Advancement Model (Cloud maturity 2012)	No documentation	No documentation	No documentation	No documentation	No documentation	The model as an assessment, advancement and benchmark tool.	2 pages on the company website	No documentation
Maturity model for Cloud Computing (Urguhart 2012)	None	No apparent iterations	No apparent evaluation	No apparent methods	"Moving into the cloud" as a complex and uncertain process	Model as an aid for organisation to move into the cloud	2 pages Blog entry	Description of model and characteristics, no apparent development process involved
Cloud Computing Adoption Model (Sorofman 2012)	Reference to the CMM	No apparent iterations	No apparent evaluation	No apparent methods	Cloud Computing is a "game changer" that requires organisations to react to change	Model as an aid to a graduated, stepwise approach for the adoption of cloud technologies	2 pages Blog entry	Description of model and characteristics, no apparent development process involved