

Adopting the Cloud

A multi-method approach towards developing a cloud maturity model

F. W. van Dijk

Friso Willem (F.W.) van Dijk: *Adopting the Cloud: A multi-method approach towards developing a cloud maturity model*
Master Business Information Technology, Final Project

Supervisors

Prof. Dr. Jos van Hillegersberg (*Faculty of BMS, Universiteit Twente*)
Dr. M. Daneva (*Faculty of EEMCS, Universiteit Twente*)
M. Chin (*Director Sourcing & IT Governance, METRI*)

Location

Universiteit Twente, Enschede

Summary

Context

While there is abundant scientific literature on cloud computing, very little of it focuses on the challenge of adopting this new technology in organisations. Additionally, few guidelines and best practices exist to help practitioners evaluate organisational capabilities and assess and improve cloud readiness. While the benefits of cloud computing become increasingly clear, an increasing number of organisations is looking to adopt the technology. This development calls for a model supporting these organisations in their endeavour to adopt cloud computing.

This research aims to fill this gap in scientific literature by creating a cloud computing maturity model. This is accomplished by identifying the required capabilities for cloud adoption and placing them on a maturity scale.

Results

During the literature review, existing cloud maturity models were evaluated with a framework developed based on scientific rigour and the benefits and challenges of cloud computing. Seven models were identified in a literature study comprising of both scientific and grey literature, which were all deemed inadequate in some form. Thus, the decision was made to develop a new cloud maturity model.

The model created in this thesis research was developed with a Delphi study, in which 14 experts on cloud computing were consulted on cloud computing in multiple questionnaire rounds. The expert group was diverse in nature, including from both cloud consumers and providers, as well as consultants and academics. This was supplemented with a literature study, taking inspiration from existing maturity models and applying it to the domain of cloud computing. This resulted in a model comprised of 14 focus areas in four dimensions, each of these focus areas containing multiple statements for each of the five maturity levels.

Application

The model is intended to be a tool for IT management to support their cloud adoption. The process by which is applied was developed in collaboration with METRI in order to leverage their cloud expertise. This process consists of four stages.

1. Relevant managers fill out the assessment.
2. Consultant discusses assessment results with each person who completed it in order to validate the results.
3. Consultant aggregates assessment results.
4. Consultant presents the organisation's strong and weak points with regard to cloud computing, with advise for improvement.

Validation

The model was validated through follow-up interviews with two of the participants in the Delphi study and through two case studies. The interviews validated the final stage of the model, whereas the case studies show the applicability of the model in a practical setting.

Conclusions

The most important result is the cloud maturity model itself, as it presents a broad and inclusive view of the organisational capabilities required for cloud computing. The model incorporates a broad spectrum of organisational areas affected by cloud computing.

The second contribution is the framework for assessing cloud maturity models. This framework has been established to assess existing cloud maturity models and was used to develop the cloud maturity model developed in thesis.

The third contribution is the elicitation of several organisational areas affected by cloud computing that were previously not mentioned in scientific literature in the context of cloud adoption: IT strategy, IT governance, Enterprise Architecture and Business Process Management.

Acknowledgements

Oftentimes, we see a quote and project our lives or our work on those letters. Some part of a text taken out of its context and reduced to a framework on which you project your life. I believe models can do the same. They present to us an image that gives a common and relatable framework for communication on complex topics. With that in mind, I decided I wanted to work on a model for my master thesis. The document before you shows that I succeeded in doing so, although it is my effort alone.

I would like to thank everyone at METRI for providing their cooperation and an energetic environment to help me in my research. In specific, I would like to thank Paul Cornelisse for his guidance during the initial stages, Sytse van der Schaaf for his patience and advice during the drawn-out parts of the study. And last but not least, I would like to thank Michael Chin for his tutelage and guidance during the whole project, teaching lessons in IT governance and everything surrounding business.

From the Universiteit Twente, I was supported by two supervisors who were always ready to answer my questions in our regular sessions or over email. Thank you Jos van Hillegersberg for your advice on process and the numerous suggested papers. Thank you Maya Daneva for your advice on procedure and your critical view on my discussion chapter.

I would also like to thank those outside of METRI and the Universiteit Twente who stood by me through it all and helped with proofreading this document. You know who you are.

And finally, I would like to thank Davida Flinsenbergh for her patience and aid during the moments where I felt like the king of Ephyra. Thank you for being there and thank you for saying yes.

Friso van Dijk

Contents

1. Introduction.....	1
1.1 Research Problem.....	1
1.2 Research Questions.....	3
1.3 Research Methodology.....	3
1.4 Thesis Structure.....	4
2 Background.....	6
2.1 Cloud Computing	6
2.1.1 Defining Cloud Computing	6
2.1.2 Benefits of Cloud Computing	9
2.1.3 Challenges of Cloud Computing	11
2.2 Maturity Models.....	12
2.2.1 Displaying Maturity in Maturity Models.....	13
2.2.2 Maturity Model Development.....	14
2.2.3 Maturity Measurement	17
3 Comparing Cloud Maturity Models.....	18
3.1 Identifying Cloud Maturity Models	18
3.1.1 Filtering the Results.....	18
3.1.2 Expanding on Scientific Literature.....	19
3.2 Identified Cloud Maturity Models.....	19
3.2.1 Duarte Cloud Maturity Model.....	20
3.2.2 Weiss Cloud Computing Maturity Model.....	21
3.2.3 Cloud Maturity Model 3.0.....	21
3.2.4 AWS Cloud Transformation Maturity Model.....	22
3.2.5 Forrester Model for Cloud Maturity	24
3.2.6 Cloud Computing Maturity Model	24
3.2.7 Cloud Adoption Model for Governments and Large Enterprises.....	25
3.3 Assessment of Identified Cloud Maturity Models	26
3.3.1 Assessment Elements from Literature	27
3.3.2 Mapping the Maturity Models on the Identified Elements	28
3.4 Discussion of Assessments	31
3.4.1 Duarte CMM	31
3.4.2 Weiss CCMM.....	31

3.4.3 CMM3	32
3.4.4 AWS CTMM	32
3.4.5 Forrester MCM.....	32
3.4.6 CCMM	33
3.4.7 CAM.....	33
3.5 Conclusion.....	34
4 Delphi Study	36
4.1 Delphi Study	36
4.1.1 Delphi Study	36
4.1.2 Delphi Study Design.....	37
4.2 Conceptual Model.....	40
4.2.1 Expert Interview METRI Cloud9 Model.....	40
4.2.2 Conceptual Model	43
4.3 Delphi Round 1	47
4.3.1 The Split in Three Domains	47
4.3.2 Infrastructure Domain	48
4.3.3 Platform Domain	49
4.3.4 Software Domain.....	50
4.3.5 Revised Model.....	52
4.4 Delphi Round 2.....	53
4.4.1 Response on Round 1 Changes	53
4.4.2 Focus Area Brainstorm	54
4.4.3 Expanded Cloud Maturity Model	55
4.5 Delphi Round 3.....	69
4.6 Delphi Round 4.....	75
4.7 Reorganising the Cloud Maturity Model.....	75
4.8 Conclusion.....	77
5. Validation	78
5.1 Follow-up Interviews.....	78
5.1.1 First Interview	78
5.1.2 Second Interview.....	79
5.1.3 Interview Conclusions	79
5.2 Case Studies.....	80
5.2.1 Case Study Method.....	80

5.2.2 International Trade Organisation	80
5.2.3 Waste Collector.....	81
5.2.4 Case Study Conclusions	82
5.3 Conclusion.....	83
6. Discussion	84
6.1 Research Methodology Used.....	84
6.2 Cloud Maturity Model Reflection	84
6.3 Contribution to Research	85
6.4 Contribution to Practice.....	86
6.5 Research Limitations and Future Work	86
7. Conclusion.....	88
7.1 Prior Model Assessment	88
7.2 Cloud Maturity Model Development	89
7.3 Cloud Maturity Model Validation.....	90
7.4 Answering The Main Research Question	91
8. Bibliography.....	92
Appendix A	96
Appendix B	97
Appendix C	102
Appendix D	108
Appendix E.....	118
Appendix F.....	128

List of Figures

Figure 1 Benefits of cloud computing with maturity [14]	1
Figure 2 Challenges of cloud computing with maturity [14]	2
Figure 3 Cloud service and delivery models	7
Figure 4 Level of self-supplied/-managed resources for different service models [2].....	8
Figure 5 A focus area maturity model example [18].....	14
Figure 6 Duarte Cloud Maturity Model [1].....	20
Figure 7 First level of the Weiss Cloud Computing Maturity Model [42]	21
Figure 8 Example roadmap of the Cloud Maturity Model [43]	22
Figure 9 Amazon Web Services Cloud Transformation Maturity Model [44]	23
Figure 10 Forrester Model for Cloud Maturity [46].....	24
Figure 11 Cloud Computing Maturity Model [47]	25
Figure 12 Cloud Adoption Model for Governments and Large Enterprises [26].....	26
Figure 13 Viewing anonymous answers in Spilter	40
Figure 14 METRI Cloud9 model	41
Figure 15 Schematic of the model construction.....	44
Figure 16 CMM3 roadmap [54].....	44
Figure 17 First version cloud maturity model with inspirational dimensions.....	45
Figure 18 First version cloud maturity model	46
Figure 19 Infrastructure domain	48
Figure 20 Platform domain	49
Figure 21 Software Domain	50
Figure 22 Revised cloud maturity model	52
Figure 23 METRI's IT Organisational model with mapped focus areas	76
Figure 24 Assessment for vendor management level 1 through 3	76
Figure 25 Waste collector overall maturity	82
Figure 26 Revised cloud maturity model	89
Figure 27 METRI's IT Organisational model with mapped focus areas	90

List of Tables

Table 1 Relation between procedure model and document chapters	4
Table 2 Procedure model steps not in document	5
Table 3 Applicability of maturity model development methods: a comparison.....	16
Table 4 Number of papers per stage	19
Table 5 Comparison of cloud maturity models on identified elements	29
Table 6 Comparison of cloud maturity models on scientific rigour	30
Table 7 Delphi panel composition and participation per group	39
Table 8 Traceability matrix of capabilities and maturity levels.....	55
Table 9 Consolidating capability areas to focus areas	56

1. Introduction

This chapter introduces the research topic by first describing the research problem and associated research questions. This is followed by the research methodology and display the structure of this thesis according to the described methodology.

1.1 Research Problem

In the past few years, an upward trend in the adoption of cloud computing has been identified and the market is growing rapidly [3]. This can be attributed to the new model in the use of IT services, where computational resources and software are acquired and paid for as services through a network [4]. Several benefits can be identified in this approach. First, computing resources can be acquired on an as-needed basis [5, 6]. This shifts the operating model from capital expense to operating expense, with a smoother curve in the costs of adopting new IT solutions. In addition, this allows cloud providers to utilise a multi-tenant model, where multiple cloud consumers are using a shared set of resources, allowing economies of scale and an overall cost reduction [7].

This pay-per-use service model also allows organisations in becoming more agile, as they are relieved of maintaining a physical IT infrastructure and gain access to a low cost scalable platform [8]. This development supports organisations to focus on their core business processes, as the management of the physical infrastructure is handled by professionals on the cloud provider's side [9], and lets organisations innovate faster [6].

While these benefits create willing customers, cloud adoption comes with its own set of specific challenges, such as changing security requirements and the change in costing model [10-12]. The role of the IT organisation changes due to these new service models, shifting from a hands-on 'keeping it in the air' organisation to an organisation focused on managing different service providers through vendor management [11] and keeping the IT landscape in check with an increased importance on service integration and architecture [12, 13].

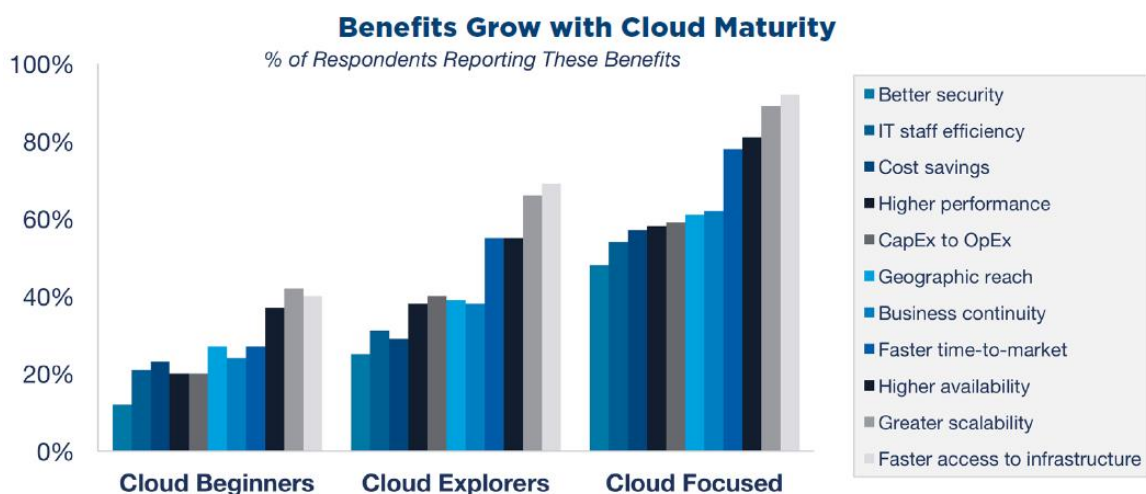


Figure 1 Benefits of cloud computing with maturity [14]

Despite these challenges, organisations are able to realise the benefits of adopting cloud computing and generally embrace the new technology. RightScale [14] shows two conclusions in its ‘State of the Cloud’ survey, performed among 1002 technical professionals of all organisational layers involved with cloud computing. They first show an increase in the benefits of cloud computing and, secondly, a decrease in the associated challenges as organisations become more mature in cloud use. This has been illustrated in Figure 1 and Figure 2 respectively. It shows a fairly linear growth in the benefits of cloud computing, but a more staggered decrease in challenges. This is due to the increase in complexity of the cloud services used when growing in maturity.

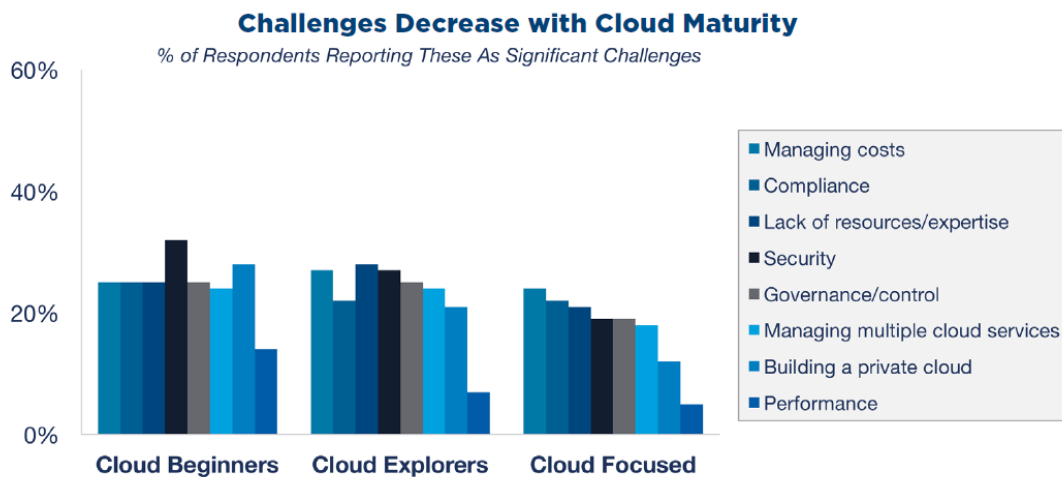


Figure 2 Challenges of cloud computing with maturity [14]

While many organisations are able to overcome these challenges, there appears to be a lack of systematic methods to review their business needs and to weigh the potential gains of adopting cloud computing against the challenges and risks [15].

In this light, METRI, the IT benchmarking and consulting firm instigating this research, identified that organisations are eager to adopt cloud computing, but are reliant on the guidance of their cloud providers in that process. There appears to be a lack of vendor-neutral management tools for self-assessment to support their capability planning and the creation of an adoption strategy.

To alleviate this issue, METRI attempted to create a staged model for cloud adoption, requesting the aid of the University of Twente to further develop their model with scientific grounding by identifying the underlying capabilities required for cloud adoption. These are characteristics of a maturity model, which give organisations the ability to assess their current state and to give them the means to transform their organisation towards their preferred end state [16]. With this question, the scope of this research is to develop or extend an internal cloud maturity model for IT management. This aims to fill the knowledge gaps brought forward by METRI and identified in literature.

1.2 Research Questions

The goal of this study is to create a cloud maturity model to address the lack of systematic means to review business needs regarding cloud computing. The following main research problem has been formulated to support this goal:

What constitutes a maturity model for cloud adoption that contains both the stages for cloud adoption and corresponding organisational capabilities?

The following subquestions were formulated in order to assess the current state of cloud maturity models and to identify whether already existing models could be used as a base for future development.

RQ1. Which cloud maturity models are available in current scientific literature?

RQ2. What does a model for assessment of cloud maturity models consist of?

Building on the previous research questions, the development of a cloud maturity model requires several key elements. The following subquestions have been created to identify these.

RQ3. Which stages of cloud adoption relate to each maturity level?

RQ4. Which factors need to be accounted for when assessing an organisation's cloud maturity?

RQ5. How can each of the maturity levels in a cloud maturity model be defined?

RQ6. How do the elements identified in literature relate to the maturity model?

These sub questions focus on the design of the maturity model, whereas applicability in practice is a further requirement. In order to validate the model adequately, it requires validation in a practical setting. The following subquestion has been established for this purpose.

RQ7. Do the model elements and requirements hold up in practice?

1.3 Research Methodology

Several methods for the development of maturity models exist [16-20]. Each of these methods is applicable to different types of maturity models, but they are similar in their process. The methods of De Bruin, Freeze, Kaulkarni and Rosemann [20] and Becker, Knackstedt and Pöppelbuss [16] are the two methods not limited to any specific type of maturity model, and can thus be considered to be general methods. All other methods are more specialised in their approach, focusing on either grid maturity models [17], focus area maturity models [18] or situational maturity models [19].

In selecting the method, the type of maturity model that best fits the research problem was an unknown factor. This led to the decision to use the method of Becker, Knackstedt and Pöppelbuss [16] for the present thesis. This method is an adaptation of the guidelines laid out in the Design Science Research Methodology [21] and builds upon the work done by De Bruin, Freeze, Kaulkarni and Rosemann [20]. It is applicable to all types of maturity models and thus lends itself well to the assessment and development of maturity models without specifying the type in advance.

Becker, Knackstedt and Pöppelbuss [16] noted a lack of scientific rigour in many maturity models, leading to sketchily documented maturity models in which “*The authors only rarely reveal their motivation and the development of the model, or their procedural method and the results of their evaluation*”. To combat the continuation of this trend they proposed a procedure model for the development of maturity models for IT management. This procedure model will be used in the present research.

The procedure model consists of seven steps:

1. *Problem definition*: During the problem definition phase, the targeted domain and the target group of the maturity model need to be determined. At the same time, the problem relevance must be clearly demonstrated.
2. *Comparison of existing maturity models*: A comprehensive comparison of existing maturity models is required for a reasoned determination of the design strategy.
3. *Determination of development strategy*: A documented decision needs to be made for the design strategy. The main design strategies are: construction of a completely new model, combination of several models into a new singular mode, and the transfer of structures or contents from existing models to a new context.
4. *Iterative maturity model development*: This is the central phase of the development process. It involves several iterations of four steps (select design level, select approach, design model section and test result), which at the highest level constitutes the model architecture, but is also applicable to specific model elements.
5. *Conception of transfer and evaluation*: The different forms of results communication for the academic and user communities need to be determined.
6. *Implementation of transfer data*: The maturity model should be made accessible to the planned target audiences through the forms decided upon in phase six.
7. *Evaluation*: The evaluation phase should establish whether the designed model provides the projected benefits and an improved solution for the problem. The outcome of this phase may cause another design iteration of one or more phases or a rejection of the model as a whole.

1.4 Thesis Structure

This research was conducted according to the procedure method of Becker, Knackstedt and Pöppelbuss [16]. Table 1 shows the relation between the steps of the procedure model and the document chapters.

Procedure model step	Chapter
1. Problem definition	1.1 Research problem
2. Comparison of existing maturity models	3 Comparison of cloud maturity models
3. Determination of development strategy	3.5 Comparison conclusions
4. Iterative maturity model development	4 Delphi study, 5 Validation

Table 1 Relation between procedure model and document chapters

This research aims to develop a tool and create the transfer data required for using the model. Due to the scope of this project, it was unfeasible to include all steps in the research. Table 2 displays the remaining steps in of the procedure model outside the scope of this document. The distinction between the validation chapter and the evaluation step is the scope of these segments. The validation is a test of the current model in practice, whereas the evaluation includes a broader scope, such as measuring the realised benefits against the projected benefits. This part falls outside of the scope of this research.

5. Conception of transfer and evaluation	Master thesis, whitepaper, assessment tool
6. Implementation of transfer data	
7. Evaluation	Not in research scope

Table 2 Procedure model steps not in document

2 Background

This chapter introduces the scientific background of the project and the definitions used in this document. First, cloud computing is introduced and defined, detailed with findings on its benefits and challenges. Secondly, types of maturity models, their conception and the development of maturity measurement instruments are detailed.

2.1 Cloud Computing

Cloud computing emerged in the early 2000s as a computing model where organisations or individuals obtain computing power and software solutions over the internet or other networks. It has been described as the fifth stage in the evolution of IT infrastructure models: the general purpose and minicomputer era; the personal computer era; the client/server era; the enterprise computing era; and finally the cloud and mobile computing era [4]. Cloud computing is the culmination of decades of research in virtualization, distributed computing, grid computing, utility computing, networking, and web and software services [22].

Nowadays, cloud computing has become a global trend, with the public cloud market forecasted to grow by 16.5% in 2016, projecting a global revenue of \$204 billion [3]. Amazon Web Services (AWS) is globally the largest provider of cloud services, with Microsoft Azure, Google Cloud, VMware and IBM as its challengers. Out of these, Google Cloud and Microsoft offer cloud services to consumers as well – Google Drive and Gmail, and OneDrive and Hotmail respectively – whereas the rest solely focuses on the business-to-business market.

Enterprises are showing an increasing interest in cloud computing services to support (critical) business functions. For this reason, cloud computing has been listed as one of the five most influential technologies on a global basis [23] and was deemed the third most significant IT investment in 2013 [9]. The cloud computing market is not only growing in the total number of adopters, but also in the number of enterprises adopting more than one cloud service. One survey reported the adoption numbers for small and medium enterprises (SMEs) to be 60% for at least using one cloud service, with 30% having purchased five or more cloud services [24]. With regards to current adoption, a recent survey found that enterprises use three public and three private clouds on average, with 82% of large enterprises pursuing a multi-cloud strategy [25].

2.1.1 Defining Cloud Computing

Although several definitions of cloud computing can be found in scientific literature, the most widely adopted comes from the National Institute of Standards and Technology (NIST), as used by Bayramusta and Nasir [9], and El-Gazzar, Hustad and Olsen [11], Dillon, Wu and Chang [12], Trivedi [26]. This study follows the same definition.

The following definition of cloud computing is given by NIST [27]:

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

This definition is extended by the decomposition of cloud computing in the following five characteristics:

1. *On-demand self-service*: a customer can provision computing capabilities as needed automatically, without human interaction with each service provider.
2. *Broad network access*: capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
3. *Resource pooling*: the provider's computing resources are pooled to serve multiple customers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
4. *Rapid elasticity*: resources can (automatically) be elastically provisioned and released to scale rapidly outward and inward on basis of demand.
5. *Measured service*: cloud systems automatically control and optimise resources by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilised service.

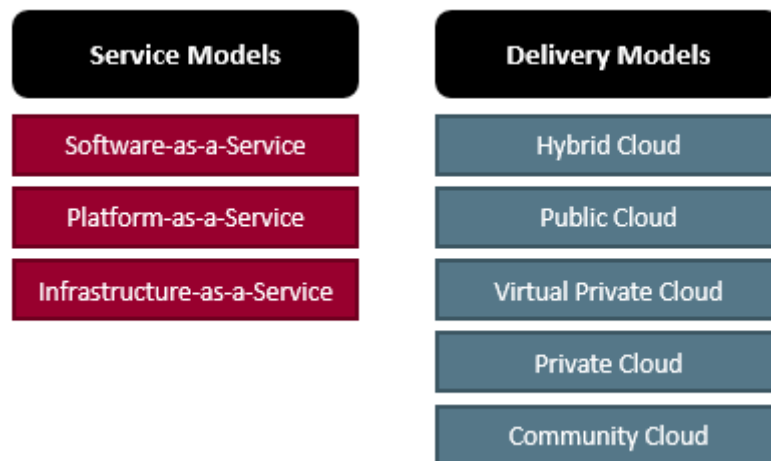


Figure 3 Cloud service and delivery models

In cloud computing, there is a clear distinction between its service models and its delivery models. Cloud service models are the cloud service that is purchased, whereas the delivery model is the hosting infrastructure of the service. Figure 3 gives an illustration of the available cloud service models and delivery models.

Cloud service models come in three main branches: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Figure 4 illustrates the level of managed resources for the customer and provider for several traditional service models as well as the three cloud service models.

1. *Software-as-a-Service (SaaS)*: With SaaS, a provider offers its (proprietary) software products in a cloud model. Consumers can access the software through a thin client interface (e.g. a web interface) or a program interface. In this model, the customer does not manage or control the underlying cloud infrastructure, but has only limited available customisation option, which are built into the software itself [27].

2. *Platform-as-a-Service (PaaS)*: PaaS is one step further down in its level of abstraction, allowing the customer to deploy their own applications on the cloud architecture (be it consumer-created or acquired). The cloud provider manages the underlying cloud architecture, where the consumer has control over the deployed applications and possibly configuration settings for the hosting environment [27].
3. *Infrastructure-as-a-Service (IaaS)*: With IaaS, the service provider offers an environment on which the consumer is able to deploy and run software, ranging from operating systems to applications. The cloud provider manages the cloud architecture, but the consumer has control over all functionalities, such as operating system, storage and deployed applications. Cloud providers may offer further options to consumers, such as limited control of select network components, but this is not required by definition [27].

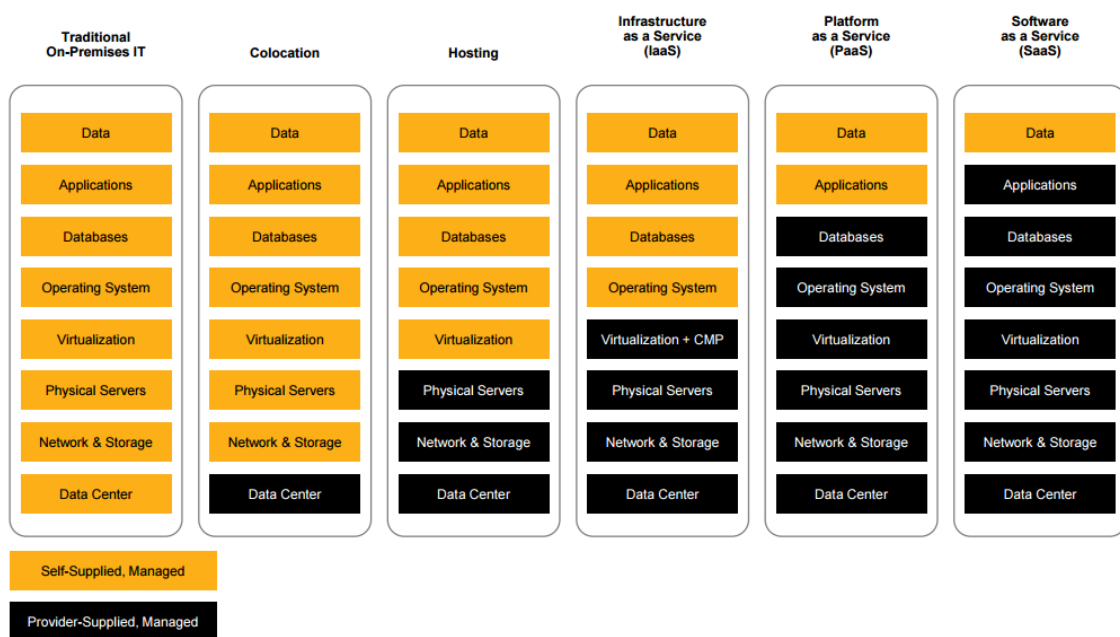


Figure 4 Level of self-supplied/-managed resources for different service models [2]

Next to these three cloud service models, five deployment models can be identified in scientific literature:

1. *Public Cloud*: This is the current dominant deployment model. Within the public cloud, the cloud service provider has full ownership of the cloud, meaning the physical infrastructure and cloud architecture, the level of ownership depending on the type of service models offered. They offer their services through the internet, offering the advantages of cloud computing to their customers. Anyone can sign up for these cloud services, with no restrictions on use set by the cloud provider. The key selling point of the public cloud is that the server architecture, and everything on top of that, depending on the service model, is managed by the cloud provider, essentially making the cloud service a piece of centralised infrastructure [12, 27].
2. *Private Cloud*: Private cloud, also referred to as an internal or enterprise cloud, delivers advantages similar to the public cloud delivery model. The main difference between the two is that a private cloud is hosted on a proprietary architecture (i.e. an organisation's

intranet or hosted data center), while still offering flexibility, scalability, provisioning, automation and monitoring. The driving forces in adopting a private cloud are optimising the utilisation of existing in-house resources, security concerns (e.g. data privacy and trust), data transfer costs from a local IT infrastructure to a public cloud, and full control over mission-critical activities [12, 27]. It must be noted that any cloud requires a multi-tenant model and that not all so-called private clouds have multiple tenants.

3. *Community Cloud*: The cloud infrastructure in this deployment model is provisioned for exclusive use by a specific community of organisations with shared concerns. A community cloud may be operated by one or more of the participating organisations or a third party. A community cloud offers a degree of the economic scalability of the public cloud while still being able to alleviate some of the concerns regarding trust and security these organisations have towards the public cloud [12, 27].
4. *Hybrid Cloud*: The hybrid cloud model is a deployment model consisting of two or more distinct deployment models (private or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability. Organisations use the hybrid model to optimising their resources by allocating non mission-critical business functions to a private cloud while controlling their mission-critical functions in a private or community cloud. The emergence of organisations with hybrid clouds raised the issue of cloud standardisation and interoperability [12, 27].
5. *Virtual Private Cloud*: A more recent deployment model is the virtual private cloud, which is a position hovering somewhere between the private and public deployment models. A virtual private cloud runs on a public cloud service, but functions as a sectioned off part of the private cloud, in which a dedicated set of 'isolated' resources is allocated. It allows organisations to apply their own corporate security policies, taking away some of the most pressing concerns organisations have with using public cloud [12].

For the sake of simplicity, oftentimes these five deployment models are aggregated into either public cloud, private cloud (not distinguished between private cloud, community cloud or virtual private cloud) and hybrid cloud. The reason to do so is because the deployment models under the umbrella of private cloud follow a similar execution style and only differ in the nature of their tenants, not by their technology or accessibility.

2.1.2 Benefits of Cloud Computing

The benefits of cloud computing are well-documented in scientific literature. This section gives an overview of the most commonly mentioned benefits.

Benefit 1: Cost reduction

A key factor in an organisation's decision to adopt cloud computing is the possibility to realise a cost reduction through reducing both investment costs (CapEx) and ongoing operating costs (OpEx) alike [8]. Adopting this OpEx model also transfers some of the risks of operating the IT systems to the provider, such as hardware failure and increased overhead costs [28].

One of the largest enablers for cost reduction is the introduction of economies of scale to IT infrastructure. While already happening in very large organisations, these economies of scale are now available to anyone [7].

Benefit 2: Changing from CapEx to OpEx

Moving to the cloud enables organisations to not have upfront capital investments due to the pay-per-use nature of cloud services [5, 6].

Marston, Li, Bandyopadhyay, Zhang and Ghalsasi [6] describe another benefit relating to this change. The shift from CapEx to OpEx enables organisations to benefit from computer-intensive business analytics that were only available to the largest of corporations before.

Benefit 3: Increased reliability

Virtualization on a cloud infrastructure permits the same data to be hosted at multiple data centers, greatly enhancing the reliability of (public) cloud services [7].

Benefit 4: Business process efficiency

Cloud computing also holds the promise of improved process efficiency through a more efficient technical infrastructure. It enables the automation of concurrent tasks, reducing the time required to carry out business processes [8].

Benefit 5: More agility

The benefits of shifting to a pay-per-use costing model and relief from owning and maintaining an IT infrastructure accumulate in increased agility for organisations. A low-cost, flexible and scalable infrastructure platform enables shorter time-to-market and a more automated development processes, allowing for greater IT agility [8]. This increased agility lowers IT barriers for organisations to innovate more rapidly [6].

Benefit 6: Focus on core business processes

Cloud computing offers organisations the ability to focus on their core business, rather than spending time and resources on IT. All IT operations will be handled by experts from the cloud service providers. [9]. With cloud functioning as commodity IT, the freed up resources can be used to focus on core competencies [8].

Benefit 7: Wide access to applications

Enabling end users to access data from any internet-enabled location facilitates remote and mobile access and makes it easier for end users to remain productive. It also allows users to collaborate from different locations on the same documents [7]. Although these benefits are not necessarily cloud-specific, it is an enabler at the least, as seen in Office365 and Google Drive.

Aside from these seven benefits, one commentary point stands out. Garrison, Kim and Wakefield [13] mention that there is one factor more important than these benefits and that is an organisation's ability to leverage them. Organisation-specific IT capabilities coupled with cloud computing can be a source for competitive advantage, but not developing these capabilities and only adopting cloud computing gives very little.

2.1.3 Challenges of Cloud Computing

Cloud computing also comes with several challenges, on which documentation in scientific literature was abundant. This section reviews each of the identified challenges.

Challenge 1: Security

Security is perhaps the most influential inhibitor of cloud computing adoption, which occurs due to the distributed nature of cloud computing. Having your applications and data on another's hardware seems daunting to many [12]. Kshetri [29] even mentions that the security, privacy and compliance cost may outweigh the costs/benefits from cloud computing in certain scenarios.

El-Gazzar, Hustad and Olsen [11] confirm the view that, in scientific literature, security issues are the most serious barrier to cloud computing adoption by showing that publications in both technical and managerial fields focus on these issues. They also state that reliability and trust are the main inhibitors for cloud adoption in SMEs.

El-Gazzar, Hustad and Olsen [11] show in a Delphi study that the risk level of cloud computing is significantly higher than those of traditional IT outsourcing due to the nature of cloud computing being based on shared virtual resources and data transfer over the internet, in addition to remote data hosting. This statement is reinforced by their finding that 'risk of losing control over resources' is the most important issue in cloud computing, which is an overarching theme on the underlying issues in cloud computing.

Interestingly enough, El-Gazzar, Hustad and Olsen [11] also concluded that business IT alignment was not a main concern when adopting cloud computing, even though it has been addressed as one of the most significant security risks [30], as it undermines corporate security policies. They also found that clients are generally not proficient enough in their data security governance, a view supported by Khorshed, Ali and Wasimi [31]. In their study, there was a call for an independent third-party to monitor cloud computing services and provide security audits, which would alleviate several of the security concerns, albeit at a higher cost [11].

On the provider's side, studies show that they tend to regard the security issues as a lack of security competence and skill among clients. However, several articles refuse this premise by mentioning that cloud computing has some specific risks on the cloud provider's side due to the shared vulnerabilities of the technology and their unwillingness to disclose their security practices in full detail [11, 30, 31].

Challenge 2: Costing model

While migrating the IT landscape to cloud platforms reduces infrastructure costs, it raises the cost of data communication. Also, the cost per unit (e.g. a VM) of computing resource used is likely to be higher than hosting it on-premise [12].

Challenge 3: Charging model

The charging model of cloud computing services is more complicated than that of the traditional data centers. The unit of cost analysis is now an instantiated virtual machine, which shares resources with other tenants, and not the (static) physical resources used [12].

Challenge 4: Service Level Agreements (SLAs)

Although control over underlying resources is relinquished, cloud consumers do need to ensure quality, availability, reliability, and performance of these resources. These are provided through SLAs. Both the definitions of these SLAs, as well as the implementation of it, pose additional challenges with the complexity of cloud computing [12].

Challenge 5: Not knowing what to migrate

With all the security and privacy concerns mentioned, organisations are still debating which processes should be moved to the cloud. Organisations are conservative in employing IaaS as compared to SaaS. This is partly because mission-critical processes are being kept in-house [12].

Challenge 6: Cloud interoperability

Each cloud offering has its own method on how cloud clients/applications/users interact with the cloud, leading to a diffuse landscape with little standardisation. This is an inhibitor to the development of cloud ecosystems [12].

2.2 Maturity Models

Organisations are continuously required to gain and retain a competitive advantage. In this light, an organisation's IT management is responsible for the effective and efficient design of IT to realise business goals, such as improving IT quality, increasing economic efficiency and reducing the time to market. The main goal of IT management is the continuous improvement of IT performance to realise the maximum potential effectiveness and efficiency for the least amount of resources [16]. Maturity models are an instrument for an informed approach to organisational improvement, to be used as an evaluative and comparative basis [20].

To be able to measure an organisation's current state and its improvement, there are two requirements: an organisation's ability to assess the current state of its capabilities and a comparison of the current state of capabilities with predefined goals in a comprehensible manner. A maturity model assists in fulfilling these requirements, as it gives both an assessment and a growth path in a set direction [16]. Secondary uses of maturity models originating from the assessment are self-assessment and benchmarking [32].

This report will use the definitions of maturity model and capabilities given by Smits and Van Hillegersberg [33], incorporating all elements of these models:

The basic concept of a MM consists of a number of areas—henceforth called focus areas—which mature along a predefined path to achieve higher levels of maturity. A higher level of maturity is defined as a better means to fulfil its purpose; the predefined path is described by a set of capabilities. Capabilities are the ability to mobilize and deploy resources to achieve a goal.

In addition, the current scientific literature, the following four types of maturity models have been identified:

- *CMM-like models*: Models that adopt the approach of the Capability Maturity Model use a more formal and complex design. These models identify a number of common features and key practices in each process area to address its goals. These models are mainly

concerned with process improvement and describe an evolutionary path from ad-hoc to mature processes, often on a five-point Likert scale [34, 35].

- *Maturity Grids*: A maturity grid consists of a textual description for each maturity level displayed on a grid. Fraser, Moultrie and Gregory [34] state that these models often have no standardised method of assessment, although a more recent methodology does include this in its development steps[17]. These models are usually of a moderate complexity and can be described in a few pages [32].
- *Situational Maturity Models*: Situational maturity models are designed to take into account the specifics of an organisation, i.e. instead of applying all maturity requirements an organisation can decide to discard those that do not apply [34]. These models alleviate some of the issues regarding the formalisation and standardisation of other maturity models, although they give up their comparative nature when used in different settings.
- *Hybrids and Likert-like questionnaires*: Likert-like questionnaires are composed of questions or statements of good practices, on which the answer is a score on a 1-n range relative to the organisations' performance. Hybrid models use a combination of questionnaire and definitions of maturity, often without a description of the activities to be performed [34].

The following sections describe certain aspects of maturity models in more detail, elaborating on displaying the maturity in maturity models, methods for maturity model development and the measurement of maturity (assessment methods).

2.2.1 Displaying Maturity in Maturity Models

Maturity models have can be divided into two categories: fixed-level models and focus area models. Fixed-level models distinguish a fixed number of maturity levels. This notation of maturity found its conception in the Capability Maturity Model [35] as a five-point Likert scale, with five representing the highest level of maturity [20]. Each maturity level is associated with a number of processes to be implemented or criteria to be met. A limitation of fixed-level models is their implicit interdependence between the processes making up the maturity levels, leading to unclarity on the prioritisation of which processes to implement [20]. As a result, fixed-level maturity models may be perceived as too large and heavy to use [18].

Focus area models attempt to solve the issues of fixed-level maturity models. This type of model is based on the concept that a number of differentiated focus areas have to be developed in order to achieve maturity in its domain. Each focus area has a series of progressively more mature capabilities attached, specific to the focus area identified [18]. This allows for a more granular view on maturity, as each focus area has its own progress and those lagging behind can be more easily identified. Figure 5 shows a focus area maturity model with maturity levels from A to D and the maturity in each focus area horizontally as a grey bar. This allows for an uncoupling of a singular maturity level for a focus area from the overall level of maturity and focuses more on the dependencies between the different capabilities.

Although focus area maturity models appear to be a fifth type of maturity model, the idea of showing maturity through the focus area design is applicable to each of the maturity model types.

<i>Focus Area</i>	<i>Maturity Scale</i>	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Development of architecture			A			B			C						
Use of architecture				A			B				C				
Alignment with business			A				B				C				
Alignment with the development process				A				B		C					
Alignment with operations					A				B			C			
Relationship to the as-is state					A					B					
Roles and responsibilities					A		B					C			
Coordination of developments								A			B				
Monitoring					A		B		C		D				
Quality management									A		B			C	
Maintenance of the architectural process								A		B		C			
Maintenance of architectural deliverables						A			B					C	
Commitment and motivation			A					B		C					
Architectural roles and training					A		B			C			D		
Use of an architectural method					A						B				C
Consultation				A		B				C					
Architectural tools								A				B			C
Budgeting and planning					A							B		C	

Figure 5 A focus area maturity model example [18]

2.2.2 Maturity Model Development

Maturity models represent an anticipated, desired or typical evolution path presented as discrete stages. The initial stage represents an organisation having little capabilities in the considered domain, which contrasts with the highest stage of maturity representing a conception of total maturity. The stages in between represent a path of continuous progression of the organisation's capabilities [16].

In order to realise such a model, several methods have been proposed for the creation of a maturity models, although there is no consensus on the subject [18, 33]. This section describes the five methods identified in scientific literature in chronological order.

De Bruin, Freeze, Kaulkarni and Rosemann [20] have assessed several maturity models in different domains and identified six general phases that constitute the process of developing a maturity model:

1. *Scope*: Determine the scope of the desired model. This phase involved specifying the focus domain of the model and its most important stakeholders. This stage also determines the specificity and extensibility of the model.
2. *Design*: The second phase consists of deciding on the architecture of the model and identifying the model's audience. The design of the model should incorporate the needs of the intended audience and clarify on how these needs will be met.
3. *Populate*: This stage concerns the content of the maturity model. In this phase you identify what is being measured and how this can be measured. Domain components and the method of measurement are defined.
4. *Test*: The model must be tested for relevance and rigour. Both the construct of the model and its instruments must be tested for validity, reliability and generalisability.
5. *Deploy*: The model is being made available for use and its generalisability is verified.
6. *Maintain*: Some form of repository is set up to support model evaluation and further development.

Becker, Knackstedt and Pöppelbuss [16] propose a procedure model for the development of maturity models. They identified seven requirements for the development of maturity model, from which they deduced a “generic and consolidated procedure model for the design of maturity models.” The procedure model consists of seven steps:

1. *Problem definition*: During the problem definition phase the targeted domain and the target group of the maturity model need to be determined. At the same time, the problem relevance must be clearly demonstrated.
2. *Comparison of existing maturity models*: A comprehensive comparison of existing maturity models is required for a reasoned determination of the design strategy.
3. *Determination of development strategy*: A documented decision needs to be made for the design strategy. The most important design strategies are: construction of a completely new model; combination of several models into a new singular mode; and the transfer of structures or contents from existing models to a new context.
4. *Iterative maturity model development*: This is the central phase of the development process. It involves several iterations of four steps (select design level, select approach, design model section and test result), which at the highest level constitutes the model architecture, but is also applicable to specific model elements.
5. *Conception of transfer and evaluation*: The different forms of result transfer for the academic and user communities need to be determined.
6. *Implementation of transfer data*: The maturity model should be made accessible to the planned target audiences through the forms decided upon in phase six.
7. *Evaluation*: The evaluation phase should establish whether or not the designed model provides the projected benefits and an improved solution for the problem. The outcome of this phase may cause another design iteration of one or more phases or a rejection of the model as a whole.

Mettler and Rohner [19] propose a design exemplar for situational maturity models. Their proposition consists of three steps, albeit only shown through their exemplar without elaboration on their method itself:

1. Problem identification and motivation.
2. Objectives of the solution.
3. Design and development, which consists of several steps of its own: basic maturity model design; specification of maturity levels; configuration parameters; and a proof of concept.

Van Steenberghe, Bos, Brinkkemper, Van De Weerd and Bekkers [18] propose a method for the development of focus area maturity models. It consists of ten steps:

1. *Identify and scope the functional domain*: For a maturity model to be useful, it must be scoped properly. This phase is also important for identifying existing maturity models for the same or related functional domains.
2. *Determine focus areas*: The focus areas within the chosen domain need to be identified.
3. *Determine capabilities*: Each focus area consists of several different capabilities which represent progressive maturity levels.

4. *Determine dependencies*: Dependencies between the capabilities are identified. These dependencies do not limit a singular focus area, but may span across the whole set.
5. *Position capabilities in matrix*: Capabilities are positioned in the matrix. Capabilities that are dependent on other capabilities are always positioned further to the right.
6. *Develop assessment instrument*: In order to use the focus area maturity model, measures must be defined for each of the capabilities, i.e. through control questions for each capability. These questions could then be presented in a questionnaire.
7. *Define improvement actions*: For each of the capabilities, improvement actions can be defined to support practitioners in moving to that capability.
8. *Implement maturity model*: Application of the model can be done in various ways, depending on the method of assessment.
9. *Improve matrix iteratively*: When enough assessment results become available, the quantitative data can be used to improve the model. A repository must be kept to collect assessment results.
10. *Communicate results*: The results of the design should be communicated to practitioners as well as the scientific community.

Originally conceived in 2009 and updated in 2012, Maier, Moultrie and Clarkson [17] propose a “practitioner guidance” that supports the development and application of maturity grids. They propose a four stage approach after reviewing 24 maturity grids:

1. *Planning*: The aim, purpose, requirements, scope and target audience of the maturity grid are defined in this stage. In addition, this stage also requires the development of success criteria.
2. *Development*: The different parts of the maturity grid are defined, such as the process areas, maturity levels, cell text and the administration mechanisms.
3. *Evaluation*: The maturity grid is validated and verified against its success criteria. If necessary, more development iterations take place.
4. *Maintenance*: This phase is an ongoing phase, ensuring continuous accuracy and relevance of the maturity grid. Changes must be evaluated and documented thoroughly.

Although no consensus exists on which of these methods to use, they share common traits, as identified by Van Steenberg, Bos, Brinkkemper, Van De Weerd and Bekkers [18]. They identified four common process phases: scope; design model; develop instrument; and implement & exploit. In their own proposed method, they use these four overarching phases to structure their own method.

Aside from their similarities, these methods are applicable to different scenarios, as shown in Table 3. The methods of De Bruin, Freeze, Kaulkarni and Rosemann [20] and Becker, Knackstedt and Pöppelbuss [16] are the two methodologies not limited to any specific type of maturity model, and can thus be considered to be general methods.

	De Bruin	Becker	Mettler	Van Steenberg	Maier
Type of maturity model	Any	Any	Situational	Focus area	Grid

Table 3 Applicability of maturity model development methods: a comparison

2.2.3 Maturity Measurement

In the measurement of maturity, three distinct approaches can be identified: self-assessment, third-party assisted assessment and outsourced assessment [20]. This section briefly describes each of these approaches.

Self-assessment is the easiest method of maturity assessment. It gives the model user the tools to perform an assessment, which requires information about the own capabilities and level of maturity [32]. The assessment questionnaire comes in two general levels of detail: a quick scan, meant to give a quick but generalised overview of an organisation's maturity; and a self-assessment, aiming to give the target audience the tools to perform a maturity assessment by themselves. Examples of questionnaire assessments are given in [18, 36].

A third-party assisted assessment has a lot of similarities to a self-assessment, except that the organisation receives help from an expert in the process [32]. This eases the tasks of gathering the necessary data and structuring the outcomes.

The third assessment method is the outsourced assessment, which fully relies on third parties to perform the assessment [32]. This requires a domain experts to visit an organisation and perform an assessment through either interviews or a checklist. This method is suited for a more qualitative assessment of an organisation's maturity. One downside of this method is that it is more laborious and that a well-designed questionnaire may give comparable results to the more labour-intensive outsourced assessment [37].

Each assessment method has its merits, with no clear indication in the identified articles to which method is commonly accepted. Their difference mostly lies in how thorough the conducted assessment is and its time investment, which calls for a best fit for a situation.

3 Comparing Cloud Maturity Models

Seven cloud maturity models were identified in our literature search: three from academia and four from practitioners. This chapter describes the search process and gives a description of the models themselves. It is followed by the creation of a set of evaluation criteria for cloud maturity models and the evaluation. The chapter closes with a discussion of the comparison results in the scope of the initial two research questions.¹

3.1 Identifying Cloud Maturity Models

To identify the cloud maturity models in use, we will perform a systematic literature study as described by Kitchenham [39]. This section describes the search process to identify current cloud maturity models and formulate inclusion and exclusion criteria for publication selection.

A short introductory search using “cloud maturity model” on the Scopus database yielded one result, a 2013 publication. Using (“cloud computing” AND “maturity model”) yielded 25 results after excluding conference reviews. The low number of scientific publications was reason to expand the search, where orientation on practitioners’ models through Google, using the same terminology, gave an the impression that cloud maturity and cloud adoption were interchangeable.

With this knowledge, we set out with the following query on Scopus: (“cloud computing” AND (“maturity model” OR “adoption model”)). After the exclusion of conference reviews, this yielded 44 publications. We considered splitting the keyword model from maturity and adoption, creating the following query: (“cloud computing” AND ((“maturity” OR “adoption”) AND model)). This, however, bloated the results with different types of models, as the keywords did not appear in sequence. The search was performed on September 21, 2016.

3.1.1 Filtering the Results

The second stage of the literature study consists of filtering the acquired results for inclusion by first reading the titles and abstracts, followed by filtering based on a full publication review. The filtering process was performed with the following inclusion and exclusion criteria:

Inclusion: (I1) The main focus of the publication is cloud computing adoption. (I2) The publication proposes either a new model or an incremental improvement of an existing model for cloud adoption.

Exclusion: (E1) If a publication does not use distinct levels of maturity or adoption, then we exclude it because it does not follow a maturity approach. (E2) If a publication focuses on a model only aimed at adopting a single cloud service, meaning that one would have to iterate through the model several times to adopt more cloud services, then we exclude it because it does not indicate a model for continuous improvement, or maturity. (E3) If a publication is not written in English, it will be excluded from this study.

¹ This chapter has been informed through the research completed in the Research Topic course [38]

After reviewing the titles and abstracts on these criteria, 4 out of 44 publications were assessed to be within the scope of this research. These four publications were then subjected to a full publication review. two of the publications were then excluded. Okai, Uddin and Arshad [40] was excluded on E2, since it provided a staged model for adopting one or more cloud solutions, lacking any form of continuity in the model, which is imperative for a maturity model. Alkhater, Chang, Wills and Walters [41] failed to pass E1 in not incorporating a staged approach towards cloud adoption.

3.1.2 Expanding on Scientific Literature

With only 2 included publications from academia, we followed the approach used by Weiss, Repschlaeger, Zamekov and Schroedl [42], which incorporated practitioners' models, master theses, and PhD dissertations. Information Systems is an applied research field and as such, practitioners' models should not be dismissed. To gather these, Google, Google Scholar² and DuckDuckGo³ were consulted with the same queries used in Scopus.

Google was used because it is the world's leading search engine in market share. Google Scholar was used for its inclusive nature, allowing for the identification of master theses and PhD dissertations. DuckDuckGo was used because they do not store tracking data and user history, and as such may present no-bias results that Google might have omitted. DuckDuckGo did not present additional cloud maturity models, but did confirm the findings from Google.

From this search, selected publications were investigated against the inclusion and exclusion criteria. From practitioners, we selected publications from consultancy firms, cloud providers, and industry congregations. From Google Scholar we selected publications on their title out of the first 50 results. This yielded three relevant results, out of which one contained a model. The total results of this step are 4 models by practitioners and 1 from a master thesis.

The results of this process per iteration can be found in Table 4. In total, seven cloud maturity models have been identified; two from scientific literature, with four practitioner models and one master thesis through alternative methods.

Iteration	Total number of results
Scopus query	44
Filtering on abstract review	4
Filtering on full review	2
Extended query (including practitioner models)	7

Table 4 Number of papers per stage

3.2 Identified Cloud Maturity Models

This section describes the seven identified cloud maturity models. The description encompasses both the model itself, describing its scope, constructs and origins, as well as any available information on its development.

² <http://scholar.google.com>

³ <http://www.duckduckgo.com>

3.2.1 Duarte Cloud Maturity Model

The Cloud Maturity Model (Duarte CMM) [1] is a model based on the outsourcing lifecycle. The model's scope is the migration of IT services to the cloud in organisations where this decision has already been made.

The model is an adaptation of the outsourcing lifecycle, combined with the continuous approach for process improvement of the Capabilities Maturity Model Integration for Services (CMMI-SVC). It comes supported with a set of 54 key activities, divided over four phases and nine building blocks. Each of the lifecycle phases has an assigned maturity based on the number of key activities positively ranked, with the aim of demonstrating organisational maturity in process segments instead of a singular model approach. Figure 6 illustrates a possible outcome of the assessment.

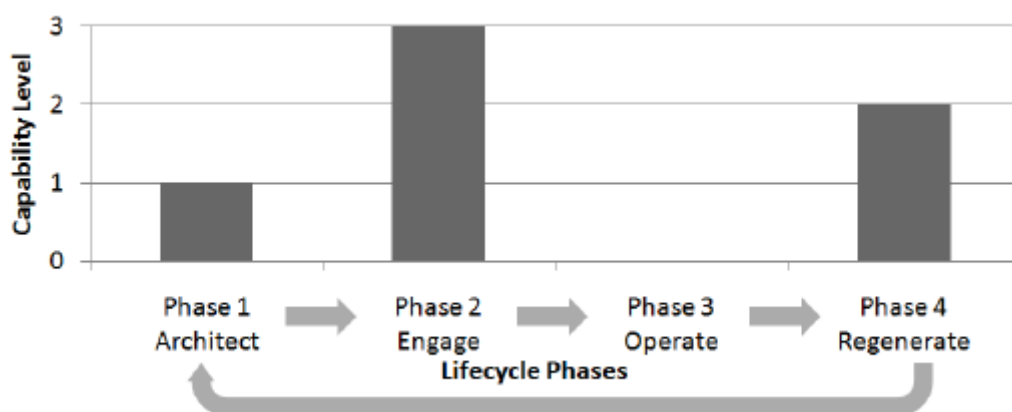


Figure 6 Duarte Cloud Maturity Model [1]

The maturity model was developed with the purpose of giving answers of what constitutes cloud adoption and demystifying cloud computing. This was achieved through interviews with twelve cloud experts, having a median experience of eight years, with an average of ten. The experience is not specifically defined as cloud computing experience, but since values of over 20 years were listed, we assume that this is experience in the IT field. The median company size of the interviewees was 150 FTE, with an average of 15000 FTE.

The interviews aimed to validate the outsourcing lifecycle for relevance in the area of cloud computing. 50 out of the 54 key activities have been identified as important for cloud computing, making the outsourcing lifecycle usable for cloud computing.

The step from identifying the relevance of the key activities of the outsourcing lifecycle in cloud computing to the creation of the maturity model and its assessment is not addressed in this publication. Another question left open is what constitutes maturity, as it is unclear whether merely checking off more items on the list gives a higher maturity or if there is an order in which the capabilities are deemed to be achieved. When assuming the first, we conclude that this model is no maturity model at all, but rather a guideline for cloud adoption. When assuming the second option, we conclude that the model is incomplete without defining which key activities are linked to which maturity level.

3.2.2 Weiss Cloud Computing Maturity Model

The Cloud Computing Maturity Model (Weiss CCMM) [42] was developed using the procedural model of Becker, Knackstedt and Pöppelbuss [16], described in section 2.2.2. The scope of the model is assisting organisations using cloud computing to assess and improve their cloud capabilities. The model is aimed for use at every level of IT and business management within an organisation.

The model itself is constructed out of six domains – a synonym for focus areas – and five maturity levels, following the traditional five-point Likert scale based on the Capability Maturity Model Integration. It is a grid maturity model, giving a description for each of the level/domain cells, with the addition of two cells per maturity level: the challenges of growing to that maturity level, called effects, and recommendations to deal with these challenges. Figure 7 gives an illustration of the first level of the Cloud Computing Maturity Model.

Domain		Governance	Security	Organisational Readiness	Processes	IT Infrastructure	Operational IT management
Level	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
Level 1: Initial	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					

Figure 7 First level of the Weiss Cloud Computing Maturity Model [42]

The domains in the model consist of a grouping in four organisational and two technical domains. The organisational domains are: governance; security; organisational readiness (the capabilities required for cloud adoption); and process. The technical domains are IT infrastructure and operational IT management. These domains are derived from their literature study.

Development of the model stopped, as the authors noted, after the initial development. They recommend the model to be used as a guideline for further development of cloud maturity models, as well as validating the model through validation rounds of expanding size. Although it lacks validation, it is a complete maturity grid, based on a literature review of cloud maturity models from 2012 and earlier.

3.2.3 Cloud Maturity Model 3.0

The Cloud Maturity Model revision 3.0 (CMM3) [43] has been developed by the Open Data Center Alliance Inc., a consortium of global IT organisations who “came together to deliver a unified voice for emerging [...] cloud computing requirements”⁴. The scope of the model is to provide an organisational roadmap to cloud adoption.

It is the most prominent model when searching for ‘Cloud Maturity Model’ in general purpose search engines (e.g. Google.com, DuckDuckGo). Revision 3.0 is dated January 2016. It describes the following steps to use the model:

⁴ <https://opendatacenteralliance.org/about-us/>

1. Identify business goals
2. Define use cases for CMM

Enterprise objectives are identified in the context of use cases, identifying potential technological applications and actors, and a prospective timeline, as well as the required CMM maturity level required.

 - a. (optional) Define services to be delivered

Where the use cases define the business needs regarding cloud capability, the identification of what the IT department needs to accomplish each use case is done by explicitly defining the required services.
3. Conduct CMM assessment

The assessment is conducted through stakeholder interviews to identify the relevant domains for each use case. What follows is investigating the minimum required and current maturity levels of each domain, based on selected control questions for each domain, relevant to the use case.
4. Create a report/roadmap

Define the projects required to achieve the desired maturity levels in each domain.

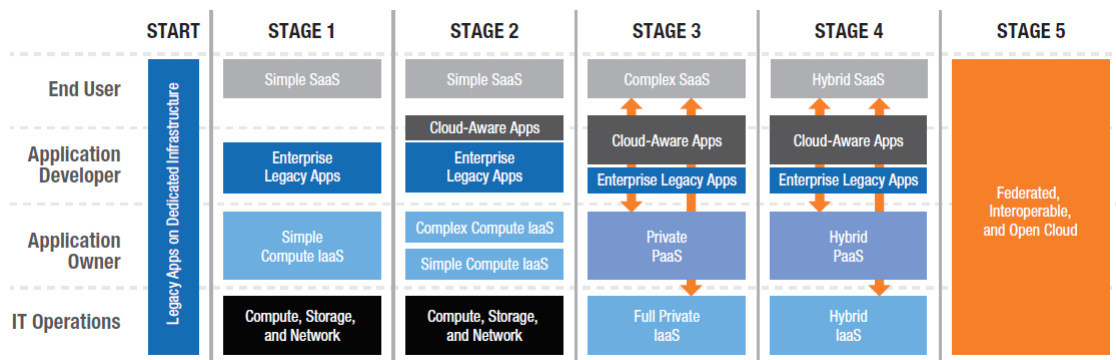


Figure 8 Example roadmap of the Cloud Maturity Model [43]

The example roadmap in Figure 8 shows two things: the roadmap focuses on business roles and aims at concrete points for cloud adoption. The roadmap is divided in stages, but in itself tells little of the capabilities involved and whether or not these are linked directly to the stages. In the sparse available public documentation mention is made of an assessment (see step 3 in the process), although the assessment itself appears hidden behind a paywall.

The cloud maturity model 3.0 bases its development and iterations on knowledge sources in and feedback from organisations (experts) using the model. A notable characteristic of the model is that it does not provide a clear image of maturity levels from the start, but rather requires organisations to perform an assessment based on business goals and use cases.

Unfortunately, no more information about this model is available publicly. The model appears promising, but the mentioned assessment and roadmap creation tools are not publicly available and, while their existence is taken into account, these could not be reviewed.

3.2.4 AWS Cloud Transformation Maturity Model

The Amazon Web Services (AWS) Cloud Transformation Model (AWS CTMM) is a vendor-specific cloud adoption model [44]. Its scope is to provide an insight into the steps and challenges

encountered when migrating IT services to Amazon's cloud services. Even though it is not a generalised cloud maturity model, since it is aimed at AWS customers, it may provide insight in the cloud adoption process and its challenges. Figure 9 shows the AWS Cloud Transformation Maturity Model.

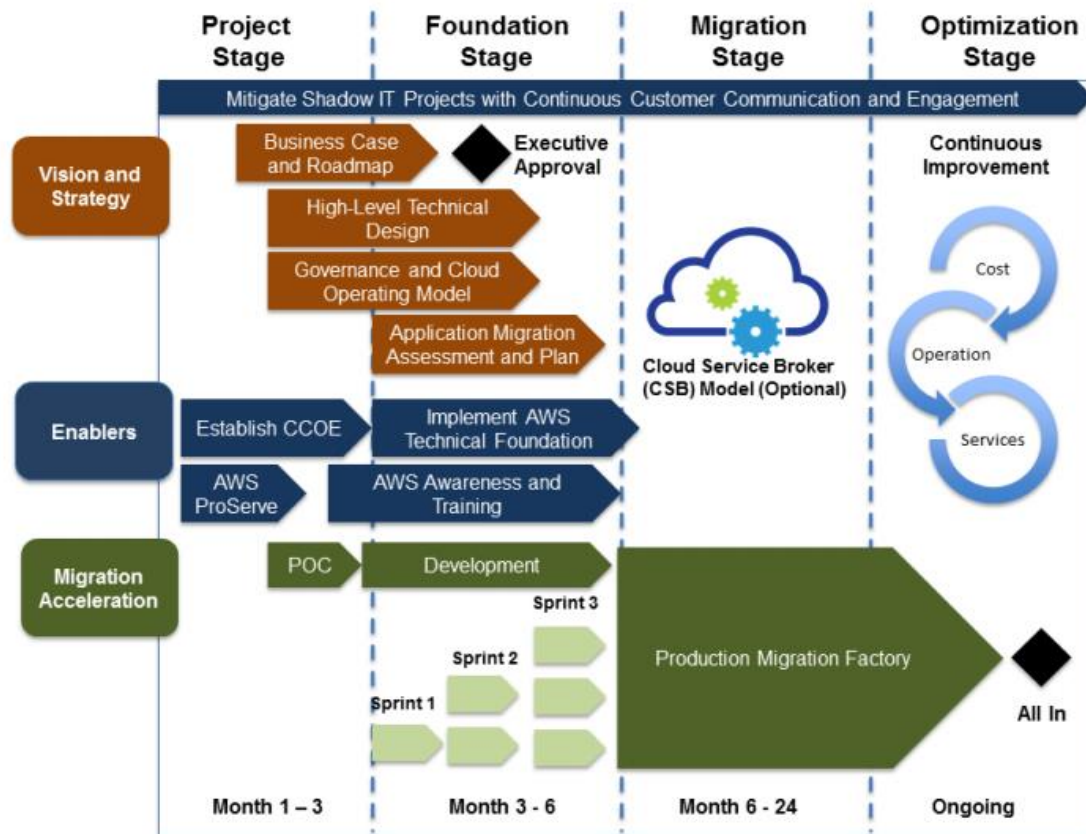


Figure 9 Amazon Web Services Cloud Transformation Maturity Model [44]

The model consists of four stages, with three focus areas. The three focus areas are: Vision and Strategy; Enablers; and Migration Acceleration. Vision and Strategy focuses on the development of a cloud adoption strategy, Enablers describe the factors relevant for adopting AWS cloud services, and Migration Acceleration describes the migration process to transform the current IT landscape to become cloud-ready and adopt the desired cloud services. For each of the stages the model identifies three factors: customer challenges; transformation activities; and outcomes/milestones of maturity.

Development of the model was done in-house at AWS, with the expertise of aiding a large number of customers in making their transition from on-premise and outsourced IT services to cloud services, however nothing is disclosed about the development of the model.

Although this is the only maturity model from AWS, the organisation has spawned other models for cloud adoption as well, the most notable being their AWS Cloud Adoption Framework, which focuses on several perspectives toward cloud adoption. The Cloud Adoption Framework is more high-level in its setup, giving guidelines for the creation of a cloud strategy (with the final goal of adopting AWS cloud services) [45].

3.2.5 Forrester Model for Cloud Maturity

The Forrester Model for Cloud Maturity (Forrester MCM) [46] was developed by Forrester, a research and advisory firm, and published as a whitepaper. Its scope is a model that gives organisations a grip on both private and public cloud. With that, it is the only cloud maturity model that explicitly states the differences between public and private cloud. Figure 10 gives an illustration of the maturity levels in the model.

The model consists of two four-cell maturity grids, one each for both private and public cloud. These two so-called paths are then consolidated in a fifth maturity level, called portfolio optimization. Each cell contains a description of the steps to take to reach the next maturity level, with the underlying, implied capabilities. However, it lacks a viewpoint beyond a purely technical/operational, only briefly mentioning strategy in the fifth stage: portfolio optimisation.

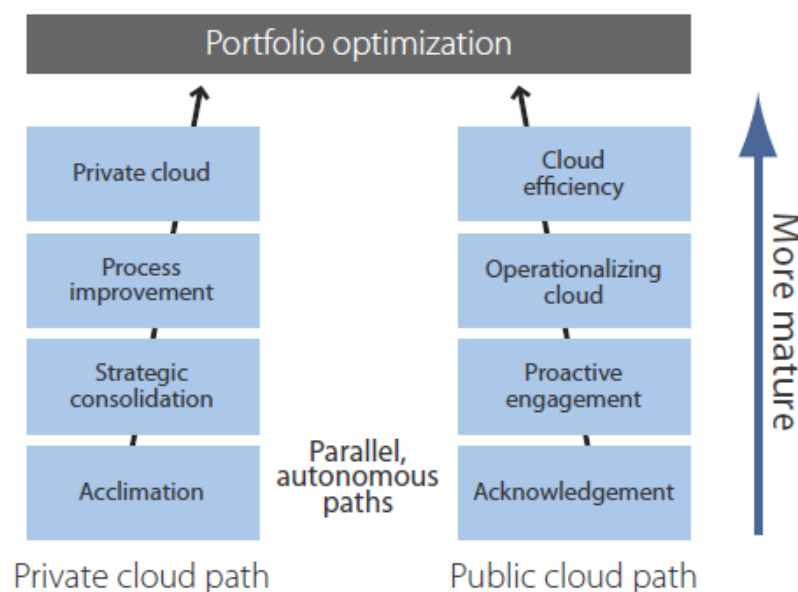


Figure 10 Forrester Model for Cloud Maturity [46]

The model stems from the identification of challenges in adopting cloud computing, stating that most companies start with cloud without a predefined plan. The identified challenges are the different financial model (operating expenses and demand-based usage) and the changing internal IT organisation. The whitepaper then explains the need for both public and private cloud delivery models in an organisation to reap the full benefits of cloud computing. Interestingly, they state that “success on the public path doesn’t determine success with private cloud,” [46] making it the only model to distinguish between the two branches of service delivery models this clearly.

3.2.6 Cloud Computing Maturity Model

The Cloud Computing Maturity Model (CCMM) [47] is a five-stage model developed by GTSI solutions. Its focus is to provide a framework for the successful implementation of cloud computing. The whitepaper first defines cloud computing and its benefits and risks, after which the model itself is presented. Figure 11 depicts the model.

The model consists of five stages, the standard for the number of maturity levels, called consolidation, virtualization, automation, utility and cloud. Each maturity level is divided in technical aspects and their key enabling capabilities. The model takes a technical orientation at lower maturity levels, later shifting towards a more management-based orientation.

Step 1 Consolidation	Step 2 Virtualization	Step 3 Automation	Step 4 Utility	Step 5 Cloud
Consolidation & Modernization of Resources	Abstraction & Resource Pooling	Adaptive, Secure, & Repeatable	Self-Service & Metering	On-Demand & Scalable
Server Consolidation	Server & Storage Virtualization	Policy-Based Provisioning & Management	Service Metrics & Metering	IaaS, SaaS, PaaS
Tiered Storage Consolidation	Desktop Virtualization	ITIL-Based Repeatable Processes	Service Level Agreements (SLAs)	Service-Oriented Architecture
Consolidation of Network Services	Virtualized Network Services	Multi-Tier Security	Incident Response & Audit	Inter-Cloud Federation
Consolidation of Disparate Applications	Application Virtualization	Multi-Tier Data Recovery	Continuous Availability & Failover	Integration of Web 2.0 & Web Portals
Key Enabling Capabilities				
Consolidation	Virtualization	ITIL Service Management	DR & COOP	Cloud Internetworking
Modernization	Thin Client Computing	Network Security	Risk / Vulnerability Management	Integration
Power & Cooling	Green IT	Data Center Security	Situational Awareness	Provisioning
High Performance Computing	Data Duplication	Infrastructure Protection		

Figure 11 Cloud Computing Maturity Model [47]

The model makes no mention of any development process, but is based on the benefits and risks of cloud computing, attempting to mitigate these by bringing structure in the cloud adoption process. That being said, there is no clear manner of assessment provided. For the technical components, this might not be an issue, but the lack of a description of the key capabilities makes these very difficult to assess (e.g. what is Power & Cooling as a capability?).

3.2.7 Cloud Adoption Model for Governments and Large Enterprises

The final assessed maturity model is the Cloud Adoption Model for Governments and Large Enterprises (CAM) [26], described in a master thesis. The scope of this model is the adoption of private cloud for large enterprises. It combines organisational cloud readiness, milestones and the implementation timeline into a single model. Figure 12 provides an overview of this model.

The model is comprised of four stages of cloud adoption:

1. Thinking (about Cloud)
Characterised as having IT as it has been known in the previous decades. IT is seen as a cost center, running on-premise enterprise applications and data centers, which do not leverage any advantages of cloud computing.
2. Initiating (reach for Cloud)
This stage builds upon the executive and organisational awareness of stage 1, focusing on creating and implementing a cloud strategy.
3. Creating (organisational Cloud)
Organisations in this stage are making definitive steps towards cloud computing adoption.

4. Riding (the Cloud)

This stage is marked by the coexistence of legacy and cloud environments, continuing moving further into cloud computing.

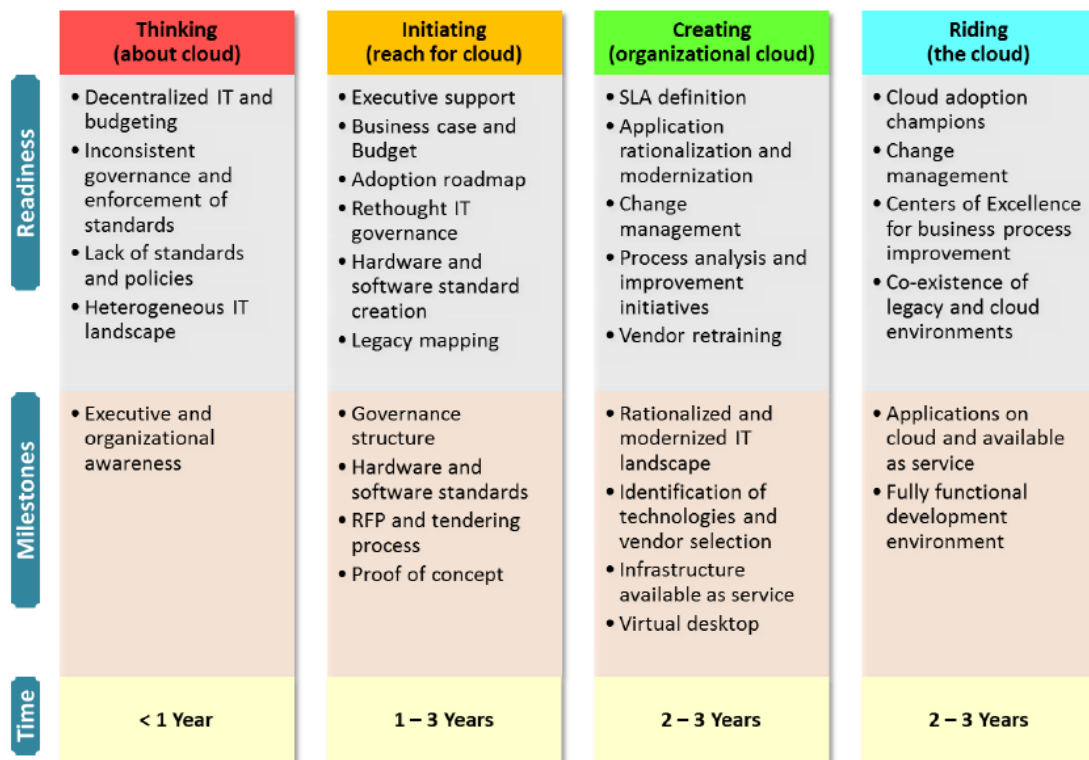


Figure 12 Cloud Adoption Model for Governments and Large Enterprises [26]

The model is based on several case studies of governments and large enterprises during their cloud adoption journey, providing a better insight into its creation than most others. However, it lacks validation, since it only maps the model to the past cases by which it was constructed and simulating a use case. These limitations are denoted by the author.

Another limitation marked by the author is the construction context of the model. Due to its focus on governments and large enterprises, it only deals with private cloud solutions, disregarding hybrid and public cloud solutions.

3.3 Assessment of Identified Cloud Maturity Models

The identified cloud maturity models were assessed on two domains: their scientific rigour; and use of elements identified in literature. This section describes the step of comparing existing maturity models. Our scope, defined in section 1.1, is to develop or extend an internal cloud maturity model for IT management.

The scientific rigour domain was tested by holding the model against the method of Becker, Knackstedt and Pöppelbuss [16], described in section 2.2.2. The assessment elements are identified through the performed background study and the choices are justified in this section.

3.3.1 Assessment Elements from Literature

As each of the models discussed in section 3.2 has the goal of presenting insight in the cloud adoption process, thereby increasing the success rate of cloud adoption, these models should touch on the challenges and benefits of cloud computing identified in section 2.1.

The first two elements are the *service and deployment models* of cloud computing. A maturity model should mention the three distinct service models (SaaS, PaaS, IaaS), as each comes with a different level of virtualization and thus a different set of required capabilities. In the same line of thought, maturity models should mention the distinction between private and public cloud solutions and the reasons and capabilities for choosing these.

In addition to these elements, it is also key to define a timeline or roadmap for migration of the IT landscape to indicate what should be migrated when. When a maturity level stands on its own, it lacks the context of what an organisation is able to do at that maturity level. For example, moving primary business processes to the public cloud requires a vastly different – and presumably more mature – set of capabilities than deciding to implement a cloud storage solution (e.g. Dropbox). As such, guidelines on *what to migrate when* is an important indicator of the usability of a cloud maturity model.

Cloud computing means not only a shift in the technology used, but also presents a different way of managing IT. The focus shifts from operating IT (keeping it running) to a directing role, where vendor management and keeping the spread-out IT landscape under control is key. *Process management* to transition the IT organisation when adopting cloud services is a key component of successful cloud adoption, and should be mentioned in a cloud maturity model.

Continuing in this line of thought, *integration* is a key component of successfully achieving this transition. Without being able to integrate the different cloud solutions, moving away from the current IT landscape would only make sense for isolated applications. Cloud service providers offer APIs and other tools for data integration, which should be mentioned in a cloud maturity model to improve its usefulness.

Aside from the IT organisation, the financing model of IT also changes with the adoption of cloud computing. IT investments shift from capital expenses to operating expenses, alleviating the requirement of an up-front investment in hardware. This eases the costing curve, but may result in more costs over time when the hardware is utilised 100% of the time, as the costs related to usage. This new costing model comes with several challenges, such as demand management to keep costs in check, but also provides opportunities, like cost attribution directly to the business units using the IT. This makes *financial management* a key part of cloud adoption and thus should be mentioned in a cloud maturity model.

What (prospective) cloud adopters perceive as the major challenge of cloud computing is its security. Although this is being outpaced by a lack of cloud expertise, security remains one of the key concerns when adopting cloud computing. Although often dismissed as a lack of security competence at the cloud consumer side, cloud computing does come with additional security risks, stemming from the shared and distributed nature of the technology. This, combined with the fact that cloud providers prefer to handle their security as a black box, gives way to the

issue of *security management*, which should at the very least be mentioned in a cloud maturity model.

Security is not a stand-alone subject, as it is often closely related to *governance* and *compliance*. The abstraction of the hardware layer and the multi-tenant model require different capabilities for these topics. Aside from the changing delivery model, they require clear frameworks to interpret what applications can be deployed on which type of deployment model (e.g. private data on private cloud).

The final identified challenge is *SLA management*, which severely changes due to the relinquishment of control over underlying resources. SLAs are put in place to ensure quality, availability, reliability and performance of these resources. Managing these SLAs and having the know-how of your requirements towards cloud service providers are important factors in cloud adoption.

In addition to these challenges, there are two defining characteristics of maturity models that are required for a model to be useful. The first is the addition of *capabilities*, either inferred (e.g. having a cloud strategy infers having the capabilities to devise such a strategy) or explicitly mentioned. A maturity model without capabilities, or with ill-defined capabilities, is not useful. The second essential characteristic is having a clear manner of *assessment*. For maturity grids, this is as easy as presenting the grid itself, but for more extensive models this can extend itself to long questionnaires with intricate scoring mechanisms. If no clearly presented manner of assessment is available, even the most well-devised maturity model becomes nothing more than a grid-like checklist.

To summarise, the following elements have been identified to assess the cloud maturity models: cloud service models; cloud deployment models; what to migrate; transitioning the IT organisation; integration; financial management; security management; governance; compliance; SLA management; capabilities; and assessment.

3.3.2 Mapping the Maturity Models on the Identified Elements

In this section, the seven cloud maturity models are assessed on the inclusion of the identified elements and their scientific rigour, of which an overview is presented in tables 5 and 6 respectively. In the assessment, a linear relation is assumed, meaning that a model containing more of the identified elements presents a better solution to the challenges surrounding cloud adoption.

Table 5 shows the elements identified in the previous section, mapping which of the cloud maturity models contain these elements. We see that two of the models, Duarte CMM and AWS CTMM, cover none of the identified elements.

Three of the identified models score in the middle of the pack, containing three to six of the identified elements. The Forrester MCM covers three elements: cloud deployment models, SLA management and a mention of what to migrate. The CCMM mentions the different cloud service models, security aspects, integration and capabilities, although the items in the model are too open to interpretation to justify the lack of an additional assessment tool. CAM holds six of the elements, being cloud deployment models, financial management, SLA management, process

transformation, inferred capabilities and a maturity-grid style assessment. CAM only partially covers cloud service models, as it mentions its focus lies on PaaS and IaaS adoption.

The two best-scoring models are the Weiss CCMM, making mention of seven of the identified elements and for part of the cells the underlying capabilities can be inferred. They lack description of financial management and the cloud service and deployment models, only briefly mentioning them in the paper. CMM3 is by far the most complete option, although it heavily depends on the desired use of the model. It can contain all of the identified elements, but the pick-and-choose nature of the focus areas for certain scenarios makes it liable to omit important areas when performing an assessment.

Requirement	Duarte CMM	Weiss CCMM	CMM3	AWS CTMM	Forrester MCM	CCMM	CAM
Cloud Service Models			•			•	~
Cloud Deployment Models			•		•		•
Financial management			~				•
Security		•	~			•	
Compliance		•	~				
Governance		•	~				
SLA management		•	~		•		•
Migrate what			~		•		
Process management		•	~				•
Integration		•	•			•	
Capabilities		~	~			•	•
Assessment tool		•	•				•
Total	0	7.5	4 to 12	0	3	4	6.5
•: used in model. ~: partial or optional							

Table 5 Comparison of cloud maturity models on identified elements

Table 6 shows the maturity models assessed against for their scientific rigour, following the procedural model of Becker, Knackstedt and Pöppelbuss [16]. Three of the models contain a comparison between existing maturity models and their shortcomings, being Duarte CMM, Weiss CCMM and CAM. However, only the Weiss CCMM makes an effort to compare existing cloud maturity models, rather than identifying the unsuitability of differently scoped maturity models to the cloud computing domain.

In terms of documentation, CMM3 is the only cloud maturity model that presents both the maturity model and required assessment tools, whereas the rest appears to present the model and, in case of Weiss CCMM and CAM, the process of creation. In terms of the Weiss CCMM and CAM, the assessment is done by identifying the position on the maturity grid, but this decision is not explicitly documented.

Requirement	Duarte CMM	WEISS CCMM	CMM3	AWS CTMM	Forrester MCM	CCMM	CAM
Comparison with existing maturity models (R1)	Analysis of existing, but unsatisfactory maturity models Based on outsourcing lifecycle and CMMI-CVS	Existing cloud maturity models are analysed using the procedure model of Becker et al.	None	None	None	None	Literature study of existing, but unsatisfactory maturity models
Iterative procedure (R2)	Not mentioned	Becker et al. procedure model, doing one partial iteration	Development of an initial model through expert opinion Further development through expert feedback (large sample size)	Not mentioned	Not mentioned	Not mentioned	Not mentioned
Evaluation (R3)	Not mentioned	Not performed, but mentioned as a limitation	Feedback from organisations	Not mentioned	Not mentioned	Not mentioned	Mapping of model to case studies used to create the model Systems modelling (simulation of different scenarios)
Multi-methodological procedure (R4)	Literature research on maturity models	Literature research on cloud maturity models	Expert opinion	Vendor expertise	Expert opinion	Expert opinion	Literature research on cloud adoption models Case studies of organisations in cloud transition Expert interviews
Identification of problem relevance (R5)	Limitations of existing maturity models	Derive development guidelines for a future cloud maturity model to assist organisations	Multi-organisational panel with the objective of developing such a model	Clients lack a guidance framework	CIOs face challenges in their cloud computing strategy	Handles required for adoption cloud computing solutions	Existing cloud adoption models lacking elements
Problem definition (R6)	Cloud maturity model based on the outsourcing lifecycle and CMMI-SVC	Need for a scientifically validated and documented cloud maturity model	Framework to guide cloud adoption	Tool for enterprise customers to assess the maturity of their cloud adoption	Operational maturity model for cloud success	Framework for successful cloud implementations	Cloud adoption models fail to address key characteristics
Targeted publication of results (R7)	Conference proceeding (8 pages)	Conference proceeding (15 pages)	Full package of model: questionnaire and description	Whitepaper (23 pages)	Whitepaper (15 pages)	Whitepaper (12 pages)	Master thesis (82 pages)
Scientific documentation (R8)	Methodology partially explained, model partially present Part of groundwork (outsourcing lifecycle applied to cloud) well-documented	Methodology explained and model description	None	None	None	None	Methodology and validation results presented

Table 6 Comparison of cloud maturity models on scientific rigour

The overall conclusion from Table 6 is that two of the scientific models (CAM and Weiss CCMM) are the only ones mentioning the limits of their models. CMM3 is the most complete model, as it offers both a user guide and assessment tool (although not publicly available), whereas all other models offer only a single publication with an often limited description of the model itself.

3.4 Discussion of Assessments

In this section, we discuss each of the identified cloud maturity models based on the above assessment and observations of the models themselves.

3.4.1 Duarte CMM

The Duarte CMM [1] aims to validate the Outsourcing Lifecycle for use in cloud adoption. It is a commendable effort in closing the knowledge gap between traditional outsourcing and cloud computing by using existing models, we must also note that cloud computing and outsourcing definingly different. They share the common characteristic of hosting IT services outside an organisation, but focusing only on this characteristic denies their differences. Compared to traditional outsourcing, cloud computing has the distinguishing characteristics of scalability, service measurement and on-demand self-service. These added characteristics are ignored in the model.

In terms of the performed assessment, the Duarte CMM does not hold up to the identified elements. In the assessment, we see the solidification of the statement that traditional outsourcing models are, in their current form, ill-suited for use in cloud adoption due to the new challenges. They cover the key aspects of IT outsourcing, but fall short when confronting the defining characteristics of cloud computing. Other than that, the Duarte CMM is a conceptual model in its broadest definition, failing to produce neither an actual model nor means of measuring the maturity. The validated list of key activities gives no indication of maturity levels and discards the continuous nature of maturity models. The documentation shows nothing more than a result image of a single assessment, while withholding the overall model and assessment tools tailored to the presented maturity model.

3.4.2 Weiss CCMM

The Weiss CMM [42] uses the procedural model of Becker, Knackstedt and Pöppelbuss [16] and uses this methodology for the first phases, up to the evaluation. It is the only publication that contains a comparison of existing cloud maturity models, coming to the conclusion that there is a need for a scientifically validated and documented cloud maturity model. Additionally, these authors point out that the identified cloud maturity models often concern themselves only with the organisational domain, thereby neglecting the technical challenges associated with cloud adoption.

They propose a cloud computing maturity model that addresses these organisational issues. However, the proposed model treats the following aspects one-sidedly: the focus areas in this proposal are based on the authors' literature study of the identified cloud maturity models after they deemed them as incomplete. By not looking past these identified models, the authors disregard several of the challenges of cloud computing and miss several of the identified elements.

A second critique is in their use of the methodology on which they criticised the identified cloud maturity models. They perform only a literature study to devise their model. Without using a multi-methodological procedure and multiple iterations, the authors fall into the same pitfalls on which they criticised other models.

3.4.3 CMM3

CMM3 [43] is a very versatile model, as it can be customised for each organisation's unique requirements and situation. This, at the same time, is the weak point for the model, because it lacks any form of continuity when new business goals need to be devised with each use. This narrows the scope of the model to a business case level, placing it outside of the strategic scope of this research.

CMM3 definitely has its strong points. When used in its entirety, it is the most complete model available. It has the potential to cover all the bases, although that heavily depends on its specific use.

A critique is that there is no clear method to compare different CMM3 outcomes, as these are heavily reliant on specific use cases and chosen relevant domains. Two organisations, or even separate business units, discussing their CMM3 maturity level might have measured separate domains and even used different control questions. This is caused by is the scope and purpose of the model. It aims to be widely usable, and incorporates ITIL processes, DevOps, IT governance and agile practices in its model, giving it a scope broader than just cloud maturity. As a whole, its size of 25 in-depth focus areas is too large to fit in a useable model.

On the topic of required elements identified, we found that the model either contains all of the elements, or at least a minimum of four. Due to the inconsistent nature of the assessment, there is a large variation based on the specific organisation's business goals.

3.4.4 AWS CTMM

AWS CTMM [44] is one of two models explicitly mentioning the challenges of cloud adoption. It provides a clearly defined task list to achieve cloud adoption, or rather cloud adoption on their platform, but it fails to adhere to the characteristics of maturity models. The AWS CTMM has no means to assess organisational maturity on a gradual scale, but rather offers a task checklist on which an organisation progresses, where completing all tasks means advancing a maturity level.

In terms of the identified elements, the AWS CTMM falls short. Although they explicitly mention the challenges of cloud computing, they do not incorporate them in their model. This shows a lack of focus towards developing a true maturity model and, as such, it appears to be a tool aimed at helping their customers transition. The AWS CTMM is a maturity model in name only, giving a staged approach to cloud adoption. Naming the timeframe for each maturity level gives the impression of good documentation and research, but dismisses the possibility that an organisation could only grows to the third level.

Being an industry model, we see that the AWS CTMM falls short on the scientific grounding as well. It is a tool to assess cloud adoption maturity, an undefined form of maturity, built from their expertise and aimed at their (potential) customers.

3.4.5 Forrester MCM

The Forrester MCM [46] offers a different perspective on cloud maturity, as it gives a decisive division between private and public cloud adoption. While commendable, the overlap in capabilities between the two is neglected, only showing a cumulation of the two in the fifth maturity level.

In its essence, the Forrester MCM is built from two different maturity grids: one for public cloud and one for private cloud. It shows maturity steps in each of these deployment models, but in a very brief manner, around four bullet points per level. Within these, it appears to give a maturity overview of an

organisation without cloud knowledge at level 1, growing to an organisation ready to adopt cloud computing at level 4.

The model offers few pointers for cloud adoption, with a brief introduction on its challenges. The assessment results reflect this, identifying only three of twelve elements and showing a lack of scientific rigour.

3.4.6 CCMM

The CCMM [47] is the only model clearly showing the capabilities on each of the maturity levels. It does, however, not provide a continuous view of one or more focus areas, but rather a diffused perspective on the technological adoption of cloud services.

The model documentation gives no clear description of the model's key enabling capabilities, leaving room for interpretation. It is also unclear which definition of capability they use. Our definition of capabilities –the ability to mobilize and deploy resources to achieve a goal – does not fit with what the CCMM displays in for example Power & Cooling or Modernization.

The model only incorporates four of the twelve identified elements. Due to the contents of the model itself, it is perceived as having a more technical focus than the scope of this study requires. One unanswered question with this model is whether or not there would be differentiation based on the cloud service models or whether this model aims to address all three.

The publication makes no mention of methodology or validation. This convenes with the assessment that the model is lacking in documentation, not on these points, nor on the required explanation of the model contents.

3.4.7 CAM

CAM [26] is solid in its scientific grounding. It applies most of the identified principles, aside from iterative development, and its limitations are documented by the author. The division in milestones and readiness is a clear one, although the terminology is confusing and may as well not exist altogether.

Aside from its scientific rigour, it falls short on the fact that it is only aimed at large organisations and governments wanting to adopt private cloud solutions. This does away with a large body of knowledge on organisations of different sizes or organisations looking towards public cloud or hybrid cloud solutions. While defined as the specific scope of the model, this limitation makes it difficult to retrofit for a greater number of cloud solutions or different sizes of enterprises, due to the specifics of the scope. If the model would be validated in practice, retrofitting might be an option, but its lack of validation gives little base to build on.

CAM also fails to answer an important aspect of cloud adoption: the group of security, governance and compliance. These three form some of the main inhibitors for cloud adoption and should be addressed in a cloud maturity model.

Another curious point is that CAM does not consider the type of applications to migrate to the cloud at which point in the adoption process. Since it exclusively deals with large organisations and governments, we can assume a complex IT landscape with a plethora of applications. Guidelines on

what types of applications to migrate when and how to handle the process of getting there would have been a welcome addition.

3.5 Conclusion

This section discusses the first two subquestions:

RQ1. Which cloud maturity models are available in current scientific literature?

RQ2. What does a model for assessment of cloud maturity models consist of?

Seven cloud maturity models were identified, coming from both scientific literature as well as industry reports. These models were then assessed on the framework developed for this purpose. The framework consists of an assessment of scientific rigour and defining the inclusion of cloud characteristics (deployment and service models), maturity model characteristics (capabilities and assessment) and a set of elements identified in literature (what to migrate, transitioning the IT organisation, integration, financial management, security management, governance, compliance and SLA management).

Only two academic models adhered to the required scientific rigour (Weiss CCMM and CAM), although neither of these were validated. Only one of the identified models covered all of the elements identified in literature (CMM3), but its form is heavily dependent on the use case at hand and thus inconsistent. With the limitations of the Weiss CCMM and CAM, we identify CMM3 as the most usable model available. With CMM3, an organisation's maturity assessment heavily depends on the assessment method used, as organisations gain the freedom to select the maturity levels applicable to their use case. The scope of CMM3 is very broad, and extends itself beyond just cloud adoption and use. It incorporates several best practices from other disciplines, such as ITIL processes. These extensions may or may not be required for cloud adoption. It raises the question of which elements and aspects are required in a cloud maturity model. This question has been partially answered by a literature study, but for a maturity model it is equally important to consult practitioners on the topic.

Although the overall picture is not as positive as expected, we can state that these models do have their merits. With CAM, the addition of milestones to a maturity model would combine the process model and maturity model approaches, possibly satisfying the need of two distinct models in one. That would create a scenario where a roadmap and a maturity model stem from the same assessment procedure, which might be a good step forward, considering the terminological confusion we see in the identified models. However, the model purposefully focuses only on private cloud adoption, and as such is not usable for public or hybrid cloud solutions.

Existing capability frameworks, such as IT-CMF and CMMI-SVC, are used in creating cloud maturity models. CCMM and CMM3 also mention ITIL in its model, and as such we can see that the inspiration for cloud maturity models can be gathered in existing frameworks, adapting them to new technology. Benefits of this approach are that the work is not completely new, and adopting ideas from other frameworks may reduce the workload. On the other hand we see that cloud computing is a disruptive technology, and that its adoption leads to major changes in the way the IT organisation is managed and financed. For example, if you go from an on-premise data center to an IaaS solution, the financial allocations to specific business units could be more precise, the security aspects shift from encryption and safe storage to safe data transfer and access management, and the business processes on that

level change drastically the more you automate. Starting from scratch is most likely not the right answer, but leaning too heavily on existing frameworks might not lead to a new standard that fully leverages the changes and benefits cloud computing can bring to an organisation, as illustrated by the Duarte CMM.

The current state of cloud maturity models is lacking in both scientific and overall completeness. The analyses of the model elements and focus areas are all based on either existing scientific publications or on practitioners' experiences. Only CAM attempted to combine the two, but did not validate the model and only briefly presented the model at the end of the publication, with the note that its narrow scope and lack of verification were its limitations. Instead of relying on existing frameworks, we found that we should first take a step back and ask which elements are required in a cloud maturity model, as has been done in section 3.3.1, and which steps belong to what level of maturity. Complementing the answers to these questions are the existing frameworks, which should be used to add the depth and knowledge of previous research to the developed framework.

4 Delphi Study

This chapter details the Delphi study performed in this research. It describes the design and panel selection process of the Delphi study and each of the four questionnaire rounds. The questionnaire rounds are preceded and interluded by stages of model creation and refinement, in which the cloud maturity model is designed based on input from the Delphi panel and additional external sources.

4.1 Delphi Study

In this section, the Delphi methodology and the application of the Delphi method to the development of the cloud maturity model will be described. The objective of the Delphi study is to gather qualitative data on the subject of cloud maturity, starting with the creation of a conceptual model before consulting a selected group of experts.

4.1.1 Delphi Study

The Delphi method is a widespread and popular methodology in Information Systems research, being a method conceived for use in a setting with incomplete knowledge about a problem or phenomena [48].

The Delphi method originated in the United States Air Force under Project Rand as a method for eliciting and refining group judgements [49]. While originally used to solicit expert opinion on a complex subject, the Delphi method has matured and can be adapted for numerous goals: as a judgement, decision-making or forecasting tool, to gather expert knowledge on a subject with a knowledge gap, or to investigate what does not yet exist [48].

A Delphi study is an iterative process involving a series of questionnaires, each building on the previous one. A Delphi study usually consists of three to four rounds [50], but this could go as low as two and up to five, based on the complexity of the topic, purpose of the research and heterogeneity of the participants [48].

Coates [51] observed:

“The value of the Delphi is not in reporting high reliability consensus data, but rather in alerting the participants to the complexity of issues, by forcing, cajoling, urging, luring them to think, by having them challenge their assumptions.”

This is in contrast with more traditional panels, where consensus is at least desired and sometimes forced, leading to distortions in research data [52].

The classical Delphi study is characterised by four key features:

1. *Anonymity of Delphi participants:* The participants of the Delphi study should be anonymous to one another, allowing them to express their opinions without social pressures towards group conformity [48]. This also reduces the effect of opinions of prominent participants dominating others [50].
2. *Iteration:* A Delphi study consists of two or more survey rounds, where each gives feedback based on previously gathered answers. This allows participants to refine their views during the process. The iteration of data collection allows the gradual formation of group opinion.

3. *Controlled feedback*: The structure of the Delphi method allows the follow-up questionnaires to be based on the answers received in the previous rounds. The input data is received by a study coordinator, who processes this data and eliminates irrelevant information. New questions are then formulated on the received information.
4. *Statistical aggregation of group response*: Delphi questionnaires are designed to allow for quantitative and statistical analysis of the data.

The Delphi method is often modified to suit the specific research circumstances, which leads to the conclusion that the classical Delphi is only one interpretation of its use [48]. Somerville [50] notes that the fourth feature of Delphi studies is structured questioning, foregoing the statistical aggregation, but underlining the goal of gathering qualitative responses.

Although the Delphi method is an excellent method to gather expert opinions on a subject, it has several limitations, which have been considered during this study:

1. *Poor selection of experts*: A danger in the Delphi method would be to have a poor selection of experts, either by only presenting a single point of view (i.e. only cloud providers in this study), or by selecting non-experts.
2. *False consensus*: The consensus achieved in a Delphi study may not be a true consensus, because the method tends to eliminate the more extreme responses. Another cause would be narrow questionnaires, leaving little room for disagreement [50].
3. *Generalising the results to a wider population*: The smaller sample size of Delphi panels means that it is often not representative of the population as a whole. As such, many researchers use several research methods to support a Delphi study [48].
4. *High attrition rate*: Another disadvantage of Delphi studies is the potentially high attrition rate. The method requires thoughtful responses to often lengthy questionnaires and active participation over a longer time span, which could lead to drop-outs in the process [50]. This can be negated by minimising frustration in the use of the surveys, communicating the expected workload clearly, providing swift feedback on the responses and through regular follow-ups with non-responders.

4.1.2 Delphi Study Design

In order to gather meaningful response through the Delphi study, a diverse panel of participants is required. Four groups have been identified to have meaningful knowledge on cloud computing in an organisational context. Respondents would need to fall in one of these four groups to be qualified as experts:

1. *Cloud consumers*: Cloud consumers with an estimated high level of cloud maturity have the required expertise in two possible areas: the transition process of an organisation when adopting cloud computing and the management of an organisation that has adopted cloud computing.
Organisations that are just starting a transition towards cloud computing or those that are in the middle of this process are eliminated from participation, as they would not yet have the required expertise to aid in the initial development of such a model.
2. *Cloud providers*: Cloud providers have experience in helping their customers transition to a cloud environment. They have knowledge on the requirements of cloud computing and

insights from the transition processes of different consumers on different levels of cloud maturity.

3. *Consultants*: Consultants with experience in cloud computing work with multiple cloud consumers in different stages of the process: making an informed decision between cloud computing and traditional outsourcing, creating a cloud strategy and assisting in executing the transition.
4. *Academics*: Researchers with expertise on cloud computing and organisational processes (not only the technical aspects) are aware of state-of-the-art research in this domain and can create links with research that has not found its way into practice yet. They are also not limited by existing processes, which may give different insights into the subject matter.

Although being classified as four groups, the panel composition will be considered homogeneous due to the narrow scope of experts in cloud computing. Cloud computing is a specialised field in which, as most of IT, businesses and academics alike attempt to find and adhere to similar best practices and standards where possible.

Delphi panel sizes generally range from 10 to 30 people in homogeneous groups, with 3 being the lowest number found in literature [48, 50]. This Delphi study aims to find a diverse group of experts, which led to the aim of selecting three to seven participants from the Cloud Consumer and Cloud Provider groups, as they were expected to give the most hands-on experience from practice. Due to the scope of the research, we aimed for eight to fifteen participants.

4.1.2.1 Expert Selection

As mentioned, the quality of the study depends highly on the expertise of the participants. In the previous section we have outlined the four categories of experts: cloud consumers, cloud providers, consultants and academics. A participant in either of these four areas would be required to have expertise on cloud computing from a high organisational level, conforming with the scope of this study.

The expert selection was conducted through a procedure similar to the one used by Okoli and Pawlowski [53]:

1. *Prepare a knowledge resource nomination worksheet (KRNW)*: The purpose of this step is to categorise experts before identifying them. This is done in order to prevent overlooking certain groups with the required expertise. Our KRNW has been described in the previous section. It was formed and agreed upon by the researcher, the research supervisors and two consultants from METRI.
2. *Populating the KRNW with names*: After the KRNW has been created, it has to be populated with names of experts to approach for participation in the Delphi study. The professional network of METRI, which as a consultancy firm has many contacts within the Dutch IT industry, as well as the personal networks of the researcher and supervisors, and an outreach on LinkedIn through the METRI page resulted in a set of 52 experts or organisations with the required expertise in-house.
3. *Inviting experts to the study*: We reached out to all contacts on the longlist through email, telephone or direct meetings. The email contained a short briefing on the research and the Delphi method, as well as the expected time commitment. The email template can be seen in Appendix A.

Out of the 52 contacts, 15 were willing to participate in the Delphi panel. The final division, and their response rate, is shown in Table 7. The first column of Table 7 indicates the four KNRW groups identified, with the second column showing the total number of participants to the Delphi study. Each of the following columns showing the number of experts who completed the surveys for each round. We note that one cloud provider abandoned the surveys before finishing the first round, one consultant and one cloud provider abandoned it after the second round. Other non-participation was excused due to lack of time or being out-of-office, after which we sent out the survey by email to the participants to ensure they were up-to-date with the material.

Group	# participating	Round 1	Round 2	Round 3	Round 4
Cloud consumers	5	5	4	4	4
Cloud providers	6	5	5	4	3
Consultants	3	3	3	2	2
Academics	1	1	1	1	1
Total	15	14	13	11	10

Table 7 Delphi panel composition and participation per group

4.1.2.2 Questionnaire Rounds

The complexity of the topic and the number of unknown factors justifies a Delphi study design in four rounds. Three rounds would be sufficient to develop the model, with the fourth one added to incorporate initial feedback and finish the study with an additional round of input.

The four rounds of the Delphi were defined as follows:

1. *Round 1 – Validation of the conceptual model:* A conceptual cloud maturity model, inspired by expert opinion and literature study, was presented to the Delphi panel for validation. The questionnaire enquired participants for in-depth feedback on each of the elements, as well as their ordering and grouping.
2. *Round 2 – Capabilities brainstorm:* The changes made to the initial model based on the first round were discussed and participants were asked for their opinion on the changes. Then each of the maturity levels were presented with the associated elements, where the experts were to match organisational roles with each maturity level.
3. *Round 3 – Capabilities validation:* The capability areas assembled in the second round were processed into focus areas, with a description for each of the maturity levels for each focus area. The panel was asked to present their views on each of the focus areas in the model.
4. *Round 4 – Model validation:* The focus area descriptions were adapted based on the responses in the third round. The updated focus areas were presented, with their changes highlighted. The participants were asked to comment on the changes.

After each round, the results were analysed. Outliers and answers with unclear motivation would receive a follow-up when required, allowing the participant room to clarify their standpoint. Responses outside the scope or intended direction of the model were addressed in the following questionnaire, with room for further remarks by the panellists. This allowed participants to follow the choices made during the study, as well as attempt to prevent reaching a false consensus by presenting opposing views with a clear rationale.

The questionnaires were administered through Spilter (www.spilter.nl), a group decision support system. Spilter allowed the researcher to fill out a questionnaire with a set of known participants, who were able to view other responses anonymously. Figure 13 shows a set of anonymised answers in Spilter. After closing the questionnaire, the meeting administrator was able to retrieve the answers with the corresponding names of the authors.

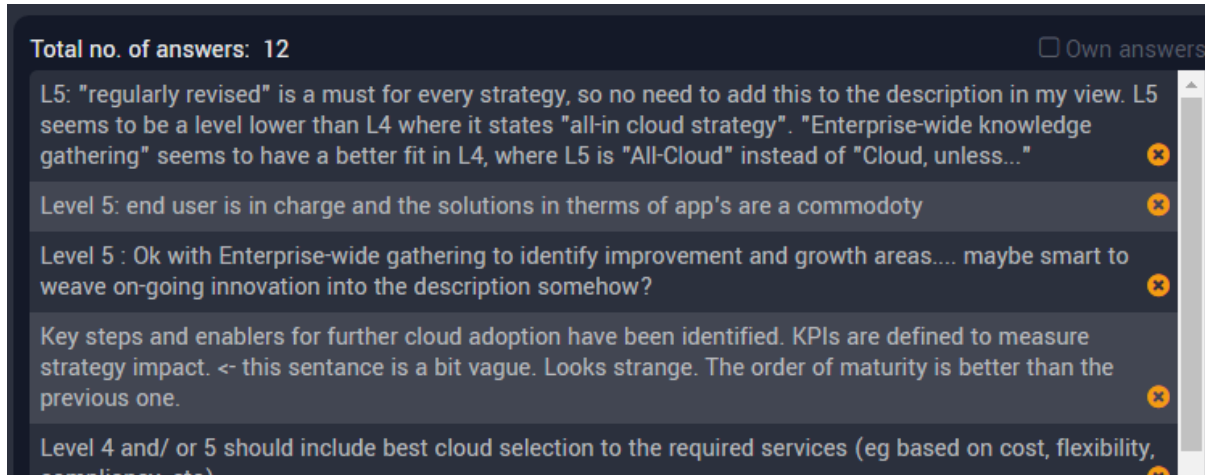


Figure 13 Viewing anonymous answers in Spilter

Each questionnaire had a communicated running time of a week, with an internal deadline of one and a half weeks after sending out the invites. Participants were reminded of the questionnaire twice, once halfway during the week and once the day before the deadline. All but three participants joined each questionnaire or provided reasons for absence for a single Delphi round.

4.1.2.3 Questionnaire Review

Each of the Delphi questionnaires was presented for review to domain experts. The pool of reviewers, while not all approached for each questionnaire, included two business consultants and one research journalist from METRI, and two researchers from the University of Twente.

The feedback received from this group was used to alter the questionnaires, improving their comprehension and presentation quality.

4.2 Conceptual Model

This section describes the process of the initial model creation. The model is based on the conceptual Cloud9 model by METRI. This section starts off with an interview with the creator of Cloud9, followed by the initial model and its justification.

4.2.1 Expert Interview METRI Cloud9 Model

METRI has created the Cloud9 model as a conceptual cloud maturity model for use in their governance consultancy. The interviewee, Michael Chin, is the creator of the Cloud9 model. He immediately expressed that the right ideas were there, but that the model was only a concept. The interview was open-ended, with the intention of asking Chin about each of the elements, as well as their interconnectivity. The interview was conducted on 14 November 2016.

Chin stated that the intended scope of the model is to function as a roadmap for cloud adoption. He found that the clients often had the required capabilities, but lacked knowledge on how to put those to use in adopting cloud solutions.

The usability of the Cloud9 model appeared to be limited, as it had several limitations. Chin described these as follows:

1. *Lack of clearly distinguishable maturity levels:* The maturity levels were not interconnected based on evidence, but followed his gut feeling. Upon further questioning, he agreed that it was possible for organisations to skip maturity levels and follow a path different to the one presented by the model.
2. *Lack of capabilities:* The Cloud9 model only shows a set of elements, with no deeper layer behind them. While the capabilities could be assessed by visiting an organisation, it was impossible to explicitly link specific capabilities to elements in the model.
3. *No reliable method of assessment:* This weakness ties in with the previous issue, as the current method of assessment is a judgement call by a consultant. There is no measure of capabilities, making it impossible to get a reliable, consistent and standardised assessment for two different organisations or moments in time.

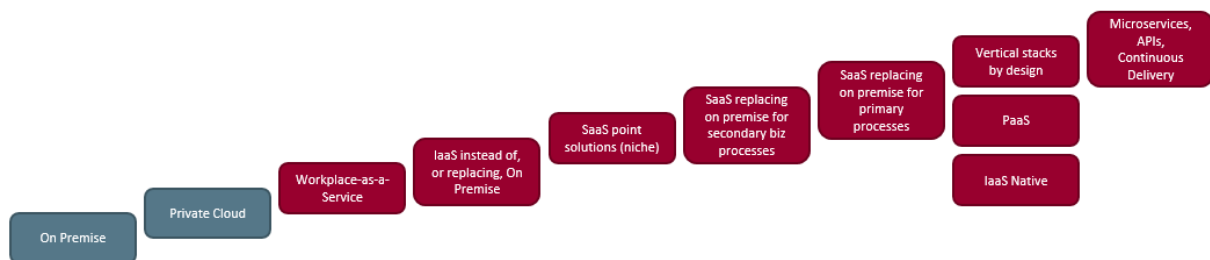


Figure 14 METRI Cloud9 model

The interview then discussed the twelve elements as seen in figure 14, distributed over the nine levels of the Cloud9 model.

On-premises: This maturity level indicates that no cloud services exist within the organisation. It is the baseline state of the model, seen from a perspective where an organisation would start with pure on-premise IT operations.

Private Cloud: Private cloud is the second maturity level in the Cloud9 model. “*Private cloud ... is not really cloud computing*” according to Chin, as it would not be able to leverage the benefits of the public cloud, such as seemingly unlimited scalability and elasticity. His perception of private cloud is that organisations convert their data centers to a private cloud, thereby not leveraging the benefits of the technology past virtualization, and then claiming that they are using cloud computing.

A counterexample to this premise was defined in the interview. An organisation keeping private data and related applications in a private cloud, and move all other processes to the public cloud, would leverage the benefits of the public cloud where possible. This could be due to compliance issues or internal security policies. This led, in discussion, to the conception of the idea that private cloud can be a component in a well-balanced organisational cloud landscape, leading to a hybrid cloud environment or a fully realised private cloud environment, depending on the organisation's requirements.

Workplace-as-a-service (WPaaS): According to Chin, some of the first organisation-wide adoptions of cloud computing are WPaaS solutions, such as Office365 and Google Apps. It was defined as the third maturity level in the model to represent an organic organisational cloud adoption. After further questioning, Chin agreed that WPaaS was essentially a mature form of SaaS.

IaaS instead of, or replacing, on-premises: The fourth maturity level is meant for organisations that have a little cloud experience and are now ready to move their computing infrastructure to a cloud service. The software and management tools are not cloud-ready, and as such do not leverage the biggest benefits of cloud computing. Chin considers it a move in name only, as he describes it as replacing the actual hardware in an already virtualized environment. A major impact of this move would be the change in cost model, switching from capital expense to operational expense.

SaaS point solutions: The fifth maturity level of the Cloud9 model describes the use of SaaS solutions in a non-integrated manner. Chin poses the example of Dropbox in an organisation, as it does not require integration with other applications, but does require several organisational capabilities. It would be one of the first steps in adopting SaaS in the organisation.

SaaS replacing on-premise for secondary business processes: This is a follow-up step in SaaS adoption, where companies would use SaaS solutions for their secondary business processes, e.g. finance and human resources. Chin makes the distinction between moving primary and secondary processes to the cloud based on the assumption that moving primary processes to the cloud is a more risky endeavour for the enterprise. Moving secondary processes first gives an organisation the capabilities and experience required to move their primary processes to the cloud.

SaaS replacing on-premise for primary business processes: The most critical phase in SaaS adoption, requiring the movement of primary business processes to SaaS solutions. Companies need to be certain of their capabilities before starting this process. Chin gave one example of a global company, having round the clock service availability. This requires a seamless transition, which is harder than it would be for secondary processes, where weekend downtime would not be as big an issue.

Vertical stacks by design: Vertical stacks by design represents a paradigm shift in IT management. It requires IT organisations to shift from the traditional layers of infrastructure, supporting software (e.g. operating system) and applications, to a model where business processes create a demand for IT, in which they will look for a solution including all traditional layers for business-defined stacks, such as finance, HR and planning. The full IT landscape will be based on business requirements, rather than having an infrastructure that new applications are placed upon. One example of a vertical stack could be a SaaS solution, where the application is the only thing in need of being managed, whereas other services require a more complex stack solution. This paradigm shift would be the first step towards enabling the use of microservices.

Chin states that, in order to fully utilise vertical stacks by design, an organisation requires the two cloud enablers of PaaS and IaaS Native:

PaaS: The meaning of PaaS here is that PaaS solutions are a fully-fledged platform, following the NIST definition. The idea behind its place in the model is that, in order to fully leverage PaaS, a company needed to be accustomed with cloud services, and would need an infrastructure leveraging cloud benefits.

IaaS Native: With IaaS native Chin refers to the redesign of applications so that they fully leverage the benefits of cloud computing by designing them in a manner that decouples them from their virtualized layers (infrastructure or platform). For a company to utilise PaaS and vertical stacks by design, it requires an architecture optimised for cloud computing.

Microservices, APIs, Continuous delivery: The immediate comment by Chin was that these are not cloud-related items. However, the idea behind this was that there should be a Cloud Walhalla, where these things are made possible through organisational capabilities, upon which he noted that cloud maturity would be an enabler for these processes. Microservices, for example, would require an agile IT organisation that is able to adapt to demand quickly.

We concluded that the Cloud9 model has the right intentions, but could not be used as a basis for a scientific cloud maturity model. Most items in the model have proper justifications, but their interrelation is unclear and based on gut feeling. For these reasons, we decided to start over by creating a new conceptual cloud maturity model, incorporating the good elements from the Cloud9 model.

4.2.2 Conceptual Model

This section describes the creation of the conceptual cloud maturity model to be presented in the first round of the Delphi study, as outlined in section 4.1.2.2.

With the development of the initial, conceptual model, the existing cloud maturity models were considered for inspiration. Using the existing body of knowledge, three candidates were assessed for the possibility of extending them:

- *METRI's Cloud9 model with new elements:* expanding on METRI's existing model and giving it a scientific foundation was the first option. The model follows a clear maturity path, with a clear reasoning in place as to why that path was taken. However, when holding the model against the defined criteria, we found it too limiting in terms of allowing an organisation to define its preferred maturity. An organisation could strive to get as mature as possible with SaaS solutions, while only treating IaaS as a place to run legacy software. METRI's Cloud9 model lacked the required level of granularity to make such decisions.
- *Weiss CCMM:* The Weiss CCMM [42] is a maturity grid containing six dimensions. In the assessment, it contained seven of the identified elements and one was partially in place. It was the most well-constructed model when evaluating it on its scientific rigour, but lacked too many of the identified elements to consider it as a starting point.
- *CMM3:* The third option under consideration was CMM3 [43], which, when used correctly, contained all identified elements. However, the model is very large, having 25 focus areas, and contains much more than we required. Building on this model would first require validation of the existing model, requiring further details of the design choices in its creation. These were unavailable.

Not being able to build on the models identified as most complete, the next logical step was to create a high-level cloud maturity model on which we could base our eventual focus areas. Figure 15 shows a schematic of the construction used in setting up the Delphi study. The goal of the conceptual model is to define the maturity levels, with further rounds giving content to the focus areas and their capabilities. Each maturity level would contain capabilities for each of the maturity levels.

Defining the Vertical Axis

Maturity models come in a grid-based format. In general, the horizontal axis contains the maturity levels and their description, while the vertical axis gives the focus areas. The horizontal axis was defined to constitute of five maturity levels initially, taking the industry standard and changing it if this became necessary later on. Each maturity level implies a growth in organisational capabilities.

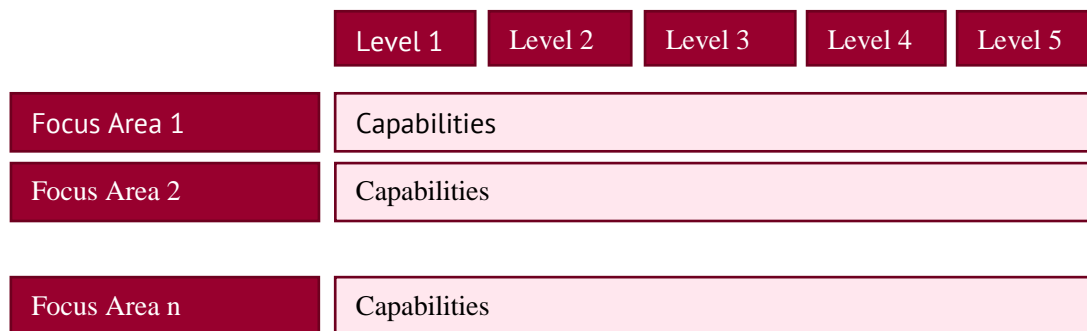


Figure 15 Schematic of the model construction

In order to define an understandable cloud maturity model, the vertical axis was first populated with the three existing cloud service models: IaaS, PaaS, SaaS. They were slightly renamed to Infrastructure, Platform and Software, to clearly create a contextual link between the model and existing components of IT operations. The cloud service models are generally well-understood and some of the most recurring terms for the topic of cloud computing.

Another consideration would be using the cloud deployment models (public/private/hybrid cloud) to define the vertical axis, but this ran into the issue that the adoption of each of the deployment models relied on an organisation's strategy more than on its capabilities. Adopting SaaS solutions on a private or a public cloud platform would in essence be no different.

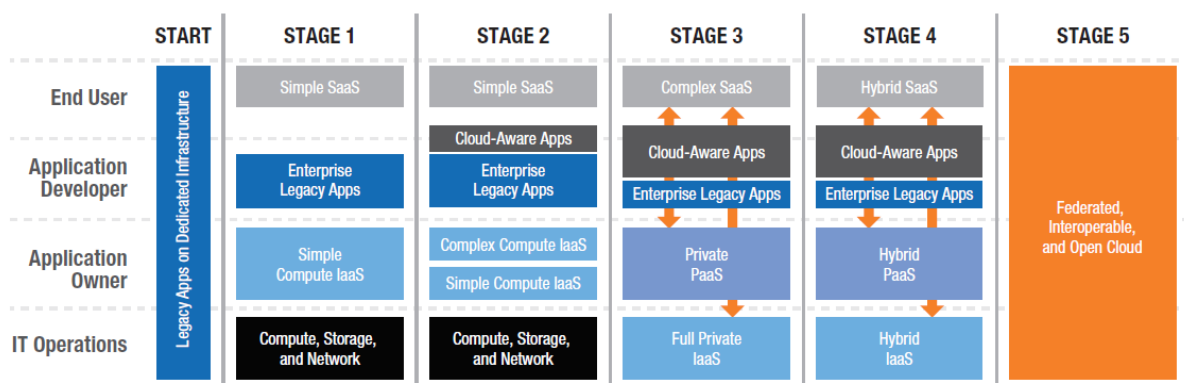


Figure 16 CMM3 roadmap [54]

When investigating the existing cloud maturity models, the CMM3 roadmap, as seen in Figure 16, gave a clear impression of what to include at which maturity level, an approach that would allow us to consolidate METRI's Cloud9 model with a more conventional maturity setup.

Drafting the model elements from METRI's Cloud9 model on five maturity levels meant splitting up the elements according to the three service models. This resulted in the following distinction:

- *Infrastructure*: IaaS instead of, or replacing, on-premise; and IaaS native.
- Platform: PaaS.
- *SaaS*: Workplace-as-a-service; SaaS point solutions (niche); SaaS replacing on-premise for secondary business processes; and SaaS replacing on-premise for primary business processes.
- *Unable to classify*: On-premise; private cloud; and microservices, APIs, continuous delivery.

Although both the infrastructure and software domains showed a growth path, there was a lack of elements. The Cloud Walhalla, as Chin described, could not be fit in these three service models. As such, we expanded on the model and identified two more domains on the vertical axis – illustrated in Figure 17 – meant for guiding purposes and not to be included in the final model. The new elements are described further below in this section.

Solution type	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Virtualization	IaaS replacing on premise		Cloud-native infrastructure	Cloud optimized infrastructure
Platform		Pre-PaaS	Developing with PaaS	Redesigning for PaaS	Cloud optimized PaaS
Software	WPaaS SaaS Point solutions		Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS
Services			APIs	Continuous Delivery	Microservices Virtual Stacks by design
Private/Public cloud	Separated		Integrating		Full Hybrid

Figure 17 First version cloud maturity model with inspirational dimensions

The inspirational domains are Services, containing several of the capabilities linked to those adoption levels, and Private/Public cloud, giving an axis showing the integration level of the different deployment models with one another.

The empty fields are incorporated in the model based on assumed capabilities. For example, developing with PaaS and moving secondary business processes to SaaS require an assumed similar level of cloud maturity, and as such these two have been put in the same maturity level.

Infrastructure

The infrastructure domain consists of four elements: virtualization at level 1; IaaS replacing on-premise at level 2; Cloud-native infrastructure at level 4; and Cloud optimized infrastructure at level 5. The gap in level three is explained through the growth in maturity, as the step from IaaS replacing on-premise to having a cloud-native infrastructure is a rather big one, requiring an architectural overhaul.

Two new elements have been introduced that were not found in the Cloud9 model. Virtualization is not an aspect of cloud computing, but is the basis on which it is built. To make use of the shared computing resources in cloud services, the software needs to run in a virtualized state. For example, AWS's Elastic Compute Cloud (EC2) is a basic IaaS platform in the sense that their infrastructure services host virtualized server instances, making virtualization a requirement for using IaaS.

The second new element is the cloud-optimised infrastructure, indicating that IaaS solutions are optimised for seamless integration between different cloud services. This allows an organisation to use multiple cloud providers with a cloud-native infrastructure.

Platform

Like the infrastructure domain, the platform domain is broken down in four steps: **pre-PaaS** at level 2; **developing with PaaS** at level 3; **redesigning for PaaS** at level 4; and **cloud-optimised PaaS** at level 5. The first maturity level for Platform is empty as that level concerns itself with ad-hoc cloud adoption, where an organisation is presumably not yet working on developing on a cloud platform. All of these elements are new compared to the Cloud9 model.

Pre-PaaS: The full set of application features is deployed on a virtualized environment, either only virtualized or on an IaaS solution. This capability is a first step in moving towards more virtualized resources.

Developing with PaaS: New applications are developed and deployed on a PaaS solution. This will start off with a few initial applications, before moving the more complex development work to PaaS.

Redesigning for PaaS: This step includes the redesign of the current application landscape to run on PaaS, allowing these to leverage the benefits of cloud computing.

Cloud-optimised PaaS: This step allows organisations to benefit fully from PaaS tooling, including automated deployments and orchestration systems locating relevant data and applications in the IT landscape.

Software

The software domain consists of five elements: **WPaaS**, which is a rebranding of SaaS, and **SaaS point solutions** at level 1; SaaS secondary processes at level 3; **SaaS primary processes** at level 4; and **Hybrid SaaS** at level 5. The second level is empty as we identified a gap between the capabilities of level 1, which requires not much in terms of organisational change, and level 3, which would require a strong set of governance tools built on more experience with cloud computing, which can be gained in the infrastructure and platform layers at level 2.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Virtualization	IaaS replacing on premise		Cloud-native infrastructure	Cloud optimized infrastructure
Platform		Pre-PaaS	Developing with PaaS	Redesigning for PaaS	Cloud optimized PaaS
Software	WPaaS SaaS Point solutions		Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS

Figure 18 First version cloud maturity model

The only new element in the software domain is **hybrid SaaS**. **Hybrid SaaS** represents fully leveraging the technological possibilities of seamless integration between public and private cloud environments. Parts with sensitive data, high data transfer or time-sensitivity are hosted on private cloud domains, with seamless integration with software running on public cloud domains to maximise the benefits of cloud computing.

In Conclusion

In this section we have shown and explained the creation of the initial, conceptual cloud maturity model, as shown in Figure 18 without its inspirational layers. This is by no means a fully developed model, but rather meant to spark a conversation about what to implement when. Its aim is to show a

conceptual model inspired by the METRI Cloud9 model, extended with knowledge from the literature review.

4.3 Delphi Round 1

The first Delphi questionnaire was sent out to 13 participants. After the initial survey was sent out, two more participants showed interest in the study, bringing the total to 15. 14 respondents returned the questionnaire on time, with one cloud provider dropping out of the study due to time concerns.

The questionnaire presented the first version of the cloud maturity model to the expert panel. They were asked to comment on the domains on the vertical axis and then on each of the elements of the model. For the latter part, short definitions of each elements were presented. The full questionnaire can be found in Appendix B.

For full disclosure, we discarded comments on specific capabilities as not relevant for the moment, although they would be used in later stages of the study. This is due to the setup of the study and this fact was disclosed to the participants.

This section discusses the responses and changes made to the model after the questionnaire.

4.3.1 The Split in Three Domains

The first set of questions regarded the split in the three cloud domains of **infrastructure**, **platform** and **software**. In general, the distinction of cloud services in these three domains appeared to be a sensible one, with 12 out of 14 participants agreeing with the distinction made. There were some critiques, mainly about the usability of this distinction.

The strict boundaries will disappear overtime. Like the Functions and Lambda functionality in Google and AWS as an example.

Infra, Platform and Software make sense on an on-premise or virtual environment. Today on the cloud there are so many services that trying to categorise the Cloud in 3 domains is too restrictive.

Whilst the difference between IaaS PaaS and SaaS is clear, I would suggest a more application centric approach, looking at the various App tiers/layers: infrastructure, frontend, middleware, backend.

One remark, at the end of the survey, showed a different perspective altogether.

I would change the model itself. A classification like that makes sense if you're conducting a market analysis to classify different Cloud providers, but from an organization/customer point of view the maturity is more related to the adoption than to the kind of components, blocks and services used.

While understandable, this model was intended as a first attempt at creating a roadmap for cloud adoption. These critiques were taken into account, but ultimately the decision was made to move forward with the existing division based on the high level of consensus between the participants. The proposed view was one of capabilities, something that this model would expand on later in the study.

4.3.2 Infrastructure Domain

After the split in three domains, the participants were asked to comment on the infrastructure domain as a whole and on each of the individual elements. Figure 19 demonstrates the visualisation of this domain accompanying these questions.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Virtualization	IaaS replacing on premise		Cloud-native infrastructure	Cloud optimized infrastructure

Figure 19 Infrastructure domain

Virtualization was included as a prerequisite for adopting a cloud infrastructure. It was defined as leveraging virtualization techniques across data centers. This was generally well-understood by the panel, as these responses stated.

Its purpose in a cloud maturity overview is to offset, to show where people are coming from.

Virtualization is almost a necessary step for a cloud migration; otherwise a redesign is needed before any cloud transition is possible.

There was one comment based on the experience from a cloud provider that showed a critique to this assumption.

It could be one of the first steps, but in our experience we have found that some customers migrate workloads directly from on-premise to the cloud without virtualizing it.

Aside from this comment, the other participants agreed that virtualization was a prerequisite for cloud computing.

IaaS replacing on-premise is the second step in the infrastructure cloud maturity, defined as private and public cloud IaaS solutions replace the on-premise infrastructure. The architecture as-is is being moved on top of an IaaS solution. This step was subscribed by the panel to be the next step in infrastructure maturity, although the wording of the element appeared to be confusing. **IaaS replacing on-premise** implied that the infrastructure would move away from an on-premise location, whereas a private cloud could be hosted on-premise and still allow an organisation to reap the benefits of moving towards an IaaS service model. This appeared to be a discrepancy between the element and its definition.

The third element, **cloud-native infrastructure**, was defined as the architecture being redesigned to leverage IaaS benefits. It was agreed to be the following step in infrastructure maturity. Aside from agreeing, there appeared to be a consensus that a clear definition of what a cloud-native infrastructure entails was required, with two responses providing a clear step towards a better definition.

To me, cloud native infrastructure is a "fully abstracted infrastructure, including storage, networking and compute layers which can be consumed on-demand and programmatically."

Cloud Native infrastructure focuses on infrastructure that can be easily used in cloud environment. So all items are ready to be automated fully. Have open API's. Can scale

by adding components and are only providing the functions one might expect in that layer.

Another remark was that, at this point in the model, the hard distinction in the three cloud domains became less suitable.

Cloud-native infrastructure should not be seen as an isolated part of the Cloud but should integrate with the platform and software layer.

The fourth and final element of infrastructure maturity is **cloud optimized infrastructure**, which was defined as the deployment of complex IaaS services across multiple cloud domains (both private and public), where the IaaS solutions are optimised for seamless integration between the different cloud services. The general consensus on this element was one of agreement, although several experts marked the element as too vague, requiring a better definition. One respondent presented his own definition, while another commented on the fact that there were two ill-defined elements in a row.

Cloud-optimised infrastructure (COI) support the way to leverage Cloud services from Cloud Service Providers to obtain the right services for the right price(model) in respect to legislation.

To me the definitions are too vague and the difference between L4 and L5 is arbitrary in its current setup.

The final question for the infrastructure domain focused on reflections on the domain as a whole. Several users commented on the inclusion of a physical component in the infrastructure domain, which is beyond the scope of cloud computing, and one response suggested adding an extra level.

Infrastructure Level 0 - physical server infrastructure (legacy) due. It's not really a cloud domain but is always a factor that plays a role towards Cloud.

4.3.3 Platform Domain

The second domain presented was the platform domain. The participants were asked to comment on each of the elements and the domain as a whole. The full domain is depicted in Figure 20.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Platform		Pre-PaaS	Developing with PaaS	Redesigning for PaaS	Cloud optimized PaaS

Figure 20 Platform domain

With level 1 being empty, the first element of the platform domain is **pre-PaaS**. **Pre-PaaS** is introduced as deploying the full application stack on IaaS as a first level of PaaS maturity. The consensus here was that this maturity step is not a part of PaaS and does not fit into the PaaS adoption cycle. Although some respondents commented that this is a logical way of introducing a new technology, we subscribed the notion that this is ill-suited to be a part of PaaS maturity.

[...] for me the first step is clearly to develop one single application on PaaS.

Developing with PaaS is the second maturity step in the platform domain. This step was agreed upon with the panel, with some suggestions for nuance, as to provide a more gradual maturity approach instead of a leap towards using a new technology at once altogether.

Using PaaS components in the ALM (Application Lifecycle Management) makes that the code that is running on production at least complies with the way the PaaS components work (e.g. CI/CD pipeline). This gives unity in working. So the availability of these components makes it a bit more mature. Using these features is totally up to the user and not to the provider. So I would change the level 3 maturity in "Development PaaS features available".

The third step in platform maturity is **redesigning for PaaS**, aiming to enunciate that existing applications require rework to be fully compatible with PaaS features and functionalities. This step got a mixed reception, both on its definition as well as its statement as a whole. It appears that the differentiation in maturity between levels 3 and 4 is unclear and that they can be performed in any order. A further point was that redesigning was often a costly approach and that rebuilding part of the application landscape may be cheaper than redesigning it.

"Redesigning for.." is not a concrete state which an organisation can be in. It could be they are also redesigning when they are in level 3 "Developing with PaaS".

For apps that have a long life span this might be an option that has benefits. Sometimes starting all over is more mature than redesigning. I tend to not agree here.

Developing with PaaS and Redesigning for PaaS shouldn't be considered different levels. In practise this is a parallel approach, it's not a chronological step.

The final step is **cloud optimized PaaS**, presented as automated deployments, with orchestration systems locating relevant data and applications in the cloud landscape, and migrating them according to business requirements. Whereas eight of the experts agreed, the remaining answers were focused on the definition and its suitability at the highest level of maturity.

Automated deployments are not PaaS specific. We run automated deployments without PaaS, so I don't agree with the definition. To me, it seems the maturity model is somehow conveying that moving to level 5 on Platform is the highest achievable point in maturity, which it should not be.

Again, taking an application centric approach, I would say that level 5 would be that PaaS is used to replace as many components in the App stack as possible, to optimize for application delivery.

When reflecting on the platform domain as a whole, one suggestion was to add a step between **pre-PaaS** and **developing with PaaS**: migrate on-premise applications to PaaS without redesign. This would smooth the adoption curve and present a clearer maturity path. This was taken into account in the revised model.

4.3.4 Software Domain

The third domain is the software domain. The participants were once again asked to comment on each of the elements and the domain as a whole. The full domain is depicted in Figure 21.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Software	WPaaS		Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS
	SaaS Point solutions				

Figure 21 Software Domain

The software domain starts off with two elements in the first level: **WPaaS** and **SaaS point solutions**. **WPaaS** is defined as a set of standardised workplace tools (i.e. Office365 or Google Suite) and have low implementation requirements, as they are mature cloud offerings and generally a natural next step for the applications already in use. The experts were divided on this issue, with some struggling with the definition by mentioning hardware in their responses, and others mentioning the change in business processes when adopting WPaaS. In general, the definition appeared to be unclear, giving rise to the question whether or not we meant virtual workstations or merely the applications being used.

SaaS point solutions are the second element in the first level of software maturity. It was defined as SaaS solutions adopted for a single business use, which requires little to no integration with the existing application landscape. There was consensus that these offerings were indeed a first step in SaaS adoption, albeit unclear what type of solutions were meant with its definition.

Agreed, upon the condition that there is no integration with the existing business landscape. I cannot think of an example of a solution that does not have any touch point with other areas of the business right now so would be interested to have an example.

The second level of the software domain contains no elements, making the next element **secondary processes SaaS**. It is defined as secondary business processes, such as Finance and HR, migrate to SaaS solutions. The distinction between secondary and primary processes was made as to the risk level of their adoption, where for example financial administration could recover from a day of downtime in a bad scenario, the losses for primary processes being unsupported by their applications would possibly grind the organisation to a halt. This reasoning was subscribed by the experts.

Through the maturity and experience there is less objection to cloud at this stage and it's the right moment to touch upon major process areas such as Finance (and HR, etc.). This part seems particularly interesting to me as you will find often the internal sponsors for the next level of adoption. Good time to start evaluating a centre of excellence early on.

Primary processes SaaS is the fourth element in the software domain. It has been defined as primary business processes are moved to the cloud, requiring more organisational capabilities than secondary processes. The reasoning from the previous element applied here, once again being supported by the experts.

Now that important secondary processes have been migrated the tangible benefits can be calculated and the ROI demonstrated. This allows for very good transparency in the to be expected ROI and business benefits, so that primary process inclusion becomes a given.

The final element in the software domain is **hybrid SaaS**, defined as fully leveraging technological possibilities of seamless integration between public and private clouds. Parts of application landscape containing sensitive data, time-sensitive processes or data-heavy processes can be hosted on a private cloud, with seamless integration with applications in public clouds. Although there was no consensus on the element, this was mostly due to debate on the definition and placement of the elements. The experts did agree that a hybrid cloud was the logical final step in the maturity path.

To me, this is more a description of running your own apps on a cloud platform, rather than consuming a SaaS service and integrating it with other apps/platforms

The hybrid concept seems like a step forward from secondary and primary process on the cloud. Why should data and time sensitive processes be private and others public?

Although it is more complex it does not have to mean the next level in maturity.

Finally, the respondents were asked to reflect on the software domain as a whole. Some remarks were made towards the maturity levels and how they could be expanded upon.

Hybrid SaaS is the ultimate 'end-state'. Something before Hybrid SaaS with iPaaS [Integration Platform-as-a-Service, ed.] could be an independent maturity stage.

SaaS has a huge ecosystem, for instance services that can be bought to integrate product X with product Y. This to me is very much part of the most mature SaaS level, where everything is done based of services that are procured, rather than built.

You could argue that SaaS point solutions is more level 2, and that some business process will skip level 1 and 2 completely. (The natural progression for level 1 to 5 feels stronger in case of Infrastructure and Platform)

4.3.5 Revised Model

Based on the response received, the initial model has been redesigned, as shown in Figure 22.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Legacy apps on dedicated infrastructure	IaaS replacing on premise		Cloud-native infrastructure	Cloud-optimized infrastructure
Platform			PaaS development Application stack on PaaS	Redesigned applications for PaaS	Cloud-optimized PaaS
Software		Mature cloud solutions SaaS Point solutions	Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS

Figure 22 Revised cloud maturity model

The first maturity level has been overhauled, now being a cross-domain element called legacy apps on dedicated infrastructure. This supports the notion that only the infrastructure layer showed a relatable starting point with virtualization.

For the infrastructure domain, virtualization was removed from level 1 and replaced with the new cross-domain element. The rest of the domain remained in place, with updates to the following definitions:

IaaS replacing on-premise: The full application landscape will be running on a public or private IaaS. This indicates a move of the virtualized infrastructure to a cloud computing platform, stripping away the requirement for owning and maintaining a physical infrastructure for those involved in hosting applications.

Cloud-native infrastructure: A cloud-native infrastructure means that the organisation will be able to deploy IaaS services across managed service providers and private clouds providing IaaS services. It consists of a fully abstracted infrastructure, in which all components can be managed through APIs.

For the platform domain, pre-PaaS was removed for not being part of PaaS maturity. This leaves level 2 empty for the platform domain. The third level sees the addition of application stack on PaaS, with developing with PaaS renamed to PaaS development. Redesigning for PaaS was renamed redesigned applications for PaaS at level 4. The following definitions are updated:

Application stack on PaaS: The application stack is deployed on PaaS solutions where possible, not yet leveraging its benefits.

Redesigning for PaaS: The modification of the current IT landscape to optimally leverage the benefits of cloud computing.

The software domain sees the renaming of WPaaS to mature cloud solutions as level 2, otherwise remaining the same. The following definitions have been updated:

Mature cloud solutions: Mature SaaS offerings are adopted in the organisation, hardly impacting business processes, but moving software solutions to a cloud environment nonetheless (e.g. Office365, Google Suite).

Hybrid SaaS: Fully leveraging the technological possibilities of seamless integration between public and private cloud environments. Parts of the application landscape with sensitive data, high data transfer or time-sensitivity are hosted on private cloud domains, with seamless integration with software running on public cloud domains to maximise the benefits of cloud computing.

4.4 Delphi Round 2

The second round of the Delphi study was sent out to 14 participants, out of whom 13 completed the survey. One was unable to participate, but was filled in on the contents before the third round of the study.

The questionnaire presented the updated version of the cloud maturity model from the first round, with questions regarding the validity of the changes. It expanded on the initial model through short descriptions of a fictional company for each of the maturity stages. The latter part questioned the panel on the capabilities associated with each maturity level. The full questionnaire can be found in Appendix C.

This section discusses the responses to the revised model, the input on capabilities for each maturity level and the redesign of the model after the questionnaire.

4.4.1 Response on Round 1 Changes

The questionnaire started off by presenting the changes made to the model after round 1, as described in section 4.3.5. The panel commented on each of the maturity levels, grouping several elements into one answer to limit questionnaire length. Although the general consensus appears worse for this iteration than the previous one, one expert observed that it was not as clearly communicated this time that this model was meant to elicit capabilities and not intended to be the final model, something which was more explicitly communicated and apparently well-understood in the first questionnaire.

Introducing the redesigned first maturity level was met with mixed opinions. The experts either agreed or disagreed on the suitability of incorporating such a starting point to the maturity model. If

this were to be changed, the disagreeing responses stated that this level should be level 0 rather than level 1.

The second maturity level, containing the reworded element mature cloud solutions, was met with mixed reactions as well. The description of the fictional company included several examples and the disagreeing comments were aimed at these examples, providing counterexamples of applications that could fit at the same or different maturity levels. One response took a swing at the model as a whole, stating that this was a roadmap, not a fully developed maturity model.

At [my previous employer] we had [a cloud CRM] implemented before we had IAAS, does that mean that we were at level 5? I think the model should not confuse a scenario with a progression.

The third maturity level garnered slightly more agreement. The fictional company description was not seen as helpful and was criticised again as being only a single scenario of an organisation adopting cloud. Another contested point was the split in primary and secondary processes, leading to questions about the maturity path.

The split between primary and secondary processes is probably done for risk mitigation purposes. If the move to Cloud goes south, then it 'only' hits our businesses secondary processes. The 'new' organisations skip this step and move primary processes in the same speed as the secondary. I agree that a lot of 'bigger' companies might follow this strategy though.

The fourth maturity level was met with a moderately positive response. Once again, there was a dispute on the definition of the elements. Redesigned applications for PaaS was criticised as being too simple a definition.

I am in doubt about the full cloud native [element]. I agree that it is more mature, but I think it is not possible to become fully cloud native without touching the application stack. And having that said, some apps just cannot be moved to a cloud.

Most experts agreed that Level 5 was correct in its current form, as it came with only minor changes to the provided definitions. Here too, however, we saw an emerging need for defining the required capabilities associated with this model, moving away from the generic elements and short descriptions.

In my opinion it is much more about how the organisation has adopted cloud principles: consume what you need, stop what you don't need, elasticity, programmatic control of the cloud, etc. These topics should perhaps be in [level] 1 to 5 as well.

4.4.2 Focus Area Brainstorm

The second part of this questionnaire was structured as an asynchronous brainstorm session focused on gathering the associated organisational capabilities for each of the maturity levels. This brainstorm session came with a set of roles and capability areas from METRI's model of IT roles and capabilities, used to give guidance to the brainstorm. This list is included in the questionnaire in Appendix C. The experts were asked to consider, but not feel limited by, these capability areas.

In response, a large selection of capability areas was given for each of the maturity levels. Table 8 shows a traceability matrix of these capability areas and their mentions at specific maturity levels.

These results have been grouped accordingly to limit the number of capability areas. As seen, not one capability was mentioned on all of the levels, and most were mentioned more than once, showing the relevance of these capability areas in multiple levels of maturity. At specific levels, the experts mentioned more specific capabilities (e.g. virtualization at level 1 for infrastructure).

Capability area/Level	1	2	3	4	5
Agile					
Business Process Management					
Change management					
Compliance					
Cost management					
Data management					
Enterprise Architecture					
Governance					
(on-premise) Infrastructure					
Operations					
Organisational understanding					
Portfolio management					
Program management					
Project management					
Risk management					
Security management					
Service integration and management					
Software development					
Strategy					
Vendor management					

Table 8 Traceability matrix of capabilities and maturity levels

What stands out is the division between levels 1-2 and levels 3-5. The capability areas of organisational understanding, risk management, security management and vendor management are only mentioned at levels 1 or 2, whereas cost management, portfolio management, program management, project management and software development are only mentioned at levels 3 and up. This indicates either a possible increased/decreased relevance of developing some capability areas at higher maturity, or a split conceived by the model structure on which the brainstorm is based.

These results were then combined with findings from literature to create the expanded cloud maturity model.

4.4.3 Expanded Cloud Maturity Model

This section describes the consolidation of capability areas into focus areas and defines the focus areas and their maturity path.

4.4.3.1 Consolidating Capability Areas

In order to expand the cloud maturity model, there was a need to define the focus areas of this model. The 22 capability areas mentioned in Table 8, now with the inclusion of the software and platform from the model they were elicited from, contained considerable overlap with the required elements

identified in the previous assessment of maturity models (section 3.3.1). In an attempt to consolidate the number of capability areas some were combined based on the contents of the capabilities proposed by the experts. Added to these were the elements defined in literature, as described in section 3.3.2, to show that all of these were covered in the expanded cloud maturity model. Table 9 gives an overview of the combinations of these capability areas.

Old capability areas	Literature elements	New focus area
Business Process Management	Process management	Business Process Management
Strategy; Organisational understanding		Cloud strategy
Compliance	Compliance	Compliance
Data management; Service integration and management	Integration	Data management
Cost management; Program management	Financial management	Financial
Governance	Governance	Governance
(On-premise) infrastructure; Change management; Portfolio management	Cloud service models	Infrastructure
Enterprise architecture; Program management; Service integration and management	Integration	IT architecture
Operations; Program management; Project management; Portfolio management		Operations
Change management; Service integration and management; Portfolio management	Cloud service models	Platform
Security management; Risk management	Security	Security
Change management; Service integration and management; Portfolio management	Cloud service models	Software
Software development; Agile		Software Development
Vendor management	SLA management	Vendor management

Table 9 Consolidating capability areas to focus areas

Not all elements defined in the literature study are found in the expanded model. The cloud deployment models, what to migrate, capabilities and assessment tool are not defined. They are found to be irrelevant in terms of capabilities (deployment models), already addressed with the roadmap

(deployment models, what to migrate) or parts of a maturity model and not related to focus areas (capabilities, assessment tool). The capabilities will be addressed in the maturity descriptions of each of the focus areas and the assessment tool will be built on these descriptions later in this study.

In the following description, the different types of elements have been colour coded as **capability areas mentioned by the experts**, **literature identified elements** and the **final focus areas**.

Organisational understanding concerned the communication of the cloud strategy to different levels of the organisation. This, combined with the **strategy** capability area, was consolidated to the focus area **cloud strategy**.

Service integration and management (SIAM) concerns itself with managing and integrating separate IT services to provide a single business-facing IT organisation. Due to its general meaning and lack of cloud-related specifics, parts of this capability area were found in the **data management**, **IT architecture**, **platform** and **software** focus areas. Because of its diversity and because the areas where SIAM was identified covered the capabilities mentioned by the experts, the decision was made to integrate SIAM in these separate focus areas.

Change management was mentioned in terms of adopting new technologies. The mentioned capabilities (train infrastructure, buy before build (adopting COTS SaaS), and educate on new software and processes) could be grouped under the three focus areas of **software**, **platform** and **infrastructure**. Change management is an integral part of cloud adoption, with the goal of this model being an aide in that process. The actual organisational change management is out of scope and more scenario-based.

Project management, concerning itself with the management of individual projects, was mentioned at level 5 only, with the capability of cloud consumption on demand only. This capability falls under operations, who eventually would perform the demand management role.

Program management is the discipline of managing a set of projects related to each other under the umbrella of one program, with the intention of improving an organisation's performance. Its main mention in the questionnaire response was smart decision making in cloud management a maturity level 5. This was incorporated in the **financial**, **IT architecture** and **operations** focus areas.

Portfolio management, focusing on managing the total set of programs and projects, is another capability area that was split and added to several focus areas. The mentioned capabilities focused on service registration and monitoring, which falls, with different specifics, under **operations**, **software**, **platform** and **infrastructure**.

Risk management was only mentioned at level 1, naming preparation and understanding as the specifics for that level. Due to the nature of **security management** and it being intertwined with risk management, the two were grouped in the focus area of **security**.

Agile is a well-known part of software development philosophy and has become a new paradigm in recent years, often replacing traditional development methodologies. As agile development is a part of software development, the two have been consolidated in the focus area of **software development**.

Of the elements identified in literature, only integration and SLA management is not a direct mapping to a focus area. **Integration** is one aspect frequently mentioned throughout the focus areas, as can be seen with SIAM. However, if done correctly, it will be planned for in the **IT architecture**.

4.4.3.2 Defining Focus Areas and their Maturity

After consolidating the capability areas into focus areas, the focus areas were defined and the impact of cloud computing on each was described. Each focus area required a maturity path, filling out all five maturity levels. As stated in the conclusion of chapter 3, existing frameworks should be used to complement the defined baseline. The maturity paths are based on scientific literature, industry reports and the questionnaire results. Knowledge gaps had to be filled in, to later be verified in the following Delphi rounds.

Business Process Management

Business process management (BPM) focuses on improving corporate performance by managing and optimising an organisation's business processes [55]. In the perspective of cloud computing, this means managing and optimising changing business processes due to the introduction of new and often more standardised software, and thus business processes. Software customisation is gradually becoming a thing of the past with SaaS as a new software delivery model, making it critical for organisations to adapt their processes to these standards if they want to keep up-to-date. In addition to that, (parts of) business processes are now performed by third parties (e.g. payroll management), making it a key factor to integrate these partners and their business processes to the organisation's.

The maturity path of the BPM focus area was inspired by the Business Process Maturity Model (BPMM) [56], which uses the following maturity path:

- Level 1. No business processes have been defined.
- Level 2. Work units are structured.
- Level 3. Common organisational processes are defined to achieve consistency.
- Level 4. The process infrastructure and associated process assets are leveraged to achieve predictable results with controlled variation.
- Level 5. The organisation's processes and its resulting products and services are continuously improved through defect and problem prevention and planned improvements.

Our focus lied on the impact of cloud maturity on BPM, rather than on BPM maturity itself. Findings other than the BPMM focused on the impact of the new technology on BPM, rather than the influence on the processes itself. This left a knowledge gap regarding the impact of cloud computing on BPM. With this knowledge gap, the following maturity path for BPM was defined through a combination of the BPMM, response to the questionnaire and a general understanding of the topic:

- Level 1. Some business process (BP) chains are documented, showing involved IT elements.
- Level 2. Every BP is documented with its underlying IT systems, SLAs and Operating Level Agreements (OLA) for handling transactions. Some element interfaces underpinning the business process are documented.

- Level 3. Common elements are aligned from a semantics and data handling perspective. A migration and consolidation plan is created for processes moving to the cloud. Moving processes are adapted to fit COTS solutions where possible. Common semantics are applied to systems and well-documented interface characteristics enable dynamic messaging queue interaction.
- Level 4. Performance of common IT elements is measured in the combined BPs, with alerting in place for performance thresholds. Systems are categorized and located according to the data they hold for the BPs. Application elements underlying BPs are designed according to well-documented cloud-native models and frameworks.
- Level 5. IT elements underlying the BP are automatically tested and monitored on IT metrics. Processes are regularly updated to align with business objectives more effectively. Automatic system scaling according to real-time BP needs. BP testing and monitoring is automated. Ad hoc BPs are designed, implemented, and monitored with supporting microservices, and eventually retired.

Cloud Strategy

A cloud strategy is the plan detailing objectives, principles and tactics for leveraging cloud computing as part of the overall IT strategy (and in support of an organisation's business strategy). It provides guidance for all levels of the organisation by communicating the organisational vision on cloud computing and its implementation and future use within the organisation.

The Fisher Business Process Maturity Model (Fisher BPMM) [57] contains strategy as one of its dimensions, giving the following maturity path:

- Level 1. Reactive to market conditions (1-2 years), driven by cost and efficiency.
- Level 2. Adapt/react to market conditions (within a year). Initial integration with partners.
- Level 3. Adapt/react to market conditions (3-6 months). The business process is a foundational element of the enterprise.
- Level 4. Adaptive to market dynamics within weeks. The enterprise is organised completely around processes. Optimised processes and execution yield a competitive advantage.
- Level 5. Predictive capabilities and market analysis. Continuously adaptive to market dynamics in near real-time. Enterprise and its partners organised around processes.

Although its focus mainly lies on business process maturity, the Fisher BPMM gave pointers on strategic maturity. The cloud maturity model initially does not concern itself with market conditions, as the decision to adopt cloud services is made before the model comes into play, the predictive capabilities do fit with higher maturity. Another point from this maturity path was that, with higher maturity, the focus shifted from a careful, introducing strategy to an all-in strategy. This notion is supported by the questionnaire results.

The questionnaire results mentioned the adoption of a cloud strategy with accompanying company objectives and a defined migration path as the starting point for this focus area. When combined with organisational understanding, the logical first goal became the creation and communication of the cloud strategy itself. This claim is supported by the enterprise strategy focus area of CMM3 [54]. The

higher maturity focused itself on the lessons from the Fisher BPMM [57], giving the following maturity path for cloud strategy:

- Level 1. Different views on cloud computing exist, with some common understanding of the business benefits of adopting cloud.
- Level 2. Common enterprise-wide cloud strategy exists, but ad hoc adoption of cloud services. Impact of cloud services on organisation has been identified.
- Level 3. Key steps and enablers for further cloud adoption have been identified. KPIs are defined to measure strategy impact.
- Level 4. All-in cloud strategy guides all new deployments and cloud services. Use and success of implementing cloud strategy is reviewed on KPIs.
- Level 5. Enterprise-wide knowledge gathering to identify improvement and growth areas. Cloud strategy enables growth and optimization of business outcomes and is regularly revised for technological developments.

Compliance

With the IT landscape and its regulations becoming increasingly complex and punishments for non-compliance becoming harsher, conforming with rules and regulations is of the utmost importance. One example is the new data protection law of the European Union, going into effect mid 2018 with penalties of up to 4% of annual revenue [58]. With cloud computing, new compliance issues arise when the hosting of IT systems and services is no longer under control of the organisation. For example, ensuring data residency in the country of origin might be an issue that arises when using a public cloud service, requiring new, cloud-related skills in the area of compliance management.

Yimam and Fernandez [59] identified six issues with cloud compliance: complexity of the regulations; overlap in regulations; lack of standard reference architectures; lack of full control and transparency; security threats; and an overlap with security. The complexity and overlap in regulations is something all organisations have to manage through clear policies on cloud compliance. Second, a lack of a standard reference architecture can be partially countered through due diligence and the creation of an internal compliance framework. The third set of issues, security threats and an overlap with security, can be managed through a solid architecture using best practices and good communication between compliance and security specialists.

The creation of a compliance framework to address the issues noted above appeared to be the main line in the maturity path. After defining the framework, it should be communicated internally and, eventually, externally, as the cloud ecosystem needs to be compliant over time [60]. At the same time, further automation in the tooling becomes available, allowing noncompliance to be automatically detected [61]. This gives the following maturity path:

- Level 1. No corporate policies or guidelines related to cloud computing are readily available.
- Level 2. Compliance requirements are made available and communicated. The compliance framework is redefined to be cloud-aware. Implementations of cloud services follow predefined procedures to ensure compliance.

- Level 3. Processes are in place to check selected areas for compliance regularly and consequences of deviation are analysed. Internal management reports are linked to each of the transitioning cloud services.
- Level 4. Compliance requirements are communicated to the ecosystem in a standardised format. Online management and monitoring systems are in place, events of non-compliance are defined automatically where possible. Compliance-aware management tools support real-time monitoring.
- Level 5. Compliance communications now has corresponding feedback loops. Corrective and preventative measures are taken based on automatic analysis. Continuous improvement of used framework, analysis and communication methods.

Data management

The practice of data management concerns itself with the architectural techniques, tools and practices for achieving consistent delivery of data across the organisation in order to meet the data consumption requirements of all applications and business processes [62]. Furthermore, it requires data access and availability controls to ensure secure and compliant use of data. With cloud computing, the more distributed nature of the IT landscape comes with new challenges, such as data access, duplication, consistency and residency.

As a combination of the data management and SIAM capability areas, the data management focus area centers on the creation of a data management framework, data classification and the challenges listed above [63]. Integration, data access and discovery through APIs were key enablers for a hybrid cloud landscape. These are becoming more relevant in the later maturity stages [54]. The resulting maturity path was as follows:

- Level 1. Limited data access and availability controls exist. Internal criteria and controls exist for managing data. Data management requires human knowledge of data and location.
- Level 2. A limited number of applications use cloud management services. Data management processes are documented in a data management framework and information sharing policies are defined. An enterprise data management function manages key master data sources. Standardised access to data repositories is realised.
- Level 3. A published data management framework exists, policies are enforced. Data access and availability controls are consistently applied across the organisation. A central set of database technologies are implemented to support a scale out database architecture. Data object access through APIs is emerging.
- Level 4. Metadata is encoded and stored in a CMS/data warehouse. Management processes are based on storage and business metadata. Access and availability of data are continually reviewed. Applications use cloud-based data services. Real-time access to data through managed access points. Semantic search engine capabilities available to support data analysis.
- Level 5. The data management framework is an integral part of the overall operating model. Information access and data security controls are integrated in the data ecosystem. Data services supporting applications are behind access APIs. An enterprise-wide data lake

has been implemented. Data is accessible through APIs and discoverable through API calls to a service brokerage catalogue. On-premise and cloud data are integrated in a seamless manner.

Financial

With cloud computing, the financing of IT services shifts from capital expenses to operating expenses. Organisations are now able to consume IT on a pay-per-use basis separated for each resource and costs can be allocated directly to the consuming business units. This requires a change in the financial management of IT, where technology now allows direct cost allocation and more detailed financial monitoring.

From the questionnaire, cost optimisation and charging consuming business units come at levels 3 and 4 respectively. Rightscale [64] names similar capabilities for cost management in the cloud: determining costs per business unit, cost optimisation, forecasting and automated reporting. These have been fit into the following maturity path:

- Level 1. IT budget without usage based cost distribution. Some projects are paid for by business on a non-usage based level.
- Level 2. Move towards pay-per-use costing, but infrequently billed internally and on a predetermined pricing model. Capital expenses are going through defined cycles. Operating expenses are collected at the end of each month and assigned to IT costs.
- Level 3. IT costs are distributed based on general usage. Consumers can check their ordered services and corresponding costs. Financial reporting and source data is available in real-time according to pre-defined financial parameters.
- Level 4. IT costs are charged per use to the business units, and the business has a constant view of the actual costs. Standard online contracts and supply management are integrated with supplier systems.
- Level 5. Constant cost monitoring in which growing costs are discussed with the business units. Integrated reporting and sharing of relevant data ensures pre-warning of procurement events and that service quality can be monitored and managed proactively.

Governance

IT governance is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its strategic goals and manage its risks. The goal of IT governance is to ensure the results of an organisation's business processes meet the strategic requirements of the organisation. It concerns itself with both demand governance, focused on the effective evaluation, selection and implementation of IT investments, and supply governance, focused on ensuring the effectiveness and efficiency of the IT organisation. With cloud computing, governance is required for both these branches, requiring a process and technology update to deal with and control cloud services.

In terms of governance, the Delphi panel focused on rethinking policies for cloud adoption and continuous improvement at level 1 and 4 respectively. The Weiss CCMM [42] also uses a governance domain, following the following maturity path:

- Level 1. No cloud-related governance. Existing structures are used informally.
- Level 2. Awareness of inherent governance issues for cloud and assessment of existing structures.
- Level 3. Determination of existing responsibilities and competencies. Risk and compliance management, and authentication and authorisation are introduced.
- Level 4. Auditing of cloud usage. Policy and service management are introduced. Organisation-wide adoption of cloud governance. Failure insurance is acquired.
- Level 5. Supplier relationship management. Customised and automated SLAs. Focus on continuous monitoring and evaluation.

This maturity path includes several topics that are grouped under different focus areas in our cloud maturity model. For example, at level 5 the topics of supplier relationship management and SLA management would fall under vendor management in our categorisation. In order to achieve a more focused look on IT governance, the maturity IT governance (MIG) model was assessed [33]. The MIG model contains 12 focus areas, several of which were regarded to be out of scope, leaving the following as a basis to adapt for cloud governance: continuous improvement, understanding and trust, functions and roles, formal networks, IT decision-making, planning and monitoring. These focus areas were combined with the Weiss CCMM maturity path and used to determine the following maturity path for governance:

- Level 1. No cloud governance policies have been established. Ad hoc cloud use is treated as regular service providers.
- Level 2. Roles and responsibilities are adopted to cloud requirements on an ad hoc basis. Cloud requirements are communicated to adoption islands. Cloud services are monitored and controlled like traditional internal IT services. Cloud service reporting exists based on provider's shared monitoring data. New services are catalogued in a database.
- Level 3. Roles and responsibilities are updated and formalised for cloud computing. Communication plans exist for cloud services and are discussed with impacted business, including setting up feedback mechanisms and reporting. Cloud service reporting is integrated in a single reporting tool. All cloud and traditional IT services are catalogued.
- Level 4. Roles and responsibilities are adapted to better suit business needs. Cloud based implications are defined for all organisational levels. Internal and external parties are included in communication. Regular audits and assessments ensure compliance with policies. Real-time reporting enables trend analysis and measurement against KPIs. Catalogued IT services can be ordered from a single portal.
- Level 5. Roles and responsibilities are continuously streamlined according to business needs. Communications are broadcasted throughout the full eco-system, with feedback loops in place. Automated audits ensure established policies. Real-time reporting alerts of performance threshold to start management processes. Recommendations of IT service workload location and ordering and charge back to accounting from a single portal.

Infrastructure

Infrastructure is the lowest abstraction level found in cloud computing, with IaaS as its service model. IaaS is the most flexible cloud service model and allows the organisation to automatically deploy servers, processing power, storage and networking. Virtualizing these physical items and managing their demand requires certain capabilities from the organisation.

The main determination for the infrastructure focus area was the cloud roadmap developed in the Delphi study. It starts off with virtualization at level 1, growing towards containerization, which can be seen as a further specialisation of virtualization. Furthermore, the growth path continues in adopting new capabilities, such as monitoring of virtualized resources and improved service delivery. This leads to the following maturity path:

- Level 1. No infrastructure processes for the leveraging of IaaS and containerization exist.
- Level 2. Virtualized infrastructure services support separate requests triggered via a provider tool. Container management systems are used to automate container creation and management. Some IaaS reporting exists based on provider's shared monitoring data. IaaS services are available for limited design elements that align with available services.
- Level 3. Virtualized infrastructure services allow for a standard interface to collect monitoring and alerting data. They are made available to external provider portals for orchestration processes through a common portal. Virtualized infrastructure components are defined to support a standardised automation virtualisation system integrated into a Configuration Management Database (CMDB). IaaS frameworks allow for repeatable instances.
- Level 4. Virtualized infrastructure services support automated deployment. Event monitoring is bound to each IaaS provider. Design blueprints are defined for IaaS and allow systematic reuse of key elements. Virtualized infrastructure supports automatic scaling. Use of containers is standardised. IaaS is implemented with well-defined standards and interfaces. Performance is automatically monitored against KPIs.
- Level 5. IaaS supports all data in the landscape and is managed with a single set of policies and rules. Virtualized infrastructure components allow on-premise systems to scale to the cloud. IaaS services are built with interoperable design elements, enabling cross-cloud application and service design. Virtualized infrastructure services are optimised to host and migrate resources to meet business objectives and allow for a Cloud Service Broker to select from available cloud services and platforms.

IT architecture

The IT architecture of an organisation is “a coherent whole of principles, methods and models that are used in the design and realisation of an entire enterprise’s organisational structure, business processes, information systems and infrastructure” [65]. With the adoption of cloud computing, creating and maintaining an enterprise architecture becomes more important when the organisation shifts from using internal to external IT services. Xin and Levina [66] even argue that a higher architectural maturity is beneficial for cloud adoption.

The IT architecture maturity path was based on the emergence of cloud computing in an organisation, starting with ad hoc cloud use and a growing awareness of cloud computing itself. Ramachandran [67] named multiple characteristics for cloud architecture, including reusable components and design patterns. The results from the Delphi questionnaire point toward integration and transitional projects, requiring a cloud-based architecture with integration components (APIs). The combination of these factors led to the following maturity path:

- Level 1. Cloud is not applied to architecture.
- Level 2. Cloud is considered when developing workflows, and the use of RESTful APIs and cloud service interfaces emerge.
- Level 3. Cloud services are considered in planning and processes are documented. Cloud design patterns are leveraged and standard cloud environment management tools are used.
- Level 4. Cloud service principles are a core element of architectural planning. Services can be modelled online, leveraging cloud building blocks. Services are constructed with automated integration into support processes.
- Level 5. Service components are modelled with a single set of tools, utilised for deploying and managing a highly automated and optimised cloud ecosystem. Application integration and infrastructure are transparent.

Operations

IT operations is defined as “the people and management processes associated with IT service management to deliver the right set of services at the right quality and at a competitive cost” [68]. When adopting cloud computing, the operations aspect of an organisation changes. Depending on the type cloud services adopted, the responsibilities for IT operations are decreased within the IT organisation. This ranges from abolishing a physical infrastructure when adopting IaaS up to having fewer controls for SaaS solutions when compared to traditional applications.

The field of operations consists of several of the aforementioned capability areas: operations, program management, project management and portfolio management. The operations capability area pointed towards a shift from traditional on-premise IT services towards cloud-based services. Program management and project management added the requirement of demand management to operations, allowing organisations to best place resources based on predetermined indicators. Altogether, the suggested capabilities in portfolio management concern themselves with service monitoring, service management tooling and service registration in a CMDB. These were combined into the following maturity path:

- Level 1. Demand management does not take cloud into consideration. Cloud service risk and compliance management processes do not exist.
- Level 2. Cloud demand management emerges. Service, risk and compliance management processes are in place across the organisation, but not integrated with cloud provider processes. Most applications use compute and storage virtualization. Some operation tools are used to monitor workloads off-premise. Cloud services in use have at least one representation in a CMDB.

- Level 3. Consistent processes for demand management have been defined. Processes for service, risk and compliance management allow for manual navigation of single issues. Leveraging virtualization for legacy applications extends to the network layer. Automation technologies are used to manage legacy.
- Level 4. Processes for demand management and shared automated processes used, with attached KPIs and reporting. Service, risk and compliance management processes are integrated between cloud consumer and provider. Cloud services are integrated across the full technology stack, providing support for legacy. Tooling is being replaced by cloud provided tools.
- Level 5. Systems automatically adjust to changing demand. Best placement of resources is determined through the use of KPIs and metadata. Service, risk and compliance management processes seamlessly handle incidents. Legacy systems seamlessly integrated with virtualization technologies. Transactions span across the entire hybrid landscape. Workloads are managed from a centralised position and existing tools are integrated into a single tool.

Platform

Platform is a broader term for the movement of an organisation toward PaaS and the challenges accompanying this move. This adoption process impacts software development and deployment. PaaS adoption comes with new opportunities as well by giving developers a development platform with standardised tools and access to scalable, virtualized hardware.

The platform focus area is concerned with the platform dimension from the initial model, providing a maturity path for PaaS adoption. At first, IaaS emerges within the organisation, giving several capabilities. Then, with more confidence and cloud experience, PaaS is adopted and capabilities concerning its use are developed, such as software architecture patterns for cloud computing and further tooling. This gave the following maturity path:

- Level 1. Applications are built using traditional development practices.
- Level 2. Developers use IaaS (virtualized infrastructure) to deploy non-cloud applications. Applications are integrated using standard, non-proprietary integration interfaces.
- Level 3. PaaS is used to develop new applications. Application structures are starting to use shared integration components. Application stacks are defined and common elements are stored in a database.
- Level 4. Re-usable service elements are available and maintained. Developers use cloud design patterns, focusing on reusing existing elements. Integration, presentation and data services are provided using PaaS APIs. Automatic provisioning and scaling is available. Different cloud platforms are utilised to optimally support applications.
- Level 5. All new applications are developed using PaaS. All applications are provisioned via PaaS using a common portal. PaaS applications are automatically pushed through test suites and into production when accepted. Dynamic orchestration enables monitoring application effectiveness by leveraging A/B and multivariate testing. Systems are deployed across cloud platforms and components interoperate seamlessly.

Security

Security is one of the primary concerns when adopting cloud computing. Information security ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability) [69]. With the advent of cloud computing, new security issues arise due to the distributed nature of the IT landscape, its increased reliance of networked communication and the storing and processing of data off-site.

Security as a focus area concerns itself with security policies and procedures, their implementation, and control through security audits [70]. The Weiss CCMM [42] supports this idea, as they use security as a dimension, providing a growth path where the security framework was expanded with cloud capabilities. This resulted in the following maturity path for our model:

- Level 1. Little understanding of cloud security, without any formal procedures.
- Level 2. Data security and privacy is evaluated on a project level for cloud. Applications are grouped and requirements are set for business critical applications.
- Level 3. A set of standard policies and procedures is published for use when adopting cloud services for all types of services. A clear differentiation is made between privacy and security. Audits are defined and performed regularly. Reports are generated when requested.
- Level 4. Existing cloud services are aligned to the standards. Monitoring against rules and policies, with automated reporting on issues. Security data is generated and automatically monitored against KPIs. Regular audits and assessments ensure data policy. Security requirements are integrated with architecture.
- Level 5. The security concept is reviewed regularly. Uniform security processes are in place within a security framework that monitors the cloud landscape in real-time with automated reporting. Automated audits ensure implementation of defined privacy and security requirements.

Software

The software focus area is about the management of software and the use of SaaS as a new software deployment model within the organisation. SaaS comes with new operational challenges and a new service model towards the business users, requiring maturity to handle these well.

In our maturity path, the focus lies on the manner of adoption of new SaaS solutions and how they are handled within the organisation. This comes down to the definition of policies, structuring the requirements for SaaS applications (e.g. security and cost requirements), classifying applications to identify which policies they are required to adhere to, and the organisation taking control over the implementation and usage process over time [54]. The second item used for SaaS adoption is integration, where multiple SaaS (and other software) offerings can be integrated into a business process chain. The final item of SaaS maturity is the self-service of business units, realised through a portal where the IT department provides its services on demand.

- Level 1. People use SaaS without really understanding the difference. No SaaS policies or blueprints exist.

- Level 2. Use of SaaS aligned to existing application classifications. Each cloud provider's security offerings are generally accepted. Use of SaaS offerings based on cloud provider's proposed methods. Limited integration exists to leverage SaaS offering's security and integration.
- Level 3. Well-defined software policies exist and offerings are consistently evaluated. A set of blueprints and reference frameworks exist. Data monitoring and credential management is used. Selected SaaS offerings integrated through cloud portal with electronic reporting defined. Defined interfaces exist and are used for SaaS integration.
- Level 4. Policies are supported by monitoring tooling and governance. Policies for location and protection of sensitive systems defined. Defined integration interfaces and tools are used to connect elements. SaaS services are automatically registered in the CMDB. Updates to existing systems are tested against the organisation's SaaS solutions.
- Level 5. Policy exceptions are automatically detected and alerted in real-time, supported by governance systems. Data exchange between SaaS offerings through defined interfaces, according to defined policies and methods. End users access an enterprise portal and access the desired service through brokers. Continuous evaluation of competing SaaS solutions is performed.

Software development

The focus area of software development consists of designing, programming, documenting and testing performed to create and maintain software applications and frameworks. With the adoption of cloud computing, the software development process changes in both its options for software delivery and its development tools. Cloud computing facilitates a shorter time-to-market and increased scalability of software products, when combined with a more agile development process.

In software development, the key factor is cloud knowledge and experience among developers. Adding to this, 12 factor application design [71] is aimed at the development of as-a-service software products. This led to the following maturity path:

- Level 1. Cloud knowledge among developers is based on personal interest. No standardised processes and tooling exist.
- Level 2. Development teams have some cloud knowledge to start developing cloud applications.
- Level 3. Required development capabilities for cloud services are defined and tooling and automation necessary for cloud adoption is developed.
- Level 4. Cloud-native application design, leveraging fully automated acceptance tests and container design. Development teams have a cloud roadmap that aligns with cloud strategy. 12 factor application design is adopted.
- Level 5. Developers have optimised service delivery, utilising lightweight services (i.e. microservices) that align with agility and reuse models adopted by the business. Zero-touch continuous deployment.

Vendor management

Vendor management is the collection of activities included in researching and sourcing vendors, and maintaining the relationships and communications between the organisation and its vendors, as well as continuously optimising the vendor portfolio. With cloud computing and a distributed IT landscape, vendor management becomes increasingly important due to its increased complexity. Factors such as data protection and infrastructure management become the responsibility of the service provider, rather than the organisation's, and requirements for scalability, reliability and disaster recovery need to be detailed in the relationship with the cloud service providers. New opportunities, such as acquiring point solutions and on-demand services on a pay-per-use basis raise new issues for vendor stability and viability as well.

Vendor management concerns itself with cloud service provider relations and contracts, including the SLAs and OLAs. The questionnaire results considered contract- and vendor management, capabilities also identified in both the Weiss CCMM [42] and CMM3 [54]. These capabilities were expanded upon by reporting and the coordination of business process integration. This gave the following maturity path:

- Level 1. No differentiation between regular and cloud SLAs, with no cloud-specific processes in place.
- Level 2. Cloud is fitted to match internal processes. Infrastructure SLAs are used to measure services. Defined products and contracts exist with partners with zero value commitments.
- Level 3. Standardised supplier contracts are defined. KPIs are defined for the expected benefits of cloud. Services and contracts are standardised and aligned to enable constant decision making.
- Level 4. Standard online contract and supply management is integrated with supplier systems, existing contracts are synchronised to common terms and processes. KPIs are defined and automatically monitored for service delivery. Real-time reporting on existing contracts enables trend analysis to identify exceptions.
- Level 5. Integrated reporting and sharing of relevant data with cloud providers. Business processes are integrated. Services can be aligned to meet business needs based on historical trends and data-driven predictions.

4.5 Delphi Round 3

The third round of the Delphi study was sent out to 14 participants, out of whom 11 completed the survey. Of the non-participants, there was one consultant, one cloud consumer and one cloud provider. Two excused themselves for their absence during this round and were filled in on the contents of this round afterwards.

The questionnaire presented the expanded cloud maturity model from the second round, with questions regarding the content of each of the focus areas. The final questions regarded further consolidation or expansion of the number of focus areas. The full questionnaire can be found in Appendix D.

This section discusses the responses to the expanded model and the changes made to the model after the questionnaire.

Business Process Management

The panel was in agreement over the maturity path in the BPM focus area. One expert commented on the lack of agile terminology, as agile BPM would allow an organisation to be more agile in itself. Another inhibitor in understanding was the use of COTS (commercial off-the-shelf) as a term, which appeared to be confusing to one of the respondents.

At level 3, COTS solutions was reworded to existing cloud offerings, resulting in the sentence of 'processes are in principle adapted to fit existing cloud offerings'. It conveyed the same message – adapting software to fit processes becomes much harder with standardised offerings – but in a more understandable wording.

Cloud Strategy

On the maturity path for cloud strategy, the experts agreed that level 5 was not mature enough and perhaps even less mature than level 4. One expert best described the overall opinion by suggesting that *"...on Level 5, there is a full Digital strategy and Cloud is an integral part of it."*

Level 3 was reworded to be less concise, as per a comment from one of the experts. The sentence of 'key steps and enablers for further cloud adoption have been identified' was extended by 'and are adopted in the cloud strategy'.

Level 5 was changed by adding the suggested full digital strategy and by clarifying the purpose of the enterprise-wide knowledge gathering. This gives the following revised description of maturity at level 5: Enterprise-wide knowledge gathering to drive a business-first digital strategy. Cloud strategy is integrated in a full digital strategy, a business-first strategy focused on enabling growth and optimisation of business outcomes through the use of digital technologies [72]. The strategy is regularly revised for technological developments to enable continuous innovation.

Compliance

The compliance focus area, while agreed upon as a maturity path, raised some questions regarding specific laws and regulations for IT services, as it impacts the selection of cloud providers and the decision to consume services from private or public clouds. The model did not account for such decisions on purpose, as these laws and regulations can differ per country and would require expertise in those areas for each of the countries an organisation plans to use cloud solutions in. As such, specifics were not included in the model.

Another issue raised by one expert was that of feedback loops. These were mentioned in level 5 as part of the compliance communication, but interpreted as feedback loops on compliance itself. The model is not intended as a compliance maturity tool, but as a cloud maturity tool. As such, specifics of compliance maturity have been omitted due to lack of relevance and conciseness of the model. This was addressed in the accompanying text.

Data management

The main concern for the data management focus area was the scope of the addressed issues. The domain of data management stretches beyond the issue of cloud adoption and, as such, concessions had to be made in what to include.

In terms of content, the topic of data classification was raised as something that was necessary to include. This led to the following additions for this focus area, assuming emerging data classification at level 3 and automated classification at level 5:

- Level 1. Manual data classification happens in new projects.
- Level 2. All data is classified manually.
- Level 3. Data is automatically classified.

Financial

The financial focus area maturity path was critiqued on two issues: cost assignment and self-service. Cost assignment was discussed for level 4, where the model stated 'IT costs are charged per use to the business units.' This was pointed out to be unrealistic as a definite requirement for cloud maturity, as this disregarded organisation-wide initiatives among others. It has been reworded to keep the intended message, but remove the absolute nature of the statement. The revised version is: 'IT costs are in principle assigned to business units.'

The second issue was that financial reporting was mentioned, but that it appeared as if the actual costs were quite black-box in a setting where self-service was the norm. As such, the following sentence has been added to level 5 to clarify this issue: 'Business units have insight into real-time financial reporting for their IT usage.'

Governance

The only comment on the governance focus area was aimed at level 4, where the maturity path mentioned 'Real-time reporting enables trend analysis and measurement against KPIs.' This came into place due to the inspiration of the five CMM-levels, where level 4 is named measured. Although the sentence was included there, there appeared to be no clear reason for it to be there and it was omitted from the model after this comment.

Infrastructure

The infrastructure focus area was criticised to be too vague in the mentioned reporting aspects at level 2, for including only a portal at level 3 and for including 'Virtualized infrastructure components allow on-premise systems to scale to the cloud.'

At level 2, the reporting aspects have been specified to minimise confusion. They now concern IaaS performance reporting, resulting in the statement 'Basic IaaS performance reporting exists based on provider's shared monitoring data.'

At level 3, the following statement was extended to include an API: 'Virtualized infrastructure services allow for a standard interface to collect monitoring and alerting data. They are made available to external provider portals for orchestration processes through an API and common portal.'

At level 5, scaling to the cloud was omitted. As one expert mentioned, scaling to the cloud is great on paper, but comes with a host of technical and compliance difficulties. It would be possible for object storage nowadays, but is not realistic to do in general with the currently available technology.

IT architecture

The IT architecture focus area received several critiques from the Delphi panel. One expert explains why the maturity path led to this debate:

Cloud Architecture, in my opinion, is about cloud native vs cloud adjusted. It is about the optimal use of the cloud differentiators like scalability, flexibility and pay per use. And yes, the ease of use by using a tool is an item as well. So this set of maturity levels is not wrong, but it looks far from complete.

This, in conjunction with the other remarks, led to a revision of the current maturity path for IT architecture. AWS has published a document on best practices of cloud architecture [73], giving rise to a new set of capabilities to include in this maturity path. The document names the following topics for best practices: scalability; disposable resources; automation; loose coupling; services; removing single points of failure; optimising for cost; and caching. These elements were added in a progressive fashion, in line with the maturity of other focus areas.

Level 1 of the maturity path saw no changes, as this was the base starting point for any organisation. Level 2 saw the addition of the first item previously placed at level 3: 'Cloud services are considered in planning and processes are documented.' This was stated by the experts to be the second maturity level, where cloud use was emerging and cloud awareness exists. Further, the APIs mentioned in the description were specified to be internal APIs, as a Delphi response stated that there is a difference in using internal and external APIs.

Maturity level 3 saw the addition of the first three elements of the AWS best practices: scalability, disposable use of resources and automation. This leads to the following description: Cloud services are preferred in planning. Cloud design patterns are leveraged. Cloud building blocks emerge, allowing for scalability, disposable use of resources, and automation.

Level 4 extended the use of APIs further by adding the use of external APIs to the list of capabilities, as well as more of the best practices: service discovery, loose coupling and single point of failure avoidance. This gave the following description: Services can be modelled online, leveraging cloud building blocks and design patterns. Services are constructed with service discovery and loose coupling principles. External APIs are incorporated in architecture design. Single points of failure are avoided by introducing redundancy and automated failure detection.

Level 5 incorporated the final elements of cost optimisation, performance optimisation and caching from the best practices, giving the following description: Service components are modelled with a single set of tools, utilised for deploying and managing a highly automated and optimised cloud ecosystem. Application integration and infrastructure are transparent. The architecture is designed to optimise for costs and performance by leveraging cloud elasticity and caching. Real-time performance monitoring is in place.

Operations

The operations focus area was received with agreement. At level 3, the mention of 'legacy' was extended to 'legacy applications' based on feedback from the Delphi panel. Level 4 saw the removal of '... and shared automated processes', turning the statement into 'Processes for demand management are in place, with attached KPIs and reporting.'

Level 5 got the critique that the management of KPIs and metadata was mentioned, but that there was a lack of tooling. This led to the addition of tooling, creating the following statement: 'Workloads are managed from a centralised position and best placement of resources is determined through the use of KPIs and metadata, with management integrated into a single tool.'

Platform

Platform was met with consensus and as such, no changes were made in this focus area.

Security

The security focus area was deemed to be too unambitious. Comments ranged from the suggestion of consolidating level 3 through 5 into two rather than three levels, to suggestions for a new level 5, such as *“The security concept is fully embedded in the development and operations.”*

This led to a revamped maturity path for security, where levels 3, 4 and 5 were (partially) moved to levels 2, 3 and 4 respectively, and a new level 5 was described. Level 1 did not see any changes.

The security maturity path also saw the addition of a new component mentioned in the Delphi results: identity and access management (IAM). IAM, as was mentioned, *“is an essential part of a mature hybrid cloud solution based on multiple types of Cloud services.”*

- Level 1. A set of standard policies and procedures is published for use when adopting cloud services for all types of services. Applications are grouped and requirements are set for business-critical applications. IAM is specified for specific users and project teams.
- Level 2. Existing cloud services are aligned to the standards. Monitoring against rules and policies, with automated reporting on issues. A clear differentiation is made between privacy and security. Audits are defined and performed regularly. Reports are generated when requested. IAM user groups are defined.
- Level 3. The security concept is reviewed regularly. Uniform security processes are in place within a security framework that monitors the cloud landscape in real-time with automated reporting. Security data is generated and automatically monitored against KPIs. Security requirements are defined per data classifier and integrated with architecture. IAM user groups are standardised and consolidated according to the least privilege principle. Two-factor authentication for key users is in place. An IAM classification framework for application calls exists.
- Level 4. The security concept is fully embedded in the development and operations. Applications and data are placed based on data security requirements. Automated audits ensure implementation of defined privacy and security requirements. Automated reporting on non-standard access. Internal and external API calls are automatically classified.

Software

For the software focus area, consensus existed on the maturity path. One expert pointed out that ‘registration of SaaS services in a CMDB’, as described at level 4, was not a regular way of doing this, as this was part of portfolio/vendor management and had no place in a CMDB. Further research provided no evidence on the contrary of this statement, and thus the only change in this focus area was the removal of this statement from level 4.

Software Development

The software development focus area saw the addition of two items based on feedback from the experts: continuous deployment and continuous integration. These two items are cloud-enabled, meaning that, while possible to achieve without the use of cloud services, they become more

achievable with higher cloud maturity. Another comment from one of the experts was that microservices are not the end state in maturity. While we subscribe that statement, the intention of the maturity model was to show that the organisation has the capability to deliver microservices, rather than to present microservices as the end state. This was to be addressed in the following survey, leaving the maturity path untouched on this point.

With the addition of continuous deployment and integration, maturity levels 4 and 5 became as follows:

- Level 1. Cloud-native application design, leveraging fully automated acceptance tests and container design, enables continuous deployment and continuous integration. Development teams have a cloud roadmap that aligns with cloud strategy. 12 factor application design is adopted.
- Level 2. Developers have optimised service delivery, utilising lightweight services (i.e. microservices) that align with agility and reuse models adopted by the business. Continuous deployment and continuous integration are standard practices in projects.

Vendor management

The vendor management focus area was met with plentiful suggestions of additions, as the maturity path did not cover the scope of the focus area as intended by the experts. Level 2 saw the first addition, where the requirement was voiced that vendor management maturity should give some insight in the motivation for vendor selection: selecting cloud providers based on business requirements.

The software focus area contained the statement 'Cloud usage is monitored and its performance is evaluated against SLAs,' at level 3. This statement, the experts stated, was better placed under vendor management at the same level of maturity, which described SLA management as one of the key activities.

Level 4 built on this statement, adding that 'Cloud service performance is automatically monitored against SLAs.' At level 5, the final maturity stage for that capability would be reached, expressed in the statement 'Real-time reporting on existing contracts enable trend analysis to identify exceptions.' This resulted in the following maturity path:

- Level 1. Cloud providers are selected based on business requirements. Cloud is fitted to match internal processes. Infrastructure SLAs are used to measure services. Defined products and contracts exist with partners with zero value commitments.
- Level 2. Standard contracts from pre-selected cloud providers are made available for business units. KPIs are defined for the expected benefits of cloud. Services and contracts are standardised and aligned to enable constant decision making. Cloud usage is monitored and its performance evaluated against SLAs.
- Level 3. Preferred cloud providers are selected based on cost and performance measurements. Standard online contract and supply management is integrated with supplier systems, existing contracts are synchronised to common terms and processes. KPIs are defined and automatically monitored for service delivery. Cloud service performance is automatically monitored against SLAs.

- Level 4. Preferred cloud providers are selected and managed based on strategic objectives. Services can be aligned to meet business needs based on historical trends and data-driven predictions. Businesses can consume cloud services via a service catalogue containing standard contracts with pre-selected cloud providers. Real-time reporting on existing contracts enables trend analysis to identify exceptions.

4.6 Delphi Round 4

The fourth round of the Delphi study was sent out to 14 participants, out of whom 10 completed the survey. Of the non-participants, there were one consultant, one cloud consumer and two cloud providers. Three participants excused themselves for their absence during this round due to scheduling issues.

The questionnaire presented the revisions of the cloud maturity model discussed in the third round, with questions regarding the changes for each of the focus areas. The full questionnaire can be found in Appendix E.

The results from the fourth questionnaire show a consensus, concluding the Delphi study. One minor change was made based on the responses. In the software development focus area, level 4 stated that 'Cloud-native application design, leveraging fully automated acceptance tests and container design, enables continuous deployment and continuous integration.' Container design was mentioned as not fitting in this part of software development. Good container design is essential for scalability, but is already covered in the development capabilities at level 3.

4.7 Reorganising the Cloud Maturity Model

The model resulting from the Delphi panel consists of 14 focus areas without a clear direction. In order to give a better overview of these focus areas and their areas of impact, they were mapped on METRI's model for the IT organisation. This decision was based on the practical application of the model, ultimately to be used by METRI. This section describes METRI's model for the IT organisation and the mapping of the focus areas to this model.

METRI's model of the IT organisation (Figure 23) consists of five dimensions in the IT organisation (support the business, transform and improve the business, govern IT, and Operate IT) and one overarching dimension indicating the focus of the IT organisation (Business).

Support the business: This dimension stands for the IT processes supporting the business in its daily operations, such as the helpdesk and on-site support. None of the focus areas from the cloud maturity model could be mapped to this element.

Transform and improve the business: This dimension indicates IT processes aimed at transforming the current IT offerings in order to improve the current business model. This starts with the IT strategy and translation towards more practical goals (enterprise architecture, BPM) and includes all activities aimed at business execution. From the cloud maturity model, we mapped all strategic and transforming focus areas to this dimension: cloud strategy, IT architecture, BPM and software development. Each of these focus areas concern themselves with either the creation and implementation of the strategy or with transforming and enabling business processes.

Manage IT: The manage IT dimension sits between transform and improve the business and IT operations to indicate the link it has between these elements. Manage IT is about managing internal and external resources that the business does not have to concern itself directly with. One focus area was mapped to this dimension: vendor management. It concerns itself with the availability and management of the resources required to transform and improve the business, while being a level above operate IT in abstraction.

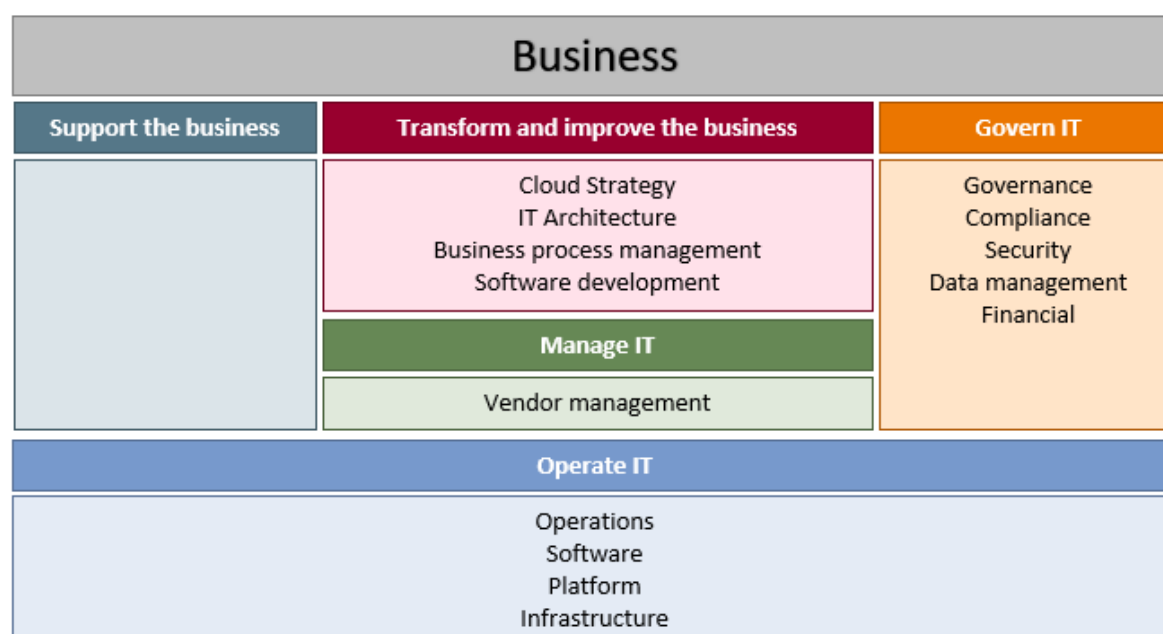


Figure 23 METRI's IT Organisational model with mapped focus areas

Govern IT: This dimension consists of all processes aimed at governing and controlling IT services and their use. IT governance, security and compliance management all fall under govern IT. The following focus areas were mapped to this dimension: governance, compliance, security, data management and financial management. The first four are overarching capability areas used in all other dimensions, whereas financial management concerns itself with controlling and managing IT costs.

Operate IT: Operate IT concerns itself with all aspects of operating and running IT. Out of the discussed focus areas, this includes operations, software, platform and infrastructure. All four are aimed at operating parts of the (cloud) IT landscape.

Manage IT				
Vendor Management		Yes	Somewhat	No
1	There is differentiation between regular and cloud SLAs.	x		
	There are cloud-specific vendor management processes in place.	x		
	Cloud providers are selected based on business requirements.	x		
2	Cloud is fitted to match internal processes.		x	
	Infrastructure SLAs are used to measure service performance.	x		
	Zero value commitments with defined products and contracts exist with several partners.			x
3	Standard contracts from preselected cloud providers are made available for business units.			x
	KPIs have been defined for the expected benefits of the cloud.			x
	Services and contracts are standardised and aligned to enable constant decision making.			
	Cloud usage is monitored and its performance evaluated against SLAs.			

Figure 24 Assessment for vendor management level 1 through 3

After mapping the focus areas to each dimension, the maturity path of each focus area was dissected. Each of the cells consisted of several statements, which were split apart and presented as separate statements in a list. From this list, an assessment tool was created in Excel, with the option to answer

yes/somewhat/no to each of these statements. These answers were then used to calculate and show maturity progress (all yes on the statements of a maturity level indicating that that level had been fulfilled). Figure 24 illustrates part of the assessment. The full questionnaire can be found in Appendix F.

4.8 Conclusion

This section attempted to answer four of the subquestions:

- RQ3. Which stages of cloud adoption relate to each maturity level?*
- RQ4. Which factors need to be accounted for when assessing an organisation's cloud maturity?*
- RQ5. How can each of the maturity levels in a cloud maturity model be defined?*
- RQ6. How do the elements identified in literature relate to the maturity model?*

The Delphi study began with defining a roadmap for cloud maturity. This roadmap was refined in the first Delphi round and met with consensus in the second round. Different stages of cloud adoption were mapped onto this model over three dimensions: infrastructure, platform and software. It was the guideline by which the final maturity model was developed, providing an image of when an organisation would adopt certain cloud solutions. The roadmap is our answer to RQ3, mapping the stages of cloud adoption for each of the cloud service models on a five-stage maturity model.

In order to answer RQ4, the Delphi panel was consulted on which areas of an organisation would be affected by cloud adoption. Both the roadmap and a list of organisational capability areas were presented to the experts to elicit the relevant capability areas for the maturity model. Their answers were supplemented by the findings from scientific literature, which were described in the assessment of the prior cloud maturity models. This resulted in a set of fourteen focus areas, three of which came from the Delphi study and were not identified in literature, while the areas identified in literature were all covered by the experts as well. These areas are Cloud Strategy, IT Operations and Software Development. This stage also answered RQ6, by showing a relation between the elements identified and incorporated in the model and those identified in literature, while at the same time providing the basis for answering RQ5.

The third phase of the Delphi study consisted of creating and validating maturity paths for each of the identified focus areas, which ultimately led to the answer of RQ5. Each of the maturity paths was developed based on scientific literature, drawing inspiration from the prior cloud maturity models, as well as existing maturity models for the specific areas, which were then adapted to fit the developments brought forth by cloud adoption. These maturity paths were presented to the experts in two iterations, refining them based on their input and ultimately reaching as good a consensus as we could hope for after the fourth Delphi round.

Overall, the Delphi study proved to be a good method to elicit knowledge from experienced practitioners, leading to the addition of three focus areas affected by cloud adoption, but not previously mentioned in scientific literature concerning cloud maturity.

5. Validation

This chapter presents the validation phase of this thesis. It starts off with two follow-up interviews with members of the Delphi panel, presenting the reorganised model and assessment. After the interviews, two case studies were performed and documented in this chapter.

5.1 Follow-up Interviews

Individual depth interviews were conducted with two of the Delphi participants to present the final model and assessment created from the focus areas and their maturity path designed in the Delphi study. This section describes both interviews and the conclusion drawn from them.

The interviews were conducted in one hour sessions for each interview, with the researcher, a consultant from METRI and the Delphi participant partaking. Several broad interview questions were created based on the personal answers each interviewee gave during the Delphi study, leading to semi-structured interviews.

5.1.1 First Interview

The first interview was conducted with one of the cloud providers, an organisation providing a community cloud. The interviewee has the function of cloud director, responsible for the timely availability of resources in the community cloud and feature development and security for their own cloud services. In addition, the interviewee was responsible for the provider's partnerships with third parties.

In terms of the overall model, as presented in section 4.7, he agreed that the structure covered the aspects of IT management and that the mapping suited the model well. The model gave a structure to the 14 focus areas and their interrelations.

When asked about the extension of the IT architecture focus area, one of his areas of expertise, he argued that the AWS best practices [73] was a solid addition. However, the importance of enterprise architecture required more highlighting in the model, as having a good architecture and making decisions supported by this architecture were of vital importance to keeping control over the IT landscape.

Another point of discussion was the financial focus area, where the maturity path lead to an organisation where business units received frequent cost updates. He argued that this may seem like an ideal scenario, reality learns that most of the provider's customers did not care and only expected a bill at the end of each quarter. Whether this was due to a low maturity at the customer's side or through an overall lack of demand for such scenarios he could not say.

In his response on the Delphi questionnaires, the interviewee mentioned the topic of digital transformation several times, stating that it was not highlighted enough in the model. Upon further questioning, he mentioned that these statements were mostly about the move towards a more agile organisation, where data and behaviour drives decisions and an organisation can adapt quickly. However, he agreed that this was not in scope of the model.

The final issue discussed was of the scope of the model itself. He stated that they used an internal cloud maturity model based on why an organisation should adopt certain cloud services, listing the

benefits for each. Continuing, he pointed out that our model gave off the perception that an organisation would move everything to the cloud, rather than explicitly point out that the model detailed the capabilities required for cloud adoption.

5.1.2 Second Interview

The second interviewee is employed at a cloud provider who build both public and private cloud solutions. His function consists of architecting public and private cloud environments to deliver the provider's services to their clients.

At first, he spoke about the difficulties in cloud adoption, relating to any new technology. He stated that the largest inhibitor was a lack of knowledge on cloud security; customers were often making the decision whether or not to use public cloud services based on them feeling more comfortable with private cloud services, as that felt more secure. This was something beyond the scope of the model, but he felt that required highlighting, as the model could help alleviate this knowledge gap somewhat by making cloud computing more concrete.

During the Delphi study, the interviewee often mentioned IAM. When asked about the topic, he stated that IAM was of vital importance to cloud computing, because properly managing IAM would allow for a more trustworthy feeling towards the cloud. This would help in his previous statement on the feeling of cloud computing being insecure.

The same feelings, he stated, take part in the discussion around compliance. With laws and regulations adapting to cloud computing (e.g. data residency laws), the issue of security became an even bigger topic and strengthened the customer's feeling that cloud computing was in essence not secure. Once again, he said, proper compliance management would help alleviate this problem.

On the topic of operations, he supported the claim that IT operations drastically change with an all-in cloud strategy. Operations would become more centralised and less specialised, as most components would be managed by the cloud providers. Organisations would find difficulty in the transition towards this new type of IT operations and the model gave a good starting point to get a grip on this situation.

The final topic discussed was the actual visualisation of the model. He pointed out that the new structure, where focus areas are mapped on the dimensions of the IT organisations, gave some much-needed clarity to the model and how the components interacted with one another.

5.1.3 Interview Conclusions

Both interviews described the adoption of cloud computing as something that does not happen in an isolated space. Organisations are often dealing with legacy applications and existing processes, which is key to take into consideration when presenting the model to its users.

Another item to watch out for was the communication of the scope of the model. The model would be ill-suited to an organisation just discovering what cloud computing is all about, since its focus lies on informing those preparing to transition (further) into the domain of cloud computing.

On the topic of visualisation and further model development since the Delphi study, both interviewees agreed that it provided clarification in both the interrelations between the elements and the method of assessment.

5.2 Case Studies

Two organisations were found willing to participate in pilot case studies for the practical application of the cloud maturity model. The first case study followed an unplanned format, due to limited availability of managerial staff, whereas the second conformed itself with the intended format of first the assessment, then a follow-up appointment and then result presentation. Below we first present the method used for these case studies. Then we provide descriptions of the organisations with regard to cloud adoption and the use of the model. The section closes with a conclusion drawn from both case studies.

5.2.1 Case Study Method

The case studies were performed to observe the usefulness of the developed cloud maturity model in practise. The usefulness was measured by the response of the participating practitioners after using the model. A preconceived format was presented to the participating organisations:

1. *Fill out assessment*: The participating practitioners were requested to fill out the assessment questionnaire. This was estimated to take 1,5 hours per practitioner.
2. *Discuss assessment individually*: The assessment results from each participant were discussed with the researcher and a consultant from METRI, upon which changes could be made to these results in order to better reflect the actual situation. This was estimated to take 1,5 hours per practitioner.
3. *Aggregate assessments*: The assessments were aggregated in order to determine the maturity for the organisation as a whole. This was done by using a 75% maturity score to proceed to the next level (e.g. one participant scores 3/5 on level 2 and another 5/5 on the same level, the average is 4/5, which is 80% of the total score, thus the maturity level is considered filled). This aggregation was done to prevent singular disagreements to prevent maturity to halt prematurely. Where required, the maturity levels were manually adjusted if the aggregation was not justified. This step required no practitioner involvement.
4. *Present findings*: The conclusions from the assessments were aggregated and presented to the organisation in a report, along with recommendations and strong points regarding their use of cloud computing. This was estimated for 1 hour with the whole group of practitioners.

This format was communicated to the participating organisation, who chose to deviate from it. One organisation, the international trade organisation, could not afford the time commitment, as described in section 5.2.2. The second organisation, the waste collector, completed the assessment with two practitioners in one assessment document, leading to a discussed assessment that resembled the final aggregate. Due to these deviations, a straight-up comparison of the case studies is not possible. As such, the focus of the case studies lies on the feedback the practitioners gave of the model.

5.2.2 International Trade Organisation

The first case study took place at an international trade organisation based in the Netherlands. Due to time constraints on the side of the case study participants, we were unable to complete a full assessment and had to work with a shortened assessment. The available time, a three hour session instead of five one-and-a-half hour sessions with a prefilled assessment, was used to present the model and ask the participating practitioners about their current involvement with cloud computing, followed by assessing three of the focus areas in a group setting.

The session took place with four members of their IT organisation, with roles from CIO to operations manager. At the end of the session, the CIO stated that one of the most valuable takeaways from the session was that it was the first time these roles came together to discuss cloud adoption, due to the previously communicated scope of the model.

Their current situation with cloud computing was that they were on their way to adopt cloud on a larger scale than the ad hoc use they had been doing until now. They experienced several challenges in their organisation in the areas of changing business processes, reorganising the IT department, cloud knowledge and cloud experience. At first, they assumed that adopting cloud services would be an easy transition, but quickly found that the process of cloud adoption was more complex than imagined. They found it hard to get a grip on the transformation process, as cloud providers focused mainly on the technological side with their advice and not on the impact on the IT organisation.

During the assessment phase, the maturity of three focus areas (cloud strategy, IT architecture and governance) was assessed. We saw differing opinions of several of the subjects. For example, communication of their IT strategy appeared to be very clear for the CIO, while operations had a different interpretation of said strategy. Such issues support the relevancy of the model, which has the goal of giving insight in cloud adoption.

Concluding the session, the three focus areas were well-constructed in content, although the statements could be phrased better at some points. The biggest issue identified was that it was difficult to identify the mindset of the statements for each focus area. As such, the general conclusion was that the model would benefit from adding the description of each focus area to the assessment itself, leaving less room for interpretation in that area.

5.2.3 Waste Collector

The second case study considered the IT organisation of a waste collector active in a number of municipalities in the Netherlands. This case study was performed according to the intended setup, in which the participants were sent the assessment beforehand. This assessment was then analysed and its results discussed with the participant in a separate session. Concluding the case study, a report was presented with the key findings from the maturity assessment. The two participants decided for themselves to fill out the assessment as a pair, rather than separately. This led to only a single follow-up discussion to place the assessment in the right context.

Their current IT landscape was somewhat cloud-oriented, as they were using SaaS for some secondary business processes and starting to adopt cloud services for some of the primary processes. In this light, they deemed themselves to have a good understanding of cloud computing and were interested in the model as a means of appreciation of their maturity.

During the follow-up discussion to the assessment, we questioned them on their use of cloud computing, vendors and their associated processes. They had well-documented processes for the adoption of new systems, which included repeatable processes for cloud adoption. Two things worth noting were that they did as few actual operating tasks as possible, having outsourced them for ten years already, and that they did this at the same vendor all that time, with which they are a trusted partner and ensure that their IT is future-proof.

After the follow-up discussion, the assessment was altered to reflect their situation better. The software development and platform focus areas were removed from considerations, as the

organisation did not concern itself with actual software development. Another consolidation was the alteration of the results for the financial focus area, where the organisation was too small to have financially independent business units and, as such, cost allocation to said business units. This led to the maturity presented in Figure 25.

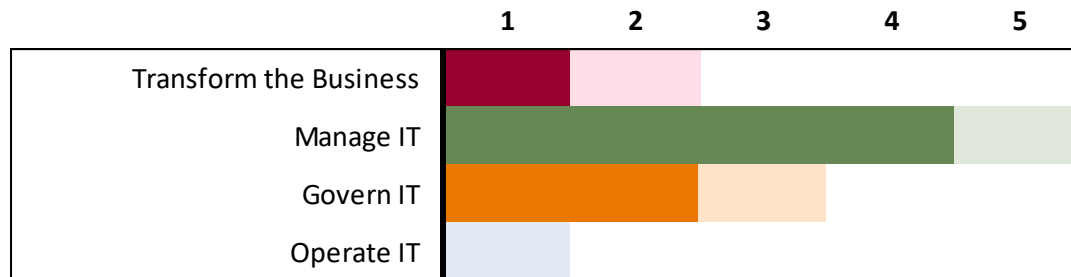


Figure 25 Waste collector overall maturity

Our main finding for their IT organisation was that they did not make a clear enough distinction between traditional outsourcing and cloud services. Both the opportunities and challenges specifically associated with cloud computing were not well-understood and did not get enough attention. This illustrates itself very well in the dimensions of transform and improve the business and operate IT, where cloud awareness and leveraging cloud benefits are the respective main hindrances for reaching a higher maturity.

When these findings were presented, they were subscribed and elaborated upon. Some areas were already in development, causing the maturity model to give an apparent lower maturity than they felt was justified. However, it did provide some adequate points for discussion and future improvements and was perceived as an overall good model and method of assessment.

5.2.4 Case Study Conclusions

From these two case studies, the major point of interest was the process of assessment. In both cases the assessment was performed by more than one person, be it due to the format or their own choice, sparking a discussion between the members of the IT organisation. This discussion and the provisioning of topics proved to be a commendable feature of the model, albeit due to use diverging from its original intent.

The model also appeared to be a good fit on offering organisations handholds for the (further) adoption of cloud services. In the first case study, the remark was made that they had already set in the move towards cloud computing and that the topics mentioned were being worked on, as well as providing coverage of the main topics associated with cloud adoption. In the second case study, we found that the organisation was already concerning itself with some of the topics laid out in the model, but was unaware of others. In both cases, we found that the model covered the expectations the organisation had of the maturity models.

One point of contention for the cloud maturity model was the size of organisations it intended. In the case study of the waste collector, they mentioned the issue of not having separate business units. This invalidated several statements, leading to the dismissal of some capabilities that were required for further maturity levels. The third party involvement in the form of the METRI consultant proved

to be a good influence here, allowing further explanation of the intention of that section of the model and the determination of relevance for the organisation itself.

Finally, there were two points of improvement for the model. First, we found that there was a requirement for more testing, as the model was unclear in some statements. Since it was a first iteration, we were aware of the issue, but welcomed any feedback on its use. Secondly, the point was made that the whole model was presented in English, which was not the daily language of choice for either of the organisations. This presented some challenges during the assessment and led to the decision for METRI to translate the model to Dutch for further use in the Dutch IT industry.

5.3 Conclusion

The validation phase of this study was performed in order to answer RQ7:

RQ7. Do the model elements and requirements hold up in practice?

From both the interviews and the first case study, we concluded that the scope of the model is the most important item to clearly communicate to the practitioners using it. In both situations, the question was asked why an organisation wants to adopt cloud computing, something the cloud maturity model does not answer. The model was clearly scoped as a tool supporting organisations wanting to (further) adopt cloud computing by identifying their current capabilities and their desired situation.

One surprising realisation from the case studies was that the model was deemed an excellent tool to drive the conversation on cloud computing, forcing the organisations to consult with different types and levels of managers and providing a list of topics. In both case studies, the discussion surrounding cloud computing and what it exactly entails was a major topic, whereas our expectations were aimed at providing focus towards further and, potentially, better use of cloud computing.

Although the first case study was performed in an unconventional format, not covering all focus areas, we deem both case studies as successful examples of using the cloud maturity model. Both organisations were positive about the outcomes of the model and saw the benefits of using the model as a tool to assess their readiness for the stages of cloud adoption.

6. Discussion

This chapter discusses the results of this project. It first reflects on the methodology used to develop the cloud maturity model [16] and the Delphi study as the main methodologies used to achieve this result. This is followed by discussing the current cloud maturity model, contrasted to the prior solutions we identified. Finally, it discusses the contributions of this study to academia and practice.

6.1 Research Methodology Used

Throughout this study, the procedural method by Becker, Knackstedt and Pöppelbuss [16] was used to ensure the necessary scientific rigour in the development of the cloud maturity model. This method proved to be a good guideline in structuring the study around the necessary elements.

In contrast to the cloud maturity models identified in literature, this study used multiple methods to support the final result. It started with a literature review on cloud computing and its benefits and challenges, as well as a review of the approaches available to create and populate maturity models. This work formed the basis of assessing the currently available cloud maturity models, showing the need for the analysis in their respective shortcomings.

The main body of this thesis consists of the Delphi study and the related development of the cloud maturity model, which is interspersed with relevant literature. This proved to be a very beneficial method, allowing both inspiration from scientific sources as well as feedback from experts in eliciting and generalising the body of the model. The setup of the Delphi methodology allowed the freedom to work with unfinished versions of the model, calling on the expertise of the panel to fill in the gaps and add to the material in ways we did not consider. This method proved beneficial to the final state of the model and the level of participation from the consulted experts.

6.2 Cloud Maturity Model Reflection

Within the process of developing the cloud maturity model, inspiration was drawn from prior models identified in both scientific and industry publications. In analysing these prior models, it was identified that each had shortcomings in scientific rigour, the inclusion of cloud-related elements, or both. This led us to take the notions of Becker, Knackstedt and Pöppelbuss [16] to heart and perform the study in a multi-method process, using interviews, literature study, a Delphi study and case studies to achieve the final result.

We found that the majority of the prior models were too narrow in their scope, not addressing the key challenges and benefits of cloud adoption. Three elements that were identified as key challenges, namely changing financial management, compliance and governance, were hardly addressed in any model. During the Delphi study, the findings of our literature study were confirmed without disclosing these beforehand to the experts. In addition, we found three areas that the experts identified as required for cloud maturity which were not prior in literature, but are significantly affected with cloud adoption. These areas are Cloud Strategy, IT Operations and Software Development.

One of the main sources of insight on the challenges of cloud computing adoption was the research of El-Gazzar, Hustad and Olsen [11], who performed a Delphi study to elicit the adoption issues of cloud computing. Their results illustrate that the focus of a Delphi study impacts its outcomes. For

example, the IT strategy is not an issue, but does concern an area that will be affected by cloud adoption. As such, identifying three new focus areas is complementary to previous work.

Altogether, the cloud maturity model proposed in this thesis is inclusive in its number of focus areas, with a total number of 14. This results in a model that is rather large and may seem daunting to an organisation looking to adopt cloud solutions. Our experience from the case studies teaches that the whole assessment takes around one-and-a-half hour to finish, not including a follow-up in which the assessment results are discussed.

One area of the current iteration of the model that requires further development is the ability to determine what organisations can achieve on each level of maturity. Whereas the initial model was based on the roadmap constructed earlier in the study, the final model is two iterations past this roadmap and the correlation between the two is suggestive. In order to fully elicit the relation between the maturity levels and an organisations current situation and goals, further research is required with quantitative data from the organisation using the model and their current cloud use.

Another limitation of the model is the size of organisations it is scoped for. While the scope is broader than previous cloud maturity models, the model takes organisations with several business units into account. These are large organisations and this excludes SMEs from using the model to its full effect. This does not apply to all focus areas or whole focus areas, but some statements use this requirement.

Our empirical evidence allows us to conclude that the current model is a step towards a broad, scientifically grounded cloud maturity model. It elicits the areas of an organisation wanting to (further) adopt cloud computing. From the case studies, the model appears to be a good instigator for constructive discussion between different parts of an organisation. Further iterations would be required to slim down the model to the bare necessities and to define the link between the maturity levels of the individual focus areas and the level of cloud adoption.

6.3 Contribution to Research

The contribution of this research to the scientific body of knowledge consists of three items. First, a framework was created and used to assess existing cloud maturity models. The identification and assessment of these models gives an overview of the available models in both scientific and industry literature and shows the strengths and shortcomings of each.

Secondly, a cloud maturity model is developed as an outcome of this research. This model is an addition to the body of knowledge concerning cloud adoption, introducing a multi-method approach to the development of cloud maturity models. The resulting model addresses issues from practice that are scarcely if at all covered in the scientific literature studied. These issues are the development of a cloud strategy and the impact of cloud computing on the overall IT operations and software development.

The third contribution is that the cloud maturity model addresses several knowledge gaps on the organisational changes seen when adopting cloud computing. It contributes to the areas of IT strategy, IT governance, enterprise architecture and BPM by stating a path for organisational development from a cloud perspective.

The major contribution of this research is the cloud maturity model itself. It gives an overview of the areas of expertise required for cloud adoption by drawing on experts to identify and further structure these. The knowledge itself existed in an unstructured and unwritten manner, whereas the research elicited these and incorporated them in a structured overview.

6.4 Contribution to Practice

The cloud maturity model offers new insights in cloud adoption by providing an expansive model constructed with cloud experts. It shows the gathered insights in 14 focus areas, giving both a broad view, in terms of general cloud maturity and a roadmap, and a narrow view, as the maturity per focus area, in one model.

When considering the model itself, the assessment tool and its means of communication, it provides a comprehensive overview of its contents, the decisions made in its construction and its applicability in practice situations. Comparatively, none of the earlier identified models has documented case studies of its application in practice.

The cloud maturity model comes with the prerequisite that the decision to adopt cloud services has already been made by the organisation looking to apply it. The model is a poor guideline in explaining what cloud computing implies and its benefits and challenges, as these were found to be well-documented in prior literature. In the case studies, we found that cloud computing was not always as well-understood as expected, making this a limitation of the applicability of the model.

In order to use the model well and assuming a good understanding of cloud computing, practitioners can use the assessment included in Appendix F to determine their maturity. If certain focus areas appear inapplicable, such as Software Development for organisations that do not create software, they can be ignored in the assessment. As noted in section 5.2 and 5.3, some statements apply to large organisations only, although the underlying capabilities are relevant to smaller organisations as well.

6.5 Research Limitations and Future Work

The resulting cloud maturity model has been constructed through the use of a Delphi study and a literature study. The Delphi study has, as a methodology, the inherent flaw that it is not a repeatable method. This means that other Delphi studies with an identical setup may elicit different focus areas for cloud computing. To address this issue, the research was supported by scientific literature, providing both a foundation and validation for the Delphi research.

Furthermore, each of the focus area maturity paths were supported by literature. The literature used was determined based on its number of citations and relevancy to the subject. This may have led to unintended oversight. Since the Delphi study had no further major critiques on the findings, they were accepted as fulfilling the requirements of the cloud maturity model.

Proposing each of these maturity paths to experts with cloud knowledge in the related fields is a logical step following this research. Subject areas such as data management were mentioned during the Delphi study to be much larger than cloud computing. Due to the scope of the thesis research, only experts on cloud computing were consulted, potentially steering the results less towards the intricacies of the complex areas of expertise and more towards the overall topic of cloud computing.

Future research should include experts in a broader range of expertise to verify and refine these findings.

Regardless of future development, the cloud maturity model is generalisable to be applied to large organisations operating as consumers in the Dutch cloud computing market. Seddon and Scheepers [74] state that, in order to argue the generalisability of a study, the representativeness of the sample for the setting as a whole needs to be defended and supported by claims made in other studies. The argument for this generalisation stems from both the case studies as well as the set of experts participating in the Delphi study. All participants are active in the Dutch market and the Delphi panel included a representative sample of the major cloud providers and consumers. This is strengthened by the conclusion of usability from the case studies. The generalisability of the model may stretch beyond the Dutch market. Several of the participants stem from organisations that are operating globally and the models that inspired ours and the technology used are globally available and applicable. However, to support the claim further generalisability, additional data (e.g. case studies, interviews) is required.

Although this research produces a workable cloud maturity model, the road for further development is wide-open. The as-a-service models in the current model are SaaS, PaaS and IaaS. These three were defined in literature and as such the only models considered. In return, emerging models, such as security-as-a-service and network-as-a-service (as an extension of software-defined networking) were not considered in the development of this cloud maturity model. As such, future research may include these as-a-service models and aim to provide a maturity path for these.

7. Conclusion

This chapter contains the main conclusions described in this thesis. The introduction identified a lack of vendor-neutral tooling to support IT management in adopting cloud computing. A maturity model was proposed as a fitting solution to this tooling problem. The main research question was:

What constitutes a maturity model for cloud adoption that contains both the stages for cloud adoption and corresponding organisational capabilities?

This was supplemented by posing a set of subquestions, which were answered in three stages in this thesis. The first stage focused on the assessment of existing cloud maturity models, based on a framework developed based upon the benefits and challenges of cloud computing. This came with the following research questions:

- RQ1. *Which cloud maturity models are available in current scientific literature?*
- RQ2. *What does a model for assessment of cloud maturity models consist of?*

The second part of this thesis aimed to create a new cloud maturity model through a Delphi study, supplemented with maturity models and relevant literature for each of the focus areas. This part answered the following subquestions:

- RQ3. *Which stages of cloud adoption relate to each maturity level?*
- RQ4. *Which factors need to be accounted for when assessing an organisation's cloud maturity?*
- RQ5. *How can each of the maturity levels in a cloud maturity model be defined?*
- RQ6. *How do the key elements relate to the maturity model?*

The final part of this research focused on the validation of the proposed cloud maturity model in a practical setting by performing expert interviews and case studies. This aimed to answer the following subquestion:

- RQ7. *Do the key elements and model requirements hold up in practice?*

This chapter will briefly summarise the answers to these subquestions in three parts: prior model assessment, cloud maturity model development and cloud maturity model validation. It will end with answering the main research question.

7.1 Prior Model Assessment

The first subquestion is:

- RQ1. *Which cloud maturity models are available in current scientific literature?*

To answer this question, a literature study was performed. Scientific literature was first consulted, resulting in a total of two cloud maturity models after filtering the results. This search was expanded to include practitioner models and other types of scientific materials (e.g. master theses and PhD dissertations). The search resulted in a total of seven cloud maturity models. In order to assess the usefulness of each of these models, the following subquestion required answering:

- RQ2. *What does a model for assessment of cloud maturity models consist of?*

From the prior review of scientific literature on cloud computing and maturity models, 12 elements essential to a cloud maturity model were identified. Two of these elements came from the general use of maturity models: a method of assessment and the clear use of capabilities. Two of the elements originated in the description of cloud computing, regarding the cloud service and deployment models. The other eight elements were derived from the challenges associated with cloud computing in scientific literature: financial management, security, compliance, governance, SLA management, what to migrate at what stage, process management and integration.

In addition to these elements regarding cloud computing, the assessment consisted of a set of criteria for scientific rigour in the development of these models. This decision was made on the basis that, in order to understand these models, the reasoning behind the conception should be clear. This part of the assessment held the models against the methodology used in this thesis.

With these elements, the identified cloud maturity models were assessed. Each of the models was lacking in scientific rigour, the cloud computing elements they included, or on both of these points. This led to the decision to create a new cloud maturity model, rather than to expand an existing one.

7.2 Cloud Maturity Model Development

The cloud maturity model development was performed with the use of a Delphi study and a supporting literature study. The Delphi study was structured around answering four subquestions, the first being:

RQ3. Which stages of cloud adoption relate to each maturity level?

This question was answered by creating a cloud adoption road map, illustrating the stages of cloud adoption through which an organisation goes. These were mapped on five maturity levels in three dimensions: software, platform and infrastructure. An initial version of this roadmap was presented to the Delphi panel and the refined version is shown in Figure 26.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Legacy apps on dedicated infrastructure	IaaS replacing on premise		Cloud-native infrastructure	Cloud-optimized infrastructure
Platform			PaaS development Application stack on PaaS	Redesigned applications for PaaS	Cloud-optimized PaaS
Software		Mature cloud solutions SaaS Point solutions	Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS

Figure 26 Revised cloud maturity model

RQ4. Which factors need to be accounted for when assessing an organisation's cloud maturity?

The second round of the Delphi study focused on eliciting the different areas in an organisation that were impacted with cloud adoption. This led to the composure of a set of fourteen focus areas, which were mapped to METRI's model of the IT organisation, as illustrated in Figure 27.

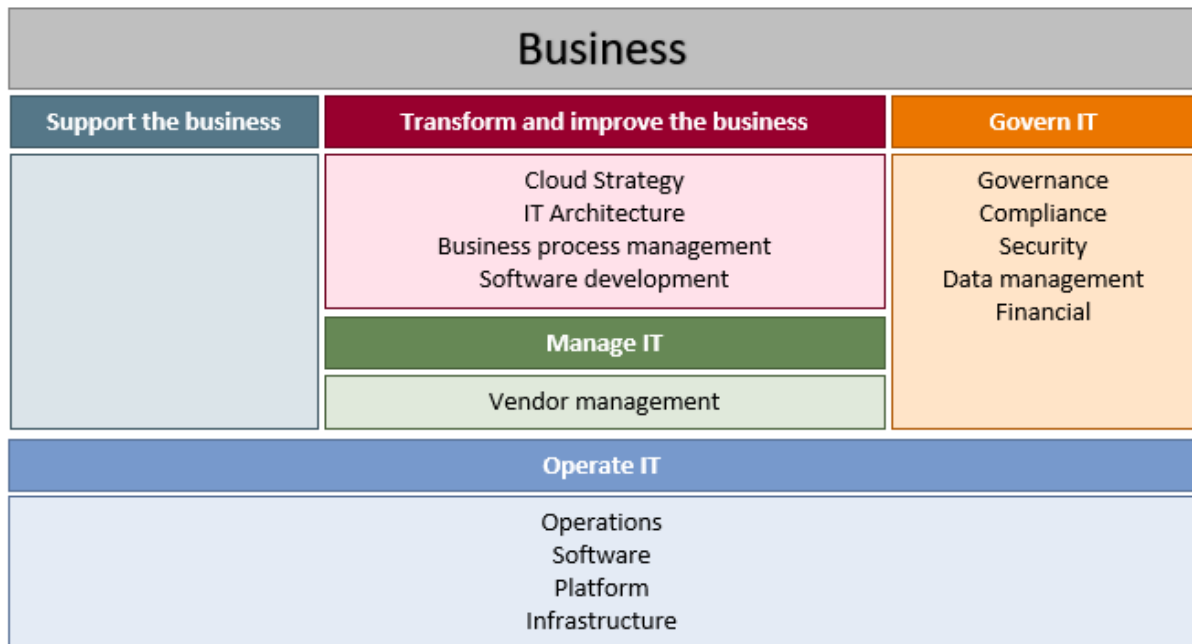


Figure 27 METRI's IT Organisational model with mapped focus areas

RQ5. How can each of the maturity levels in a cloud maturity model be defined?

The maturity levels of the model are defined through the individual maturity paths of each of the focus areas. These were conceived by consulting existing scientific literature, taking inspiration from prior cloud maturity models, non-cloud maturity models and general best practices. The results from these methods were added upon and revised based on the third and fourth Delphi rounds, resulting in the final maturity paths for each of the focus areas.

RQ6. How do the elements identified in literature relate to the maturity model?

When the focus areas were defined in the second round of the Delphi study, the list of focus areas was consolidated and held against the elements identified in literature. The elements identified in literature were all covered in the Delphi response, but the elicitation resulted in three focus areas that were not covered in the literature studied: cloud strategy, software development and IT operations.

7.3 Cloud Maturity Model Validation

The validation stage of the research was conducted through two follow-up interviews with experts participating in the Delphi study and by performing two case studies. This phase aimed to answer the following subquestion:

RQ7. Do the model elements and requirements hold up in practice?

From both the interviews and the case studies, the conclusion was that the model covered all relevant aspects affected by cloud computing. However, the case studies led to situations where the model facilitated a discussion on cloud computing and what it entails. This was a deviation from the expectation that the model solely provided a focus towards further and better use of cloud computing. These discussions proved to be a main selling point of the model.

7.4 Answering The Main Research Question

This thesis culminates in answering the main research question:

What constitutes a maturity model for cloud adoption that contains both the stages for cloud adoption and corresponding organisational capabilities?

Due to the progressive nature of the subquestions, each of the underlying aspects has been covered in their respective answers. The stages for cloud adoption were covered in the roadmap and the corresponding organisational capabilities were defined in the maturity paths of each of the focus areas.

This culminated in a cloud maturity model that, mapped on METRI's model of the IT organisation, contains 14 focus areas spread out over four dimensions. The underlying focus areas and their respective maturity levels were formed through a combination of scientific literature and expert input, providing a model that was successfully applied in two case studies.

The results are generalisable to large organisations operating as consumers in the Dutch cloud computing market and potentially beyond that, as the experts participating in this thesis research operate in that market, with a subset of them operating in globally active organisations. The claim for generalisability is further supported by the models that inspired this cloud maturity model, which are in use globally.

8. Bibliography

- 1 A. Duarte and M.M. da Silva, "Cloud Maturity Model" in *IEEE Sixth International Conference on Cloud Computing*, Santa Clara, CA, USA, 2013, pp. 606-613.
- 2 A.D. Waite, "Hybrid Architectures for Cloud Computing", Gartner, 2016.
- 3 "Gartner Says Worldwide Public Cloud Services Market Is Forecast to Reach \$204 Billion in 2016", Gartner.com, 2016. [Online] Available: <http://www.gartner.com/newsroom/id/3188817>. [Accessed: 28-Sep-2016].
- 4 K.C. Laudon and J.P. Laudon, "Managing the digital firm" in *Managing Information Systems*, B. Horan, Ed. London: Pearson Education, 2004, pp. 197-200.
- 5 A.M. Sharif, "It's written in the cloud: the hype and promise of cloud computing", *Journal of Enterprise Information Management*, 2010, 23, (2), pp. 131-134.
- 6 S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang and A. Ghalsasi, "Cloud computing—The business perspective", *Decision support systems*, 2011, 51, (1), pp. 176-189.
- 7 C.S. Yoo, "Cloud computing: Architectural and policy implications", *Review of Industrial Organization*, 2011, 38, (4), pp. 405-421.
- 8 S.D. Müller, S.R. Holm and J. Søndergaard, "Benefits of cloud computing: Literature review in a maturity model perspective", *Communications of the Association for Information Systems*, 2015, 37, pp. 851-878.
- 9 M. Bayramusta and V.A. Nasir, "A fad or future of IT?: A comprehensive literature review on the cloudcomputing research", *International Journal of Information Management*, 2016, (36), pp. 635-644.
- 10 S. Rajendran, "Organizational challenges in cloud adoption and enablers of cloud transition program", Massachusetts Institute of Technology, 2013.
- 11 R. El-Gazzar, E. Hustad and D.H. Olsen, "Understanding cloud computing adoption issues: A Delphi study approach", *The Journal of Systems and Software*, 2016, 118, pp. 64-84.
- 12 T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges", in *24th IEEE International Conference on Advanced Information Networking and Applications*, AINA 2010, Perth, Australia, 2010, pp. 27-33.
- 13 G. Garrison, S. Kim and R.L. Wakefield, "Success factors for deploying cloud computing", *Communications of the ACM*, 2012, 55, (9), pp. 62-68.
- 14 RightScale, "2017 State of the Cloud Report", 2017.
- 15 G. Conway and E. Curry, "Managing Cloud Computing-A Life Cycle Approach", in *2nd International Conference on Cloud Computing and Services Science*, CLOSER 2012, Porto, Portugal, 2012, pp. 198-207.
- 16 J. Becker, R. Knackstedt and J. Pöppelbuss, "Developing Maturity Models for IT Management – A Procedure Model and its Application", *Business & Information Systems Engineering*, 2009, pp. 213-222.
- 17 A.M. Maier, J. Moultrie and P.J. Clarkson, "Assessing organizational capabilities: reviewing and guiding the development of maturity grids", *IEEE Transactions on Engineering Management*, 2012, 59, (1), pp. 138-159.
- 18 M. Van Steenberghe, R. Bos, S. Brinkkemper, I. Van De Weerd and W. Bekkers, "The design of focus area maturity models", in *Global Perspectives on Design Science Research*, DESRIST 2010, Gallen, Switzerland, 2010, pp. 317-332.
- 19 T. Mettler and P. Rohner, "Situational maturity models as instrumental artifacts for organizational design", in *4th international conference on design science research in information systems and technology*, DESRIST '09, Philadelphia, PA, USA, 2009, pp. 22.
- 20 T. De Bruin, R. Freeze, U. Kaulkarni and M. Rosemann, "Understanding the main phases of developing a maturity assessment model", in *Australasian Conference on Information Systems*, ACIS, Sidney, Australia, 2005.

- 21 A. Hevner, S. March, J. Park and S. Ram, "Design science in information systems research", *MIS quarterly*, 2004, 28, (1), pp. 75-105.
- 22 M.A. Vouk, "Cloud Computing – Issues, Research and Implementations", *Journal of Computing and Information Technology*, 2008, 16, (4).
- 23 J. Luftman and B. Derksen, "Key issues for IT executives 2012: Doing More with Less", *MIS Quarterly Executive*, 2012, 11, (4).
- 24 J. Avrane-Chopard, T. Bourgault, A. Dubey and L. Moodley, "Big Business in Small Business: Cloud Services for SMBs", *RECALL*, McKinsey Company, 2014.
- 25 RightScale, "2016 State of the Cloud Report", 2016.
- 26 H. Trivedi, "Cloud Adoption Model for Governments and Large Enterprises", Master Thesis, MIT Sloan School of Management, Cambridge, Massachusetts, 2013.
- 27 NIST, "The NIST Definition of Cloud", 2011 [Online] Available: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. [Accessed: 16 September 2016].
- 28 Q. Zhang, L. Cheng and R. Boutaba, "Cloud computing: state-of-the-art and research challenges", *Journal of internet services and applications*, 2010, 1, (1), pp. 7-18.
- 29 N. Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution", *Telecommunications Policy*, 2103, 37, (4-5), pp. 372-386.
- 30 Cloud Security Alliance, "The Notorious Nine Cloud Computing Top Threats in 2013", 2013. [Online] Available: <https://cloudsecurityalliance.org/media/news/ca-warns-providers-of-the-notorious-nine-cloud-computing-top-threats-in-2013/>. [Accessed: 24 September 2016].
- 31 M.T. Khorshed, A.S. Ali and S.A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing", *Future Generation computer systems*, 2012, 28, (6), pp. 833-851.
- 32 T. Mettler, P. Rohner and R. Winter, "Towards a classification of maturity models in information systems" in *Management of the interconnected world*, Physica-Verlag HD, 2010, pp. 333-340.
- 33 D. Smits and J. van Hillegersberg, "IT Governance Maturity: Developing a Maturity Model using the Delphi Method" in *48th Hawaii International Conference on System Sciences*, HICSS, 2015, pp. 4534-4543.
- 34 P. Fraser, J. Moultrie and M. Gregory, "The use of maturity models/grids as a tool in assessing product development capability", in *Engineering Management Conference*, IEMC'02, 2002, pp. 244-249.
- 35 K. Paulk, "Capability maturity model for software" in *Encyclopedia of Software Engineering*, 1993.
- 36 R. Pereira and M.M. da Silva, "A maturity model for implementing ITIL V3 in practice", in *15th IEEE International Enterprise Distributed Object Computing Conference Workshops*, EDOCW, 2011, pp. 259-268.
- 37 D. Raber, J. Epple, R. Winter and M. Rothenberger, "Closing the Loop: Evaluating a Measurement Instrument for Maturity Model Design" in *49th Hawaii International Conference on System Sciences*, HICSS, 2016, pp. 4444-4453.
- 38 F.W. van Dijk, "An Assessment of Cloud Maturity Models", University of Twente Research Topics Report, unpublished, receivable from the author and the supervisors, January 2017.
- 39 B. Kitchenham, "Procedures for performing systematic reviews", Keele University, Keele, UK, 2004.
- 40 S. Okai, M. Uddin and A. Arshad, "Cloud computing adoption model for universities to increase ICT proficiency", *SAGE Open*, 2014, 4, (3).
- 41 N. Alkhater, V. Chang, G. Wills and R. Walters, "Towards an Integrated Conceptual Model for Cloud Adoption in Saudi Arabia", 2015.

- 42 D. Weiss, J. Repschlaeger, R. Zamekov and H. Schroedl, 'Towards a Consumer Cloud Computing Maturity Model-Proposition of Development Guidelines, Maturity Domains and Maturity Levels' in *2013 Pacific Asia Conference on Information Systems, PACIS*, 2013, p. 211.
- 43 Open Data Center Alliance, "Cloud Maturity Model Rev. 3.0", 2016. [Online] Available: <https://opendatacenteralliance.org/article/cloud-maturity-model-rev-3-0/>. [Accessed: 20 October 2016].
- 44 Amazon Web Services, "Cloud Transformation Maturity Model: Guidelines to Develop Effective Strategies for Your Cloud Adoption Journey", 2016. [Online] Available: <https://aws.amazon.com/blogs/publicsector/cloud-adoption-maturity-model-guidelines-to-develop-effective-strategies-for-your-cloud-adoption-journey/>. [Accessed: 24 October 2016].
- 45 Amazon Web Services, "An Overview of the AWS Cloud Adoption Framework", 2016. [Online] Available: https://d0.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf. [Accessed 24 October 2016].
- 46 V. Alvarez, J. Staten and J. McKee, "Assess Your Cloud Maturity", Forrester Research, 2012.
- 47 P. Jadhvani, J. MacKinnon and M. Elrefai, "Cloud Computing Building a Framework for Successful Transition", GTSI Solutions, 2009.
- 48 G.J. Skulmoski, F.T. Hartman and J. Krahn, "The Delphi method for graduate research", *Journal of information technology education*, 2007, 6, pp. 1.
- 49 N.C. Dalkey, B.B. Brown and S. Cochran, "The Delphi method: An experimental study of group opinion", Rand Corporation, Santa Monica, CA, USA, 1969.
- 50 J.A. Somerville, "Critical factors affecting the meaningful assessment of student learning outcomes: a Delphi study of the opinions of community college personnel", Oregon State University, 2007.
- 51 J.F. Coates, "In defense of Delphi:: A review of Delphi assessment, expert opinion, forecasting, and group process by H. Sackman", *Technological Forecasting and Social Change*, 1975, 7, (2), pp. 193-194.
- 52 H.A. Linstone and M. Turoff, "Delphi: A brief look backward and forward", *Technological Forecasting and Social Change*, 2011, 78, (9), pp. 1712-1719.
- 53 C. Okoli and S.D. Pawlowski, "The Delphi method as a research tool: an example, design considerations and applications", *Information & management*, 2004, 42, (1), pp. 15-29
- 54 Open Data Center Alliance, 'Cloud Maturity Model 3.1 Package", 2016.
- 55 T. Panagacos, "The Ultimate Guide to Business Process Management: Everything you need to know and how to apply it to your organization", Amazon, 2012 .
- 56 Object Management Group, "Business process maturity model (BPMM) version 1.0", 2008. [Online] Available: <http://www.omg.org/spec/BPMM/1.0/>. [Accessed: 25 December 2016].
- 57 D.M. Fisher, "The business process maturity model: a practical approach for identifying opportunities for optimization", *Business Process Trends*, 2004, 9, (4), pp. 11-15.
- 58 European Commission, "Questions and Answers - Data protection reform ", 2015. [Online] Available: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm. [Accessed: 12 March 2017].
- 59 D. Yimam and E.B. Fernandez, "A survey of compliance issues in cloud computing", *Journal of Internet Services and Applications*, 2016, 7, (1), pp. 1-12.
- 60 E. Tittel and K. Lindros, "Your guide to compliance in the cloud", CIO.com, 2015. [Online] Available: <http://www.cio.com/article/2901034/cloud-computing/your-guide-to-compliance-in-the-cloud.html>. [Accessed: 15 February 2017].
- 61 R. Accorsi, L. Lowis and Y. Sato, "Automated certification for compliant cloud-based business processes", *Business & Information Systems Engineering*, 2011, 3, (3), pp. 145.
- 62 Gartner, "DMI (data management and integration)", n.d. [Online] Available: <http://www.gartner.com/it-glossary/dmi-data-management-and-integration>. [Accessed: 29 March 2017].

- 63 R. Wolter and K. Haselden, "The What, Why, and How of Master Data Management", Microsoft Corporation, 2006. [Online] Available: <https://msdn.microsoft.com/en-us/library/bb190163.aspx>. [Accessed: 4 February 2017].
- 64 H. Hosseini, "Now Available: Cloud Analytics for Cloud Cost Management", RightScale, 2014. [Online] Available: <http://www.rightscale.com/blog/cloud-cost-analysis/now-available-cloud-analytics-cloud-cost-management>. [Accessed: 10 January 2017].
- 65 M. Lankhorst, "Introduction to enterprise architecture" in *Enterprise Architecture at Work*, Springer, 2013, pp. 3.
- 66 M. Xin, and N. Levina, "Software-as-a-service model: Elaborating client-side adoption factors", 2008.
- 67 M. Ramachandran, "Component-based development for cloud computing architectures" in *Cloud Computing for Enterprise Architectures*, Springer, 2011, pp. 91-114.
- 68 Gartner, "IT Operations", n.d. [Online] Available: <http://www.gartner.com/it-glossary/it-operations>. [Accessed: 22 Februari 2017].
- 69 ISACA, "ISACA Cybersecurity Fundamentals Glossary", 2016. [Online] Available: https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf. [Accessed: 2 June 2017].
- 70 Cloud Standard Customer Council, "Cloud security standards: what to expect & what to negotiate", 2013. [Online] Available: <http://www.cloud-council.org/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf>. [Accessed 14 May 2017].
- 71 A. Wiggins, "The Twelve-Factor App", 2017. [Online] Available: <https://12factor.net/>. [Accessed 29 May 2017].
- 72 M. McDonald, "Digital Strategy Does Not Equal IT Strategy", *Harvard Business Review*, 2012, 19.
- 73 J. Varia, "Architecting for the cloud: Best practices", Amazon Web Services, 2010, 1. [Online] Available: https://d0.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf. [Accessed: 18 January 2017].
- 74 P.B. Seddon and R. Scheepers, "Towards the improved treatment of generalization of knowledge claims in IS research: drawing general conclusions from samples", *European Journal of Information Systems*, 2012, 21, (1), pp. 6-21

Appendix A

Introduction Mail Cloud Maturity Research

Dear ...,

METRI is developing a Cloud Maturity Model in collaboration with the Universiteit Twente. The reason for this research is the explosive growth of cloud computing as an IT service delivery model. The research is conducted by Friso van Dijk, as the final step in attaining his master's degree Business & IT at the Universiteit Twente. He is being guided by Michael Chin, Director Sourcing and Governance at METRI.

The Cloud Maturity Model aims to give organisations the means to realise their cloud strategy. It provides an overview of the available cloud solutions, and the required capabilities and milestones to adopt these in an organisation. It allows an organisation to assess its cloud maturity, and to create a roadmap to take its cloud computing capabilities to the next level.

To realise this, we are reaching out to you as a cloud expert to participate in this research as part of an **expert panel**. This panel will be presented with four survey rounds, each on a different topic, and containing the results from previous rounds. These four rounds are used to create the Cloud Maturity Model. The Cloud Maturity Model will be validated through case studies, and the final model will be presented to the panel, with the (optional) possibility to provide feedback.

The survey questions are structured to obtain expert input and in-depth content. The survey dates and estimated required time investment are:

Date	Survey topic	Time
5 December 2016	Cloud solutions validation	30 mins
19 December 2016	Capabilities brainstorm (online)	45 mins
16 January 2017	Capabilities validation (online)	45 mins
6 February 2017	Model validation	30 mins
3 April 2017	Iterated model validation	30 mins

During the research, METRI will publish several whitepapers on Cloud Maturity, containing the most important findings of the study. These whitepapers will be published through METRI Research (www.metriresearch.com). Participants will enjoy free access to these whitepapers, as well as a testimony of participation.

As a conclusion of the research, all expert participants will be invited to join a model presentation, together with METRI consultants.

A more expansive research plan can be found in the attached document.

With kind regards,

...

Appendix B

First survey cloud maturity

Welcome and thank you for participating in this study. This survey is the first of a series of five, with a longer gap between the fourth and fifth surveys. This survey will take around 30 minutes to complete.

In this survey, we present an initial model based on literature research and expert insight. The goal of this survey is to validate or revise the model based on your input. The revised model will be shown again in the following survey.

Please keep in mind that there are no wrong answers. Our purpose here is to gather insights and we value all opinions equally. Our reasoning behind the creation of the model has purposefully been left out, to eliminate bias as much as possible. All data will be anonymised, and aggregated where possible.

Within this study, we will use the NIST definition of cloud computing:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

This definition includes three service models: IaaS, PaaS, and SaaS. Other as-a-Service models, such as Security-as-a-Service, are out of scope of the model or are a subgroup of one of the three service models, such as Workplace-as-a-Service.

Section 1: Introduction

Introductory questions

First off, we need to know a little about your company, function, and involvement with cloud computing. This data will be used to create a better picture of the panel composition.

The answers do not require highly specific information, but should be detailed enough to create an accurate image.

As mentioned, all data will be anonymised, and aggregated where possible.

What is your company's involvement with cloud computing?

Think of items such as private/public cloud, type of cloud services used, and if applicable, the type of cloud services offered.

Answer option: textbox.

What is your function within the company?

Include your involvement with cloud computing.

Answer option: textbox.

What is your personal experience with cloud computing?

Answer option: textbox.

Section 2: Cloud Domains

Conceptual cloud maturity model

The following questions will come with a conceptual Cloud Maturity Model. This model has been developed based on a literature study and expert insight. The questions will base themselves on elements on the model, and often ask for

extra input to gather insight in your thought process. First, we will provide questions on the model elements, and later on the order and overall structure of the model.

You can find the model attached on the right side of the screen on each page from now on.

The model consists of 5 maturity levels, each level representing a higher cloud maturity. It is not required that organisations finish all of level one to move to level two, as maturity can differ with each cloud domain.

On the left-hand side, a distinction has been made between three cloud domains: Infrastructure, Platform, and Software, to reflect the three cloud service types (IaaS, PaaS, and SaaS). The following questions will focus on this distinction.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Virtualization	IaaS replacing on premise		Cloud-native infrastructure	Cloud optimized infrastructure
Platform		Pre-PaaS	Developing with PaaS	Redesigning for PaaS	Cloud optimized PaaS
Software	WPaaS SaaS Point solutions		Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS

Answer options for this section:

Five-point Likert scale: strongly disagree, disagree, neither agree nor disagree, agree, strongly agree.

Optional textbox.

The distinction in three Cloud Domains is a logical one

Section 3 Infrastructure Domain

Infrastructure Domain

Each of the Cloud Domains contains several elements. The following questions are aimed to validate or improve the model. They will follow the structure of first validating the elements, and then validating the maturity path.

The Infrastructure domain follows the following path:

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Virtualization	IaaS replacing on premise		Cloud-native infrastructure	Cloud optimized infrastructure

The model elements are as follows:

Virtualization : leveraging virtualization techniques across data centers.

IaaS replacing on premise : private and public cloud IaaS solutions replace the on premise infrastructure. The architecture as-is is being moved on top of an IaaS solution.

Cloud-native infrastructure : the architecture is redesigned to leverage IaaS benefits.

Cloud-optimised infrastructure : deployment of complex IaaS services across multiple cloud domains (both private and public). The IaaS solutions are optimised for seamless integration between the different cloud services.

Answer options for this section:

Five-point Likert scale: strongly disagree, disagree, neither agree nor disagree, agree, strongly agree.

Optional textbox.

To what extent do you agree with this statement? And why?

- Virtualization is a part of cloud infrastructure maturity.
- IaaS replacing on premise is a part of cloud infrastructure maturity.
- Cloud-native infrastructure is a part of cloud infrastructure maturity.
- Cloud optimized infrastructure is a part of cloud infrastructure maturity.

Seeing this cloud domain, are there any elements you think are missing?

Answer option: textbox.

Section 4: Platform Domain

Platform Domain

The Platform domain follows the following path:

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Platform		Pre-PaaS	Developing with PaaS	Redesigning for PaaS	Cloud optimized PaaS

The model elements are as follows:

Pre-PaaS : application features are bundled and placed on IaaS.

Developing with PaaS : new applications and features are developed on a vendor-provided PaaS.

Redesigning for PaaS : existing applications are redesigned to leverage PaaS benefits.

Cloud optimized PaaS : automated deployments, with orchestration systems locating relevant data and applications in the cloud landscape, and migrating them according to business requirements.

Answer options for this section:

Five-point Likert scale: strongly disagree, disagree, neither agree nor disagree, agree, strongly agree.

Optional textbox.

To what extent do you agree with this statement? And why?

- Pre-PaaS is a part of cloud platform maturity.
- Developing with PaaS is a part of cloud platform maturity.
- Redesigning for PaaS is a part of cloud platform maturity.
- Cloud optimized PaaS is a part of cloud platform maturity.

Seeing this cloud domain, are there any elements you think are missing?

Answer option: textbox.

Section 5: Software Domain

The Software domain follows the following path:

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Software	WPaaS		Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS
	SaaS Point solutions				

The model elements are as follows:

WPaaS (Workplace-as-a-Service) : WPaaS provides companies with a suite of standardised workplace tools, such as text processors, spreadsheets and presentation tools from a cloud environment. Notable vendors are Google Suite and Office365.

SaaS point solutions : SaaS solutions adopted for a single business use, which requires little to no integration with the existing application landscape.

SaaS secondary processes : secondary business processes, such as Finance and HR, migrate to SaaS solutions.

SaaS primary processes : primary business processes are moved to the cloud, which requires more organisational capabilities than secondary processes.

Hybrid SaaS : fully leveraging technological possibilities of seamless integration between public and private clouds. Parts of application landscape containing sensitive data, time-sensitive processes or data-heavy processes can be hosted on a private cloud, with seamless integration with applications in public clouds.

Answer options for this section:

Five-point Likert scale: strongly disagree, disagree, neither agree nor disagree, agree, strongly agree.

Optional textbox.

To what extent do you agree with this statement? And why?

- WPaaS is a part of cloud software maturity.
- SaaS point solutions is a part of cloud software maturity.
- Secondary processes SaaS is a part of cloud software maturity.
- Primary processes SaaS is a part of cloud software maturity.
- Hybrid SaaS is a part of cloud software maturity.

Seeing this cloud domain, are there any elements you think are missing?

Answer option: textbox.

Section 6: Maturity Levels

Maturity Levels

The final segment of this survey focuses on the model as a whole. You are asked to validate the order of the elements, and your reasoning behind this. It is important to motivate your answers, even when you agree with the model, as we want to understand your reasoning behind it.

As a refresher, the full model has been attached to this page.

Answer options for this section:

Five-point Likert scale: strongly disagree, disagree, neither agree nor disagree, agree, strongly agree.

Optional textbox.

The order of the elements of the infrastructure domain in the total model make sense to me.

The order of the elements of the platform domain in the total model make sense to me.

The order of the elements of the software domain in the total model make sense to me.

Take into account the order of the infrastructure elements within the whole model. Are there things that should be changed?

Is there anything else you would change about the model?

Do you have any further remarks on the survey?

Final Page

Thank you for filling out the survey. The next survey will be sent out on 19 December 2016 . There was a mistake in the table sent out in the email, which said 18 December 2016 , we apologise for the inconvenience.

If you have any further questions or remarks during the waiting time, feel free to contact Friso van Dijk at xxx@xxx or +316xxxxx

You can now safely close this page, or click the NEXT button and be redirected to the login screen. You can revise your answers by simply logging in once again, until the survey closes on 9 December 2016 .

Appendix C

Second survey cloud maturity

Welcome to the second survey. First off, I would like to thank you all for the great response on the first survey. There were a lot of interesting answers, and we will take them all into consideration. That being said, not all answers are reflected in the changed model. This is because we need to have a basis to gather capabilities for cloud computing. Your comments and considerations have not been neglected, but we are waiting with further changes until later in the study.

As mentioned, the model has been changed based on your answers. This survey will kick off with a few more questions on the model, after which we pose a set of brainstorm questions. In the brainstorm questions, we ask you to name **organisational capabilities** related to each of the maturity levels (there are 5 brainstorm questions). You can come back at all times until the survey closes to add responses.

Once again, please keep in mind that there are no wrong answers. Our purpose here is to gather insights and we value all opinions equally.

Section 1: Changes to the model

Changes to the model

We have made several changes to the model, which you can see pictured below. The justification for the changes can be read below. On the right side, you find the following documents:

- **Second model.png** - this is the second iteration of the model, which can be seen below.
- **conceptual model_final.png** - this is the first model to serve as a reminder.
- **Level descriptions.pdf** - this document contains the descriptions of a company on each of the maturity levels. These will be presented again in the brainstorm, but can help with clarifying the model.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Legacy apps on dedicated infrastructure	IaaS replacing on premise		Cloud-native infrastructure	Cloud-optimized infrastructure
Platform			PaaS development		
			Application stack on PaaS	Redesigned applications for PaaS	Cloud-optimized PaaS
Software		Mature cloud solutions			
		SaaS Point solutions	Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS

Level 1

We had several participants saying that *virtualization* is more of an enabler and that it was not really cloud computing. On top of that, several suggestions were given for similar items in the other cloud domains. This led us to change the first level of the maturity model to a starting point, which represents a company moving into cloud computing.

Level 2

Based on the responses, we have decided to remove *Pre-PaaS* from the model. As some of you noted, this was not PaaS, but more an extension of IaaS replacing on premise.

We have also renamed *WPaaS* to *Mature cloud solutions*, as the scope of WPaaS appeared to be too narrow. *Mature cloud solutions* has been defined as a mature, easy to implement cloud offering that is not a secondary or primary process. WPaaS is but one example of this.

SaaS point solutions remains as-is. We found that there was some confusion about the term, and we have attempted to solve this by giving a description of a company progressing through the maturity model.

Level 3

The third level has seen the addition of *Application stack on PaaS*. This was mentioned as a step on the same maturity level as Paas development, and we have decided to add it instead of Pre-PaaS, which is a more sensical description.

Level 4 & 5

These levels have not been changed, but some of the definitions and wordings have been altered to better communicate their meaning.

To what extent do you agree with this statement? And why?

The new Level 1 of the maturity model makes sense to me.

Level 1 description (example company)

The level 1 organisation is looking to move to cloud computing. Their application landscape is hosted on dedicated infrastructure. Some individuals or teams already use SaaS offerings, but these are stand-alone, and not integrated or centrally managed.

Please elaborate on your answer.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Legacy apps on dedicated infrastructure	IaaS replacing on premise		Cloud-native infrastructure	Cloud-optimized infrastructure
Platform			PaaS development	Redesigned applications for PaaS	Cloud-optimized PaaS
			Application stack on PaaS		
Software		Mature cloud solutions	Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS
		SaaS Point solutions			

To what extent do you agree with this statement? And why?

The new Level 2 of the maturity model makes sense to me.

Level 2 description (example company)

The level 2 organisation has successfully adopted some cloud services in one or more of the cloud domains. IaaS has successfully replaced their dedicated infrastructure (either on private or public cloud). They now have incorporated a mature cloud solution (Office365), and a SaaS point solution is now available organisation-wide (a Gantt chart tool).

Please elaborate on your answer.

To what extent do you agree with this statement? And why?

The new Level 3 of the maturity model makes sense to me.

Level 3 description (example company)

The level 3 organisation has successfully moved their secondary business processes to the cloud and has started integrating the different solutions. They have started developing new services on a PaaS solution, and have moved their existing application stack on the PaaS platform. They have also shifted their secondary business processes to the cloud, as they now use SaaS solutions for HR and Finance.

Please elaborate on your answer.

To what extent do you agree with this statement? And why?

The new Level 4 of the maturity model makes sense to me.

Level 4 description (example company)

The level 4 organisation has made large steps towards being a cloud-mature organisation. Their primary business processes (such as Sales and Operation planning) are using SaaS and PaaS solutions. The infrastructure has become cloud-native (fully abstracted infrastructure, including storage, networking, and compute layers which can be consumed on-demand and programmatically), and the applications running on the PaaS platform have been redesigned to fully leverage its benefits.

Please elaborate on your answer.

To what extent do you agree with this statement? And why?

The new Level 5 of the maturity model makes sense to me.

Level 5 description (example company)

The level 5 organisation has realised the full potential of cloud computing. It uses cloud brokerage to integrate the application landscape diffused over multiple cloud providers (including private cloud), and the IT organisation is more business oriented, focusing on IT direction and servicing business needs by offering virtual stacks by design and microservices.

Please elaborate on your answer.

Section 2: Brainstorm Session

Brainstorm session

In this brainstorm session, we are looking for **organisational capabilities** related to cloud computing. An organisational capability is '*an organisation's ability to manage resources*'. Each section of the brainstorm covers one maturity level, for all cloud domains. This has been done to also cover items general for the whole maturity level. The capabilities will be coupled to the correct elements in the next survey.

As a brainstorm session, no suggestion is regarded as bad or unrelated. Since you will be able to see the anonymised responses of other participants, it may happen that you feel a point made by another participant is unclear or ill defined. In that case, feel free to add another item with similar contents, explaining the idea better. The goal of this session is to **generate capabilities**, which will be processed and offered for evaluation in the next session.

With each maturity level, a description is given of an organisation that would have reached that maturity level for each of the domains. This will help clarify the scope of that maturity level.

We have also provided an unstructured set of items to use as inspiration, displayed on the right side of the screen. Please note that these items are not capabilities, but can be subject of capabilities. The list is distilled from several sources focusing on cloud adoption and IT roles, but is not supposed to be exhaustive.

Please be descriptive in your answers.

List on right side

Roles for inspiration

IT Governance
 Security, Privacy, Compliance and Risk Management
 Line Management
 IS Service Portfolio Management
 Vendor/Cloud Portfolio Management
 IS Service Design
 Information Management
 IS Service Ownership
 Vendor and Contract Management
 Service Level Management
 Organizational Change Management
 Enterprise/Cloud Architecture
 Enterprise Data Management
 Enterprise Application Integration
 Software Refactoring and Redesign
 (Continuous) Deployment
 IT Service Operation
 Cloud Consumption Management
 Service Desk / IT Support
 Service Integration and Management (SIAM)
 Project Management
 Business Process Management
 Network Management
 Software Development Management

Maturity Level 1

Please provide as many **organisational capabilities** you can think of. The list on the right side of the screen is meant for inspiration.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Legacy apps on dedicated infrastructure	IaaS replacing on premise		Cloud-native infrastructure	Cloud-optimized infrastructure
Platform			PaaS development Application stack on PaaS	Redesigned applications for PaaS	Cloud-optimized PaaS
Software		Mature cloud solutions	Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS
		SaaS Point solutions			

The level 1 organisation is looking to move to cloud computing. Their application landscape is hosted on dedicated infrastructure. Some individuals or teams already use SaaS offerings, but these are stand-alone, and not integrated or centrally managed.

You can **edit your answers** by clicking on the orange texts in the list of answers below.

Maturity Level 2

Please provide as many **organisational capabilities** you can think of. The list on the right side of the screen is meant for inspiration.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Legacy apps on dedicated infrastructure	IaaS replacing on premise		Cloud-native infrastructure	Cloud-optimized infrastructure
Platform			PaaS development Application stack on PaaS	Redesigned applications for PaaS	Cloud-optimized PaaS
Software		Mature cloud solutions SaaS Point solutions	Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS

The level 2 organisation has successfully adopted some cloud services in one or more of the cloud domains. IaaS has successfully replaced their dedicated infrastructure (either on private or public cloud).

They now have incorporated a mature cloud solution (Office365), and a SaaS point solution is now available organisation-wide (a Gantt chart tool).

You can **edit your answers** by clicking on the orange texts in the list of answers below.

Maturity Level 3

Please provide as many **organisational capabilities** you can think of. The list on the right side of the screen is meant for inspiration.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Legacy apps on dedicated infrastructure	IaaS replacing on premise		Cloud-native infrastructure	Cloud-optimized infrastructure
Platform			PaaS development Application stack on PaaS	Redesigned applications for PaaS	Cloud-optimized PaaS
Software		Mature cloud solutions SaaS Point solutions	Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS

The level 3 organisation has successfully moved their secondary business processes to the cloud and has started integrating the different solutions. They have started developing new services on a PaaS solution, and have moved their existing application stack on the PaaS platform.

They have also shifted their secondary business processes to the cloud, as they now use SaaS solutions for HR and Finance

You can **edit your answers** by clicking on the orange texts in the list of answers below.

Maturity Level 4

Please provide as many **organisational capabilities** you can think of. The list on the right side of the screen is meant for inspiration.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5	
Infrastructure	Legacy apps on dedicated infrastructure	IaaS replacing on premise		Cloud-native infrastructure	Cloud-optimized infrastructure	
Platform		PaaS development		Redesigned applications for PaaS	Cloud-optimized PaaS	
		Application stack on PaaS				
Software		Mature cloud solutions		Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS
		SaaS Point solutions				

The level 4 organisation has made large steps towards being a cloud-mature organisation. Their primary business processes (such as Sales and Operation planning) are using SaaS and PaaS solutions. The infrastructure has become cloud-native (fully abstracted infrastructure, including storage, networking, and compute layers which can be consumed on-demand and programmatically), and the applications running on the PaaS platform have been redesigned to fully leverage its benefits.

You can **edit your answers** by clicking on the orange texts in the list of answers below.

Maturity Level 5

Please provide as many **organisational capabilities** you can think of. The list on the right side of the screen is meant for inspiration.

Cloud Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Infrastructure	Legacy apps on dedicated infrastructure	IaaS replacing on premise		Cloud-native infrastructure	Cloud-optimized infrastructure
Platform		PaaS development		Redesigned applications for PaaS	Cloud-optimized PaaS
		Application stack on PaaS			
Software		Mature cloud solutions	Secondary processes SaaS	Primary processes SaaS	Hybrid SaaS
		SaaS Point solutions			

The level 5 organisation has realised the full potential of cloud computing. It uses cloud brokerage to integrate the application landscape diffused over multiple cloud providers (including private cloud), and the IT organisation is more business oriented, focusing on IT direction and servicing business needs by offering virtual stacks by design and microservices.

You can **edit your answers** by clicking on the orange texts (your answers) in the list of answers below.

Is there anything else you would like to add?

Final page

Thank you for filling out the survey. This survey remains available until 3 January 2017 . You can come back at any time until then and add or edit your answers. The next survey will be sent out on 16 January 2017 .

If you have any further questions or remarks during the waiting time, feel free to contact Friso van Dijk at xxx@xxx or +316xxxxx

You can now safely close this page, or click the NEXT button and be redirected to the login screen.

Appendix D

Third survey cloud maturity

Welcome to the third survey. Thank you all for the responses on the previous survey. The answers were broader than we initially suspected, which has caused us some delay.

All answers are, like the second half of the previous survey, visible to all participants. Feel free to comment, expand or emphasise on certain answers. We encourage you to revisit the survey in a later stage to do so if time permits.

Once again, please keep in mind that there are no wrong answers. Our purpose here is to gather insights and we value all opinions equally.

Section 1: Focus Area descriptions

State of the research

Based on the brainstorm session in the previous survey we selected a set of focus areas in which we grouped your answers. Each focus area has a description attached for each maturity level. The purpose of this survey is to validate or improve these descriptions to fit a common view of cloud maturity.

We have identified the following focus areas:

IT Architecture
Cloud Strategy
Compliance
Security
Financial
Vendor management
Data management
Operations
Business process management
Infrastructure
Platform
Software
Governance
Software development

Each of the focus areas will be presented with a description of its maturity per level. Afterwards, we will ask you about the whole set of focus areas.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: IT Architecture

Level 1

Cloud is not applied to architecture.

Level 2

Cloud is considered when developing workflows and the use of RESTful APIs and cloud service interfaces emerge.

Level 3

Cloud services are considered in planning and processes are documented. Cloud design patterns are leveraged and standard cloud environment management tools are used.

Level 4

Cloud service principles are a core element of architectural planning. Services can be modelled online, leveraging cloud building blocks. Services construction with automated integration into support processes.

Level 5

Service components are modelled with a single set of tools, utilised for deploying and managing a highly automated and optimised cloud ecosystem. Application integration and infrastructure are transparent.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Cloud Strategy

Level 1

Different views on cloud computing exist, with some common understanding of the business benefits of adopting cloud.

Level 2

Common enterprise-wide cloud strategy exists, but ad hoc adoption of cloud services. The impact of cloud services on organisation has been identified.

Level 3

Key steps and enablers for further cloud adoption have been identified. KPIs are defined to measure strategy impact.

Level 4

All-in cloud strategy guides all new deployments and cloud services. Use and success of implementing cloud strategy are reviewed on KPIs.

Level 5

Enterprise-wide knowledge gathering to identify improvement and growth areas. Cloud strategy enables growth and optimisation of business outcomes and is regularly revised for technological developments.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Compliance

Level 1

No corporate policies or guidelines related to cloud computing are readily available.

Level 2

Compliance requirements are made available and communicated. The compliance framework is redefined to be cloud-aware. Implementations of cloud services follow predefined procedures to ensure compliance.

Level 3

Processes are in place to check selected areas for compliance regularly and consequences of deviation are analysed. Internal management reports are linked to each of the transitioning cloud services.

Level 4

Compliance requirements are communicated to the ecosystem in a standardised format. Online management and monitoring systems are in place, events of non-compliance are defined automatically where possible. Compliance-aware management tools support real-time monitoring.

Level 5

Compliance communications now have corresponding feedback loops. Corrective and preventative measures are taken based on automatic analysis. Continuous improvement of used framework, analysis and communication methods.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Security

Level 1

Little understanding of cloud security, without any formal procedures.

Level 2

Data security and privacy are evaluated on a project level for cloud. Applications are grouped and requirements are set for business critical applications.

Level 3

A set of standard policies and procedures is published for use when adopting cloud services for all types of services. A clear differentiation is made between privacy and security. Audits are defined and performed regularly. Reports are generated when requested.

Level 4

Existing cloud services are aligned to the standards. Monitoring against rules and policies, with automated reporting on issues. Security data is generated and automatically monitored against KPIs. Regular audits and assessments ensure data policy. Security requirements are integrated with architecture.

Level 5

The security concept is reviewed regularly. Uniform security processes are in place within a security framework that monitors the cloud landscape in real-time with automated reporting. Automated audits ensure implementation of defined privacy and security requirements.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Financial

Level 1

IT budget without usage based cost distribution. Some projects are paid for by business on a non-usage based level

Level 2

Move towards pay-per-use costing, but infrequently billed internally and on a predetermined pricing model. Capital expenses are going through defined cycles. Operating expenses are collected at the end of each month and assigned to IT costs.

Level 3

IT costs are distributed based on general usage. Consumers can check their ordered services and corresponding costs. Financial reporting and source data are available in real-time according to pre-defined financial parameters.

Level 4

IT costs are charged per use to the business units, and the business has a constant view of the actual costs. Standard online contracts and supply management are integrated with supplier systems.

Level 5

Constant cost monitoring in which growing costs are discussed with the business units. Integrated reporting and sharing of relevant data ensures pre-warning of procurement events and that service quality can be monitored and managed pro-actively.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Vendor management

Level 1

No differentiation between regular and cloud SLAs, with no cloud-specific processes in place.

Level 2

Cloud is fitted to match internal processes. Infrastructure SLAs are used to measure services. Defined products and contracts exist with partners with zero value commitments.

Level 3

Standardised supplier contracts are defined. KPIs are defined for the expected benefits of cloud. Services and contracts are standardised and aligned to enable constant decision making.

Level 4

Standard online contract and supply management is integrated with supplier systems, existing contracts are synchronised to common terms and processes. KPIs are defined and automatically monitored for service delivery. Real-time reporting on existing contracts enable trend analysis to identify exceptions.

Level 5

Integrated reporting and sharing of relevant data with cloud providers. Business processes are integrated. Services can be aligned to meet business needs based on historical trends and data-driven predictions.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Data management

Level 1

Limited data access and availability controls exist. Internal criteria and controls exist for managing data. Data management requires human knowledge of data and location.

Level 2

A limited number of applications use cloud management services. Data management processes are documented in a data management framework and information sharing policies are defined. An enterprise data management function manages key master data sources. Standardised access to data repositories is realised.

Level 3

A published data management framework exists, policies are enforced. Data access and availability controls are

consistently applied across the organisation. A central set of database technologies is implemented to support a scale-out database architecture. Data object access through APIs is emerging.

Level 4

Metadata is encoded and stored in a CMS/data warehouse and management processes are based on storage and business metadata. Access and availability of data are continually reviewed. Applications use cloud-based data services. Real-time access to data through managed access points. Semantic search engine capabilities available to support data analysis.

Level 5

The data management framework is an integral part of the overall operating model. Information access and data security controls are integrated into the data ecosystem. Data services supporting applications are behind access APIs. An enterprise-wide data lake has been implemented. Data is accessible through APIs and discoverable through API calls to a service brokerage catalogue. On-premise and cloud data are integrated in a seamless manner.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Operations

Level 1

Demand management does not take cloud into consideration. Cloud service risk and compliance management processes do not exist.

Level 2

Cloud demand management emerges. Service, risk and compliance management processes are in place across the organisation, but not integrated with cloud provider processes. Most applications use compute and storage virtualization. Some operation tools are used to monitor workloads off-premise. Cloud services in use have at least one representation in a CMDB.

Level 3

Consistent processes for demand management have been defined. Processes for service, risk and compliance management allow for manual navigation of single issues. Leveraging virtualization for legacy applications extends to the network layer. Automation technologies are used to manage legacy.

Level 4

Processes for demand management and shared automated processes used, with attached KPIs and reporting. Service, risk and compliance management processes are integrated between cloud consumer and provider. Cloud services are integrated across the full technology stack, providing support for legacy. Tooling is being replaced by cloud provided tools.

Level 5

Systems automatically adjust to changing demand. Best placement of resources is determined through the use of KPIs and metadata. Service, risk and compliance management processes seamlessly process incidents. Legacy systems seamlessly integrated with virtualization technologies. Transactions span across the entire hybrid landscape. Workloads are managed from a centralised position and existing tools are integrated into a single tool.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Business process management

Level 1

Some business product process chains are documented, showing involved IT elements.

Level 2

Every BP is documented with its underlying IT systems, SLAs and OLAs for handling transactions. Some element interfaces underpinning the business process are documented.

Level 3

Common elements are aligned from a semantics and data handling perspective. A migration and consolidation plan is created for processes moving to the cloud. Moving processes are adapted to fit COTS solutions where possible. Common semantics are applied to systems and well-documented interface characteristics enable dynamic messaging queue interaction.

Level 4

Performance of common IT elements is measured in the combined BPs, with alerting in place for performance thresholds. Systems are categorised and located according to the data they hold for the BPs. Application elements underlying BPs are designed according to well-documented cloud-native models and frameworks.

Level 5

IT elements underlying the BP are automatically tested and monitored on IT metrics. Processes are regularly updated to align with business objectives more effectively. Automatic system scaling according to real-time BP needs. BP testing and monitoring is automated. Ad hoc BPs are designed, implemented, and monitored with supporting microservices, and eventually retired.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Infrastructure**Level 1**

No infrastructure processes for the leveraging of IaaS and containerisation exist.

Level 2

Virtualised infrastructure services support separate requests triggered via a provider tool. Container management systems are used to automate container creation and management. Some IaaS reporting exists based on provider's shared monitoring data. IaaS services are available for limited design elements that align with available services.

Level 3

Virtualised infrastructure services allow for a standard interface to collect monitoring and alerting data. They are made available to external provider portals for orchestration processes through a common portal. Virtualised infrastructure components are defined to support a standardised automation virtualisation system integrated into a CMDB. IaaS frameworks allow for repeatable instances.

Level 4

Virtualised infrastructure services support automated deployment. Event monitoring is bound to each IaaS provider. Design blueprints are defined for IaaS and allow systematic re-use of key elements. Virtualised infrastructure supports automatic scaling. Use of containers is standardised. IaaS is implemented with well-defined standards and interfaces. Performance is automatically monitored against KPIs.

Level 5

IaaS supports all data in the landscape and is managed with a single set of policies and rules. Virtualised infrastructure components allow on-premise systems to scale to the cloud. IaaS services are built with interoperable design elements, enabling cross-cloud application and service design. Virtualised infrastructure services are optimised to host and migrate resources to meet business objectives and allow for a Cloud Service Broker to select from available cloud services and platforms.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Platform**Level 1**

Applications are built using traditional development practices.

Level 2

Developers use IaaS (virtualised infrastructure) to deploy non-cloud applications. Applications are integrated using standard, non-proprietary integration interfaces.

Level 3

PaaS is used to develop new applications. Application structures are starting to use shared integration components. Application stacks are defined and common elements are stored in a database.

Level 4

Re-usable service elements are available and maintained. Developers use cloud design patterns, focusing on re-using existing elements. Integration, presentation and data services are provided using PaaS APIs. Automatic provisioning and scaling is available. Different cloud platforms are utilised to optimally support applications.

Level 5

All new applications are developed using PaaS. All applications are provisioned via PaaS using a common portal. PaaS applications are automatically pushed through test suites and into production when accepted. Dynamic orchestration enables monitoring application effectiveness by leveraging A/B and multi-variant testing. Systems are deployed across cloud platforms and components interoperate seamlessly.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Software**Level 1**

People use SaaS without really understanding the difference. No SaaS policies or blueprints exist.

Level 2

Use of SaaS aligned to existing application classifications. Each cloud provider's security offerings are generally accepted. Use of SaaS offerings based on cloud provider's proposed methods. Limited integration exists to leverage SaaS offering's security and integration.

Level 3

Well-defined software policies exist and offerings are consistently evaluated. A set of blueprints and reference frameworks exist. Data monitoring and credential management is used. Selected SaaS offerings integrated through cloud portal with electronic reporting defined. Defined interfaces exist and are used for SaaS integration.

Level 4

Policies are supported by monitoring tooling and governance. Policies for location and protection of sensitive systems defined. Defined integration interfaces and tools are used to connect elements. SaaS services are automatically registered in the CMDB. Updates to existing systems are tested against the organisation's SaaS solutions.

Level 5

Policy exceptions are automatically detected and alerted in real-time, supported by governance systems. Data exchange between SaaS offerings through defined interfaces, according to defined policies and methods. End users access an enterprise portal and access the desired service through brokers. Continuous evaluation of competing SaaS solutions is performed.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Governance

Level 1

No cloud governance policies have been established. Ad hoc cloud use is treated as regular service providers.

Level 2

Roles and responsibilities are adopted to cloud requirements on an ad hoc basis. Cloud requirements are communicated to adoption islands. Cloud services are monitored and controlled like traditional internal IT services. Cloud service reporting exists based on provider's shared monitoring data. New services are catalogued in a database.

Level 3

Roles and responsibilities are updated and formalised for cloud computing. Communication plans exist for cloud services and are discussed with impacted business, including setting up feedback mechanisms and reporting. Cloud service reporting is integrated into a single reporting tool. All cloud and traditional IT services are catalogued.

Level 4

Roles and responsibilities are adapted to better suit business needs. Cloud-based implications are defined for all organisational levels. Internal and external parties are included in communication. Regular audits and assessments ensure compliance with policies. Real-time reporting enables trend analysis and measurement against KPIs. Catalogued IT services can be ordered from a single portal.

Level 5

Roles and responsibilities are continuously streamlined according to business needs. Communications are broadcasted throughout the full eco-system, with feedback loops in place. Automated audits ensure established policies. Real-time reporting alerts of performance threshold to start management processes. Recommendations of IT service workload location and ordering and charge back to accounting from a single portal.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Software development

Level 1

Cloud knowledge among developers is based on personal interest. No standardised processes and tooling exist.

Level 2

Development teams have some cloud knowledge to start developing cloud applications.

Level 3

Required development capabilities for cloud services are defined and tooling and automation necessary for cloud adoption is developed.

Level 4

Cloud-native application design, leveraging fully automated acceptance tests and container design. Development teams have a cloud roadmap that aligns with cloud strategy. 12 factor application design is adopted.

Level 5

Developers have optimised service delivery, utilising lightweight services (i.e. microservices) that align with agility and re-use models adopted by the business. Zero-touch continuous deployment.

After reading through all focus areas, do you think we missed any critical focus areas?

Several focus areas have been considered, but were rejected because they did not benefit the overall model or were merged with existing focus areas. These are: SIAM, IS service design, Risk management, Organisational understanding, portfolio management, project management.

These are all items that would be impacted with cloud adoption, but in defining the scope and eliciting the maturity levels these focus areas did not add enough value to the model.

The current focus areas are:

IT Architecture
Cloud Strategy
Compliance
Security
Financial
Vendor management
Data management
Operations
Business process management
Infrastructure
Platform
Software
Governance
Software development

If possible, please give a description of what you think maturity would look like when suggesting a focus area.

After reading through all focus areas, do you think some are obsolete or should be consolidated?

Please give your reasoning why a focus area would be obsolete or should be consolidated.

The current focus areas are:

IT Architecture
Cloud Strategy
Compliance
Security
Financial
Vendor management
Data management
Operations
Business process management
Infrastructure

Platform
Software
Governance
Software development

Is there anything you would like to add?

Final Page

Thank you for filling out the survey. This survey remains available until 27 January 2017 . You can come back at any time and add or edit your answers. The next survey will be sent out on 9 February 2017 .

If you have any further questions or remarks during the waiting time, feel free to contact Friso van Dijk at xxx@xxx or +316xxxxx

You can now safely close this page, or click the NEXT button and be redirected to the login screen.

Appendix E

Fourth Survey Cloud Maturity

Welcome to the fourth survey. Thank you all for the responses on the previous survey. The answers were varied and in-depth, which we appreciated very much.

All answers are visible to all participants. Feel free to comment, expand or emphasise on certain answers. For this reason, we encourage you to revisit the survey in a later stage if time permits.

Once again, please keep in mind that there are no wrong answers. Our purpose here is to gather insights and we value all opinions equally.

State of the research

We have updated each of the focus areas based on the feedback received in the previous survey. There were plenty of interesting remarks, and we have highlighted the changes.

Before we start off with the questions, there are three points that need addressing, the model scope, the end state of the model, and the model visualisation:

1. **The scope of the model:** The model focuses on the what question of cloud adoption, and not on the realisation of these items: the how. This has been a conscious decision, as the model in its current state would grow out of bounds. Knowing how to go from level 2 to 3 would require much more in-depth knowledge for each focus area and might widely differ per company. That makes the how question unfit for a maturity model, as we aim to generalise just enough so that it remains helpful, but does not become bloated.
2. **End state of the model:** Several mentions have been made that microservices/PaaS/SaaS might not be the best end state. We fully agree on that point. However, the purpose of the model is to gain insight in which organisational capabilities are required to grow in cloud computing. For example, microservices are not an end state and final solution to your problems in whatever area. However, the use of microservices is enabled by cloud computing maturity and would be a great capability to have. The same goes for SaaS/PaaS/IaaS/on-premise, which can exist in any mix a company deems necessary. However, we believe that the ability to deal with each of those effectively (except when you don't use them at all) is an indication of organisational cloud maturity. That does not mean that we advocate a SaaS-only scenario, which is unrealistic in almost all scenarios.
3. **Model visualisation:** From the previous survey, we found that the relation to the model created in the first two surveys and the focus areas was unclear. This was something that was unclear for us as well. The model created by the focus areas is bigger than the model initially created and it does not serve well as a visualisation of what we currently have. However, it was a great inspiration to decide what to place on each maturity level. Currently we're calling it a roadmap for cloud adoption, since it visualises only part of the entire model. Right now we are still looking for other manners of visualisation, but this falls out of the scope of these surveys.

The survey will once again show each of the focus areas with its maturity description, with a highlight and motivation of the changes made. As a reminder, we've posted the focus areas on the right side throughout the rest of the survey.

There's room for remarks or suggestions below (optional).

Section 1: Maturity Descriptions

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: IT Architecture

Level 1

Cloud is not applied to architecture.

Level 2

Cloud services are considered in planning and processes are documented. Cloud is considered when developing workflows and the use of internal APIs and cloud service interfaces emerge.

Level 3

Cloud services are preferred in planning. Cloud design patterns are leveraged. Cloud building blocks emerge, allowing for scalability, disposable use of resources, and automation.

Level 4

Services can be modelled online, leveraging cloud building blocks and design patterns. Services are constructed with service discovery and loose coupling principles. External APIs are incorporated in architecture design. Single points of failure are avoided by introducing redundancy and automated failure detection.

Level 5

Service components are modelled with a single set of tools, utilised for deploying and managing a highly automated and optimised cloud ecosystem. Application integration and infrastructure are transparent. The architecture is designed to optimise for costs and performance by leveraging cloud elasticity and caching. Real-time audits are enabled by continuous monitoring and automation of controls.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Cloud Strategy**Level 1**

Different views on cloud computing exist, with some common understanding of the business benefits of adopting cloud.

Level 2

Common enterprise-wide cloud strategy exists, but ad hoc adoption of cloud services. The impact of cloud services on organisation has been identified.

Level 3

Key steps and enablers for further cloud adoption have been identified. KPIs are defined to measure strategy impact.

Level 4

All-in cloud strategy guides all new deployments and cloud services. Use and success of implementing cloud strategy are reviewed on KPIs.

Level 5

Enterprise-wide knowledge gathering to identify improvement and growth areas. Cloud strategy enables growth and optimisation of business outcomes and is regularly revised for technological developments.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Compliance**Level 1**

No corporate policies or guidelines related to cloud computing are readily available.

Level 2

Compliance requirements are made available and communicated. The compliance framework is redefined to be cloud-aware. Implementations of cloud services follow predefined procedures to ensure compliance.

Level 3

Processes are in place to check selected areas for compliance regularly and consequences of deviation are analysed. Internal management reports are linked to each of the transitioning cloud services.

Level 4

Compliance requirements are communicated to the ecosystem in a standardised format. Online management and monitoring systems are in place, events of non-compliance are defined automatically where possible. Compliance-aware management tools support real-time monitoring.

Level 5

Compliance communications now have corresponding feedback loops. Corrective and preventative measures are taken based on automatic analysis. Continuous improvement of used framework, analysis and communication methods.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Security

Level 1

Little understanding of cloud security, without any formal procedures.

Level 2

Data security and privacy are evaluated on a project level for cloud. Applications are grouped and requirements are set for business critical applications.

Level 3

A set of standard policies and procedures is published for use when adopting cloud services for all types of services. A clear differentiation is made between privacy and security. Audits are defined and performed regularly. Reports are generated when requested.

Level 4

Existing cloud services are aligned to the standards. Monitoring against rules and policies, with automated reporting on issues. Security data is generated and automatically monitored against KPIs. Regular audits and assessments ensure data policy. Security requirements are integrated with architecture.

Level 5

The security concept is reviewed regularly. Uniform security processes are in place within a security framework that monitors the cloud landscape in real-time with automated reporting. Automated audits ensure implementation of defined privacy and security requirements.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Financial

Level 1

IT budget without usage based cost distribution. Some projects are paid for by business on a non-usage based level

Level 2

Move towards pay-per-use costing, but infrequently billed internally and on a predetermined pricing model. Capital expenses are going through defined cycles. Operating expenses are collected at the end of each month and assigned to IT costs.

Level 3

IT costs are distributed based on general usage. Consumers can check their ordered services and corresponding costs. Financial reporting and source data are available in real-time according to pre-defined financial parameters.

Level 4

IT costs are charged per use to the business units, and the business has a constant view of the actual costs. Standard online contracts and supply management are integrated with supplier systems.

Level 5

Constant cost monitoring in which growing costs are discussed with the business units. Integrated reporting and sharing of relevant data ensures pre-warning of procurement events and that service quality can be monitored and managed proactively.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Vendor management

Level 1

No differentiation between regular and cloud SLAs, with no cloud-specific processes in place.

Level 2

Cloud is fitted to match internal processes. Infrastructure SLAs are used to measure services. Defined products and contracts exist with partners with zero value commitments.

Level 3

Standardised supplier contracts are defined. KPIs are defined for the expected benefits of cloud. Services and contracts are standardised and aligned to enable constant decision making.

Level 4

Standard online contract and supply management is integrated with supplier systems, existing contracts are synchronised to common terms and processes. KPIs are defined and automatically monitored for service delivery. Real-time reporting on existing contracts enable trend analysis to identify exceptions.

Level 5

Integrated reporting and sharing of relevant data with cloud providers. Business processes are integrated. Services can be aligned to meet business needs based on historical trends and data-driven predictions.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Data management

Level 1

Limited data access and availability controls exist. Internal criteria and controls exist for managing data. Data management requires human knowledge of data and location.

Level 2

A limited number of applications use cloud management services. Data management processes are documented in a data management framework and information sharing policies are defined. An enterprise data management function manages key master data sources. Standardised access to data repositories is realised.

Level 3

A published data management framework exists, policies are enforced. Data access and availability controls are consistently applied across the organisation. A central set of database technologies is implemented to support a scale-out database architecture. Data object access through APIs is emerging.

Level 4

Metadata is encoded and stored in a CMS/data warehouse and management processes are based on storage and business metadata. Access and availability of data are continually reviewed. Applications use cloud-based data services. Real-time access to data through managed access points. Semantic search engine capabilities available to support data analysis.

Level 5

The data management framework is an integral part of the overall operating model. Information access and data security controls are integrated into the data ecosystem. Data services supporting applications are behind access APIs. An enterprise-wide data lake has been implemented. Data is accessible through APIs and discoverable through API calls to a service brokerage catalogue. On-premise and cloud data are integrated in a seamless manner.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Operations

Level 1

Demand management does not take cloud into consideration. Cloud service risk and compliance management processes do not exist.

Level 2

Cloud demand management emerges. Service, risk and compliance management processes are in place across the organisation, but not integrated with cloud provider processes. Most applications use compute and storage virtualization. Some operation tools are used to monitor workloads off-premise. Cloud services in use have at least one representation in a CMDB.

Level 3

Consistent processes for demand management have been defined. Processes for service, risk and compliance management allow for manual navigation of single issues. Leveraging virtualization for legacy applications extends to the network layer. Automation technologies are used to manage legacy.

Level 4

Processes for demand management and shared automated processes used, with attached KPIs and reporting. Service, risk and compliance management processes are integrated between cloud consumer and provider. Cloud services are integrated across the full technology stack, providing support for legacy. Tooling is being replaced by cloud provided tools.

Level 5

Systems automatically adjust to changing demand. Best placement of resources is determined through the use of KPIs and metadata. Service, risk and compliance management processes seamlessly process incidents. Legacy systems seamlessly integrated with virtualization technologies. Transactions span across the entire hybrid landscape. Workloads are managed from a centralised position and existing tools are integrated into a single tool.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Business process management

Level 1

Some business product process chains are documented, showing involved IT elements.

Level 2

Every BP is documented with its underlying IT systems, SLAs and OLAs for handling transactions. Some element interfaces underpinning the business process are documented.

Level 3

Common elements are aligned from a semantics and data handling perspective. A migration and consolidation plan is created for processes moving to the cloud. Moving processes are adapted to fit COTS solutions where possible. Common

semantics are applied to systems and well-documented interface characteristics enable dynamic messaging queue interaction.

Level 4

Performance of common IT elements is measured in the combined BPs, with alerting in place for performance thresholds. Systems are categorised and located according to the data they hold for the BPs. Application elements underlying BPs are designed according to well-documented cloud-native models and frameworks.

Level 5

IT elements underlying the BP are automatically tested and monitored on IT metrics. Processes are regularly updated to align with business objectives more effectively. Automatic system scaling according to real-time BP needs. BP testing and monitoring is automated. Ad hoc BPs are designed, implemented, and monitored with supporting microservices, and eventually retired.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Infrastructure

Level 1

No infrastructure processes for the leveraging of IaaS and containerisation exist.

Level 2

Virtualised infrastructure services support separate requests triggered via a provider tool. Container management systems are used to automate container creation and management. Some IaaS reporting exists based on provider's shared monitoring data. IaaS services are available for limited design elements that align with available services.

Level 3

Virtualised infrastructure services allow for a standard interface to collect monitoring and alerting data. They are made available to external provider portals for orchestration processes through a common portal. Virtualised infrastructure components are defined to support a standardised automation virtualisation system integrated into a CMDB. IaaS frameworks allow for repeatable instances.

Level 4

Virtualised infrastructure services support automated deployment. Event monitoring is bound to each IaaS provider. Design blueprints are defined for IaaS and allow systematic re-use of key elements. Virtualised infrastructure supports automatic scaling. Use of containers is standardised. IaaS is implemented with well-defined standards and interfaces. Performance is automatically monitored against KPIs.

Level 5

IaaS supports all data in the landscape and is managed with a single set of policies and rules. Virtualised infrastructure components allow on-premise systems to scale to the cloud. IaaS services are built with interoperable design elements, enabling cross-cloud application and service design. Virtualised infrastructure services are optimised to host and migrate resources to meet business objectives and allow for a Cloud Service Broker to select from available cloud services and platforms.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Platform

Level 1

Applications are built using traditional development practices.

Level 2

Developers use IaaS (virtualised infrastructure) to deploy non-cloud applications. Applications are integrated using standard, non-proprietary integration interfaces.

Level 3

PaaS is used to develop new applications. Application structures are starting to use shared integration components. Application stacks are defined and common elements are stored in a database.

Level 4

Re-usable service elements are available and maintained. Developers use cloud design patterns, focusing on re-using existing elements. Integration, presentation and data services are provided using PaaS APIs. Automatic provisioning and scaling is available. Different cloud platforms are utilised to optimally support applications.

Level 5

All new applications are developed using PaaS. All applications are provisioned via PaaS using a common portal. PaaS applications are automatically pushed through test suites and into production when accepted. Dynamic orchestration enables monitoring application effectiveness by leveraging A/B and multi-variant testing. Systems are deployed across cloud platforms and components interoperate seamlessly.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Software

Level 1

People use SaaS without really understanding the difference. No SaaS policies or blueprints exist.

Level 2

Use of SaaS aligned to existing application classifications. Each cloud provider's security offerings are generally accepted. Use of SaaS offerings based on cloud provider's proposed methods. Limited integration exists to leverage SaaS offering's security and integration.

Level 3

Well-defined software policies exist and offerings are consistently evaluated. A set of blueprints and reference frameworks exist. Data monitoring and credential management is used. Selected SaaS offerings integrated through cloud portal with electronic reporting defined. Defined interfaces exist and are used for SaaS integration.

Level 4

Policies are supported by monitoring tooling and governance. Policies for location and protection of sensitive systems defined. Defined integration interfaces and tools are used to connect elements. SaaS services are automatically registered in the CMDB. Updates to existing systems are tested against the organisation's SaaS solutions.

Level 5

Policy exceptions are automatically detected and alerted in real-time, supported by governance systems. Data exchange between SaaS offerings through defined interfaces, according to defined policies and methods. End users access an enterprise portal and access the desired service through brokers. Continuous evaluation of competing SaaS solutions is performed.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Governance

Level 1

No cloud governance policies have been established. Ad hoc cloud use is treated as regular service providers.

Level 2

Roles and responsibilities are adopted to cloud requirements on an ad hoc basis. Cloud requirements are communicated to adoption islands. Cloud services are monitored and controlled like traditional internal IT services. Cloud service reporting exists based on provider's shared monitoring data. New services are catalogued in a database.

Level 3

Roles and responsibilities are updated and formalised for cloud computing. Communication plans exist for cloud services and are discussed with impacted business, including setting up feedback mechanisms and reporting. Cloud service reporting is integrated into a single reporting tool. All cloud and traditional IT services are catalogued.

Level 4

Roles and responsibilities are adapted to better suit business needs. Cloud-based implications are defined for all organisational levels. Internal and external parties are included in communication. Regular audits and assessments ensure compliance with policies. Real-time reporting enables trend analysis and measurement against KPIs. Catalogued IT services can be ordered from a single portal.

Level 5

Roles and responsibilities are continuously streamlined according to business needs. Communications are broadcasted throughout the full eco-system, with feedback loops in place. Automated audits ensure established policies. Real-time reporting alerts of performance threshold to start management processes. Recommendations of IT service workload location and ordering and charge back to accounting from a single portal.

How can we improve the maturity descriptions?

Please be specific (which level, do we rephrase/add/remove). You can add multiple answers.

Focus area: Software development

Level 1

Cloud knowledge among developers is based on personal interest. No standardised processes and tooling exist.

Level 2

Development teams have some cloud knowledge to start developing cloud applications.

Level 3

Required development capabilities for cloud services are defined and tooling and automation necessary for cloud adoption is developed.

Level 4

Cloud-native application design, leveraging fully automated acceptance tests and container design. Development teams have a cloud roadmap that aligns with cloud strategy. 12 factor application design is adopted.

Level 5

Developers have optimised service delivery, utilising lightweight services (i.e. microservices) that align with agility and re-use models adopted by the business. Zero-touch continuous deployment.

Section 2: Focus Areas

After reading through all focus areas, do you think we missed any critical focus areas?

Several focus areas have been considered, but were rejected because they did not benefit the overall model or were merged with existing focus areas. These are: SIAM, IS service design, Risk management, Organisational understanding, portfolio management, project management.

These are all items that would be impacted with cloud adoption, but in defining the scope and eliciting the maturity levels these focus areas did not add enough value to the model.

The current focus areas are:

IT Architecture

Cloud Strategy

Compliance
Security
Financial
Vendor management
Data management
Operations
Business process management
Infrastructure
Platform
Software
Governance
Software development

If possible, please give a description of what you think maturity would look like when suggesting a focus area.

After reading through all focus areas, do you think some are obsolete or should be consolidated?

Please give your reasoning why a focus area would be obsolete or should be consolidated.

The current focus areas are:

IT Architecture
Cloud Strategy
Compliance
Security
Financial
Vendor management
Data management
Operations
Business process management
Infrastructure
Platform
Software
Governance
Software development

Is there anything you would like to add?

Final Page

Thank you for filling out the survey. This survey remains available until 27 January 2017 . You can come back at any time and add or edit your answers. The next survey will be sent out on 9 February 2017 .

If you have any further questions or remarks during the waiting time, feel free to contact Friso van Dijk at xxx@xxx or +316xxxxx

You can now safely close this page, or click the NEXT button and be redirected to the login screen.

Appendix F

Name	
Organisation	
Function	

About the model

The METRI Cloud Maturity Model consists of 14 focus areas, divided into 5 dimensions, as depicted in the model below. Each of the focus areas consists of a set of questions, resulting in an overall view of the organisational maturity when the assessment is complete.

Using the assessment

Each sheet in this document handles a separate dimension of the model, with the questions divided over several focus areas. In each row, place an 'x' as an answer in the relevant column. When finished, the final results can be viewed in the Results sheet.

Each focus area has a description next to it, aimed at setting the right scope to answer the questions in. Try to assume this mindset for each focus area in answering these questions

Business		
Support the business	Transform and improve the business	Govern IT
	Cloud Strategy IT Architecture Business process management Software development	Governance Compliance Security Data management Financial
	Manage IT	
	Vendor management	
Operate IT		
Operations Software Platform Infrastructure		

Transform and Improve the Business

Transform and Improve the Business					
Cloud Strategy		Yes	Somewhat	No	Cloud Strategy Description A cloud strategy is the plan detailing objectives, principles and tactics for leveraging cloud computing as part of the overall IT strategy (and in support of an organisation's business strategy). It provides guidance for all levels of the organisation by communicating the organisational vision on cloud computing and its implementation and future use within the organisation.
1	Cloud computing is considered in our strategy.				
	Business benefits of cloud computing are understood by involved c-level executives.				
	Involved c-level executives have a shared vision of cloud computing.				
2	An enterprise-wide cloud strategy exists.				
	The impact of cloud services on the organisation has been identified.				
	Adoption of cloud computing happens on an ad hoc basis.				
3	Key steps and enablers for further cloud adoption have been identified and incorporated in the strategy.				
	KPIs are defined and used to measure the impact of the cloud strategy.				
	An all-in cloud strategy guides all new deployments and cloud services.				
4	Use and success is of the strategy is measured by KPIs and the strategy adjusted based on metrics.				
	A digital strategy is in place with a business-first mentality.				IT Architecture Description The IT architecture of an organisation is "a coherent whole of principles, methods and models that are used in the design and realisation of an entire enterprise's organisational structure, business processes, information systems and infrastructure" (Lankhorst 2013). With the adoption of cloud computing, creating and maintaining an enterprise architecture becomes more important when the organisation shifts from using internal to external IT services.
	Feedback loops exist to adjust the strategy based on enterprise-wide knowledge gathering.				
The strategy is regularly revised for technological developments to enable continuous innovation.					
IT Architecture		Yes	Somewhat	No	
1	Cloud computing is considered in our enterprise architecture.				
	Cloud services are considered in planning.				
	Cloud services are documented.				
2	Cloud is considered when developing workflows.				
	Internal APIs and service interfaces are used.				
	Cloud services are preferred in planning.				
3	Cloud design patterns are defined, leveraged and reused.				
	Cloud building blocks exist to enable scalability, disposable use of resources, and some automation.				
	Services can be modelled in online tooling, leveraging cloud building blocks and design patterns.				
4	Services are in principle constructed with service discovery and loose coupling principles.				
	External APIs are incorporated in the architecture.				
	Single points of failure have been addressed by introducing redundancy and automated failure detection and resolution.				
5	Service components are modeled with a single set of tools for deploying and managing a highly automated and optimised cloud ecosystem.				
	Application integration and infrastructure are transparent in the architecture.				
	The architecture is designed to optimise for costs and performance by leveraging cloud elasticity and caching.				
Component performance is monitored in real-time.					

Business Process Management		Yes	Somewhat	No	BPM Description
1	Some business product chains are documented, showing the involved IT elements.				Business process management focuses on improving corporate performance by managing and optimising an organisation's business processes (Panagacos 2012). In the perspective of cloud computing, this means managing and optimising changing business processes due to the introduction of new and often more standardised business processes. Software customisation is becoming a thing of the past with SaaS as a new software delivery model, making it critical for organisations to adapt their processes to these standards if they want to keep up-to-date.
2	Every business process is documented with its underlying IT systems, SLAs, and OLAs for handling transactions.				
	Some element interfaces underpinning the business process are documented.				
	Common elements are identified and aligned from a semantics and data handling perspective.				
	A migration and consolidation plan is created for processes moving to or impacted by the cloud.				
3	Processes are in principle adapted to fit existing cloud offerings.				
	Common semantics are applied to systems.				
	Well-documented interface characteristics enable dynamic messaging queue interactions.				
	Performance of common IT elements is measured in the combined business processes, with triggers in place to alert on performance thresholds.				
4	Systems are categorised and located according to the data held by the business processes.				
	Application elements underlying business processes are designed according to well-documented cloud-native models and frameworks.				
	IT elements underlying the business processes are automatically tested and monitored on relevant metrics.				
	Processes are regularly updated to align more effectively with business objectives.				
5	Automatic system scaling according to real-time business process needs is in place.				
	Business process testing and monitoring is automated.				
	Ad hoc business processes are designed, implemented, and monitored with supporting microservices, and eventually retired.				
Software Development		Yes	Somewhat	No	Software Development Description
1	Developers are not specifically trained on cloud computing and existing knowledge is based on personal interest.				Software development is the process of designing, programming, documenting and testing in order to create and maintain software applications and frameworks. With the adoption of cloud computing, the software development process changes both in the options of software delivery (i.e. SaaS) and in its development tools (i.e. automated testing, using PaaS). One of the benefits of cloud computing is a faster time-to-market and scalability of software products, which requires a more agile development process.
	No standardised processes and tooling for developing for cloud exists.				
2	Developments have enough hands-on cloud knowledge to start developing cloud applications				
3	Required development capabilities for cloud services are defined.				
	Tooling and automation of testing necessary for cloud adoption is developed.				
4	Cloud-native application design is in place, realised by leveraging fully automated acceptance tests, continuous deployment and continuous integration.				
	Development teams have a cloud roadmap that aligns with the cloud strategy.				
	12 factor application design is adopted.				
	Developers have optimised service delivery, utilising lightweight services (i.e. microservices) that align with agility and re-use models adopted by the business.				
5	Continuous deployment and continuous integration are standard practices in software development.				

Manage IT

Manage IT				
Vendor Management		Yes	Somewhat	No
1	There is differentiation between regular and cloud SLAs.			
	There are cloud-specific vendor management processes in place.			
2	Cloud providers are selected based on business requirements.			
	Cloud is fitted to match internal processes.			
	Infrastructure SLAs are used to measure service performance.			
	Zero value commitments with defined products and contracts exist with several partners.			
	Standard contracts from preselected cloud providers are made available for business units.			
3	KPIs have been defined for the expected benefits of the cloud.			
	Services and contracts are standardised and aligned to enable constant decision making.			
	Cloud usage is monitored and its performance evaluated against SLAs.			
4	Preferred cloud providers are selected based on cost and performance measurements.			
	Standard online contract and supply management is integrated with supplier systems.			
	Existing contracts are synchronised to common terms and processes.			
	KPIs are defined and automatically monitored for service delivery.			
	Cloud service performance is automatically monitored against SLAs.			
5	Preferred cloud providers are selected and managed based on strategic objectives.			
	Services can be aligned to meet business needs based on historical trends and data-driven predictions.			
	Businesses can consume cloud services via a service catalogue containing standard contracts from preselected cloud providers.			
	Exceptions are identified through real-time reporting on existing contracts and trend analysis.			

Vendor Management Description
Vendor management is the collection of activities included in researching and sourcing vendors, and maintaining the relationships and communications between the organisation and its vendors. With cloud computing and a distributed IT landscape, vendor management becomes increasingly important.

Govern IT

Govern IT					Governance Description
Governance		Yes	Somewhat	No	
1	Cloud governance policies have been established.				<p>"IT governance is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals" (Gartner). It concerns itself with both demand governance, focused on the effective evaluation, selection and implementation of IT investments, and supply governance, focused on ensuring the effectiveness and efficiency of the IT organisation. With cloud computing, governance is required for both these branches, requiring a new skillset and mechanics to keep a grip on the IT landscape.</p>
	Ad hoc cloud use is no longer treated as regular service providers.				
	Roles and responsibilities are aligned to cloud requirements on an ad hoc basis.				
2	Cloud requirements are communicated to front runners in adoption.				
	Cloud services are no longer monitored and controlled like traditional IT services.				
	Cloud service reporting exists based on provider's shared monitoring data.				
	New services are catalogued in a database.				
3	Roles and responsibilities are updated and formalised for cloud computing.				
	Communication plans exist for cloud services and are discussed with impacted business, including setting up feedback mechanisms and reporting.				
	Cloud service reporting is integrated in a single reporting tool.				
	All cloud and traditional IT services are catalogued.				
4	Roles and responsibilities have been adapted to better suit business needs.				
	Cloud based implications are defined for all organisational levels.				
	Internal and external parties are included in communication.				
	Regular audits and assessments ensure compliance with policies.				
5	Catalogues IT services can be ordered from a single portal.				
	Roles and responsibilities are continuously streamlined according to business needs.				
	Communications are broadcasted throughout the full ecosystem, with feedback loops in place.				
	Automated audits verifies compliance with established policies.				
	Real-time reporting alerts of performance thresholds to start management processes.				
	Recommendations of IT service workload location, service ordering, and charge back to accounting is integrated into a single portal.				
Compliance		Yes	Somewhat	No	Compliance Description
1	Corporate policies or guidelines related to cloud computing are readily available.				<p>With the IT landscape and its regulations becoming increasingly complex, conforming with rules and regulations is of the utmost importance. With cloud computing, new compliance issues arise when the hosting of storage and IT systems is no longer under control of the organisation. For example, ensuring data residency in the country of origin might be an issue that arises when using a public cloud service, requiring new, cloud-related skills in the area of compliance management.</p>
	Compliance requirements are made available and communicated.				
2	The existing compliance framework is redefined to be cloud-aware.				
	Implementations of cloud-services follow predefined procedures to ensure compliance.				
3	Processes are in place to check selected areas for compliance regularly.				
	Consequences of compliance deviation are analysed and managed.				
	Internal management reports are linked to each of the transitioning cloud services.				
4	Compliance requirements are communicated to the ecosystem in a standardised format.				
	Online management and monitoring systems are in place and events of non-compliance are defined automatically where possible.				
	Compliance-aware management tools are in use and support real-time monitoring.				
5	Compliance communications have corresponding feedback loops.				
	Corrective and preventative measures are taken based on automated analysis.				
	The compliance framework, analysis tools and communication methods are continuously improved.				

Security		Yes	Somewhat	No	Security Description
1	Cloud security is understood and formal procedures are in place.				Security is one of the primary concerns when adopting cloud computing. Information security is the practice of preventing unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction of information. With the advent of cloud computing new security issues arise due to the distributed nature of the IT landscape and its increased reliance of networked communication.
	A set of standard policies and procedures is published for use when adopting cloud services of any type.				
2	Requirements are set for business critical application in accordance to cloud.				
	Identity and Access Management (IAM) is specified for specific users and project teams.				
3	Existing cloud services are aligned to newly set cloud security settings.				
	Cloud services are monitored against rules and policies with automated reporting on issues.				
	Security and privacy are differentiated in the security framework.				
	Security audits are defined and performed regularly.				
	Security reporting happens on demand.				
	IAM user groups are defined.				
	The cloud security concept is reviewed regularly.				
4	Uniform security processes are in place within a security framework.				
	The cloud landscape is monitored in real-time with automated reporting.				
	Security data is generated and automatically monitored against KPIs.				
	Security requirements are defined per data classifier and integrated with architecture.				
	IAM user groups are standardised and consolidated according to the least privilege principle.				
	Two-factor authentication for key users is in place.				
	An IAM classification framework for applications calls is in place.				
5	The security concept is fully embedded in development and operations.				
	Applications and data are placed based on data security requirements.				
	Automated audits ensure implementation of defined privacy and security requirements.				
	Non-standard access is automatically reported.				
	Internal and external API calls are automatically classified.				

Data Management		Yes	Somewhat	No	Data Management Description
1	Limited data access and availability controls exist.				Data management concerns itself with the architectural techniques and tools, and practices for achieving consistent delivery of data across the organisation in order to meet the data consumption requirements of all applications and business processes (Gartner). Furthermore, it requires data access and availability controls to ensure secure and compliant use of data. With cloud computing, the more distributed nature of the IT landscape comes with new challenges, such as data access, duplication, consistency and residency.
	Internal criteria and controls exist for managing data.				
	Data management requires human knowledge of data and location.				
2	Several applications use cloud management services.				
	Data management processes are documented in a data management framework.				
	Information sharing policies have been defined.				
	An enterprise data management function manages key master data sources.				
	Standardised access to data repositories has been realised.				
3	A pulished data management framework exists and data management policies are enforces.				
	Data access and availability controls are consistently applies across the organisation.				
	A central set of database technologies has been implemented to support a scale out database architecture.				
	Data (object) access through APIs is emerging.				
	Manual data classification happens in new projects.				
4	Metadata is encoded and stored in a CMS/data warehouse and management processes are based on storage and business metadata.				
	Access and availability of data is continuously reviewed.				
	Applications use cloud-based data services.				
	Data is accessible in real-time through managed access points.				
	Semantic search engine capabilities are available to support data analytics.				
	All data is classified manually, new projects use automated data classification.				
5	The data management framework is an integral part of the overall operating model.				
	Information access and data security controls are integrated in the data ecosystem.				
	Data services supporting applications are behind access APIs.				
	An enterprise-wide data lake has been implemented.				
	Data is accessible through APIs and discoverable through API calls to a service brokerage catalogue.				
	On-premise and cloud data are integrated in a seamless manner.				
	Data is automatically classified.				
Financial		Yes	Somewhat	No	Financial Description
1	The IT budget makes use of usage based cost ditribution.				With cloud computing, the financing of IT services shifts from capital expenses to operating expenses. Organisations are now able to consume IT on a pay-per-use basis and costs can be allocated directly to the consuming business units. This requires a change in the financial management of IT, where technology now allows direct cost allocation and more detailed financial monitoring.
	Some IT projects are paid for by business units on a non-usage based level.				
2	Pay per use costing is used and billed internally on a predetermined pricing model.				
	Capital expenses are going through defined cycles.				
3	Operating expenses are collected periodically and assigned to IT costs.				
	IT costs are distributed based on general usage.				
	IT consumers (business units) can check their ordered services and corresponding costs.				
4	Financial reporting is available in real-time according to pre-defined parameters.				
	IT costs are in principle charged per use to the consuming business units.				
	Consumers (business units) have a constant view of the actual costs.				
5	Standard online contracts and supply management are integrated with supplier systems.				
	Constant cost monitoring exists, and growing costs are discussed with consuming business units.				
	Business units have insight in real-time financial reporting for their IT usage.				
	Integrated reporting and sharing of relevant data ensures pre-warning of procurement events.				
	Integrated reporting and sharing of relevant data ensures that service quality can be monitored and managed pro-actively.				

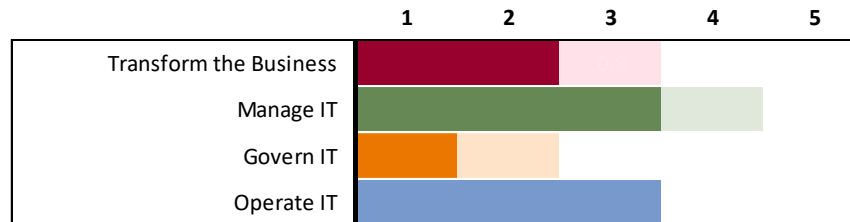
Operate IT



Operate IT				Operations Description
	Operations	Yes	Somewhat	
1	Demand management take cloud into considerations.			IT operations are defined as “the people and management processes associated with IT service management to deliver the right set of services at the right quality and at a competitive cost for customers” (Gartner). When adopting cloud computing, the operations aspect of an organisation changes. Depending on the cloud services adopted, the responsibilities for IT operations are decreased, abolishing a physical infrastructure when adopting IaaS, up to having no control on anything but data for SaaS solutions.
	Cloud services risk and compliance management processes exist.			
2	Cloud demand management exists on a basic level.			
	Service, risk and compliance management processes are in place across the organisation, but not integrated with cloud provider processes.			
	Most applications use compute and storage virtualization.			
	Some operation tools are used to monitor workloads off-premise.			
	Cloud services in use have at least one representation in a CMDB.			
3	Consistent processes for demand management have been defined.			
	Processes for service, risk and compliance management allow for manual navigation of a single issues.			
	Leveraging virtualization for legacy applications extends to the network layer.			
	Automation technologies are used to manage legacy applications.			
	Processes for demand management are in place, with attached KPIs and reporting tooling.			
4	Service, risk and compliance management processes are integrated between cloud consumer and provider.			
	Cloud services are integrated across the full technology stack, providing support for legacy.			
	Tooling is being replaced by cloud provided tools.			
	Systems automatically adjust to changing demand.			
	Workloads are managed from a centralised position and best placement of resources is determined through the use of KPIs and metadata, with management integrated in a single tool.			
5	Service, risk and compliance management processes automatically process incidents in a seamless manner.			
	Legacy systems are seamlessly integrated with virtualization technologies.			
	Transactions span across the entire hybrid landscape.			

Software		Yes	Somewhat	No	Software Description
1	SaaS is used on an ad hoc basis.				The software focus area is about the management of software and the use of SaaS within the organisation. SaaS comes with new operational challenges and a new service model towards the business users, requiring maturity to handle these well.
	SaaS is used without knowledge of the difference of SaaS and regular software.				
2	SaaS usage is aligned to existing application classifications.				
	Each cloud provider's security offerings are generally accepted.				
	Use of SaaS offerings is based on cloud provider's proposed methods.				
	Integration of SaaS offerings is limited.				
3	Well-defined software policies exist and SaaS offerings are consistently evaluated.				
	A set of blueprints and reference frameworks exists for migrating software to SaaS.				
	Data monitoring and credential management is used.				
	Selected SaaS offerings are integrated through a cloud portal with defined electronic reporting.				
4	Defined interfaces exist and are used for SaaS integration.				
	Software policies are supported by monitoring tooling and governance.				
	Policies for location and protection of sensitive systems are defined.				
	Defined integration interfaces and tools are used to connect elements.				
5	Updates to existing systems are tested against the organisation's SaaS solutions.				
	Policy exceptions are automatically detected and alerted in real-time, supported by governance systems.				
	Data exchange between SaaS offerings happens through defined interfaces, according to defined policies and methods.				
	End users access an enterprise portal and access the desired service through service brokers.				
	Continuous evaluation of competing SaaS solution is performed.				
Platform		Yes	Somewhat	No	Platform Description
1	Applications are built using traditional development practices.				Platform, like software, is a broader term for the movement of an organisation toward PaaS and the challenges accompanying this move. This adoption process impacts software development and deployment. PaaS adoption comes with new opportunities as well, allowing the organisation to fully realise the benefits of this new technology.
2	Developers use IaaS (virtualised infrastructure) to deploy non-cloud applications.				
	Applications are integrated using standard, non-proprietary integration interfaces.				
3	PaaS is used to develop new applications.				
	Application structures are use shared integration components.				
4	Application stacks are defined and common elements are stored in a database.				
	Reusable service elements are available and maintained.				
	Developers use cloud design patterns, focusing on reusing existing elements.				
	Integration, presentation and data services are provided using PaaS APIs.				
5	Automatic provisioning and scaling is available.				
	Different cloud platforms are utilised to optimally support applications.				
	All new applications are developed using PaaS.				
	All applications are provisioned via PaaS, using a common portal.				
5	PaaS applications are automatically pushed through test suites and into production when accepted.				
	Dynamic orchestration enables the monitoring of application effectiveness by leveraging A/B and multi-varian testing.				
	Systems are deployed across cloud platforms and components interoperate seamlessly.				

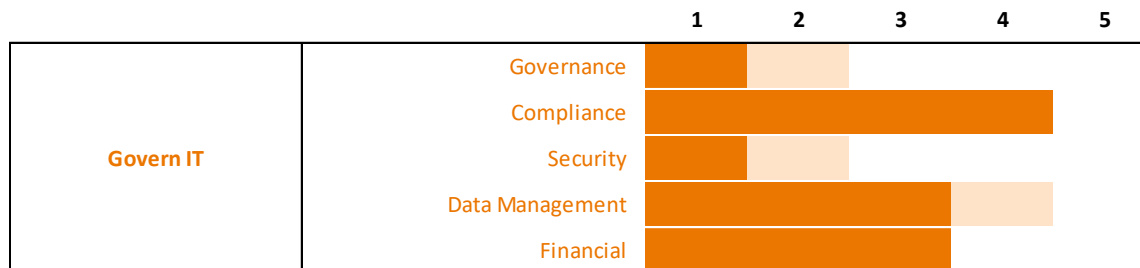
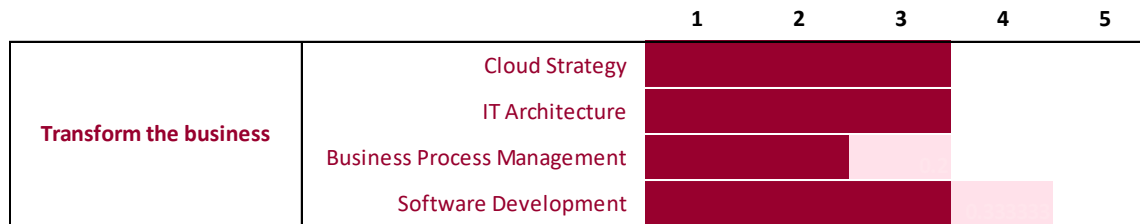
Infrastructure		Yes	Somewhat	No	Infrastructure Description
1	IaaS and containerisation are not leveraged.				Infrastructure is the lowest abstraction level found in cloud computing, with IaaS as its service model. IaaS is the most flexible cloud service model and allows the organisation to automatically deploy servers, processing power, storage and networking. Virtualising these physical items and managing their demand requires certain capabilities from the organisation.
	Virtualised infrastructure services support separate requests triggered via a provider tool.				
2	Container management systems are used to automate container creation and management.				
	Basic IaaS performance reporting exists based on provider's shared monitoring data.				
3	IaaS services are available for applications that align with available service.				
	Virtualised infrastructure services allow for a standard interface to collect monitoring and alerting data.				
	Virtualised infrastructure services are made available to external provider portals for orchestration processes through an API and common portal.				
	Virtualised infrastructure components are defined to support a standardised automation virtualisation system integrated into a CMDB.				
	IaaS frameworks allow for repeatable instances.				
4	Virtualised infrastructure services support automated deployment.				
	Event monitoring is bound to each IaaS provider.				
	Design blueprints are defined for IaaS and allow systematic reuse of key elements.				
	The virtualised infrastructure supports automatic scaling.				
	The use of containers is standardised.				
	IaaS is implemented with well-defined standards and interfaces.				
5	Infrastructure performance is automatically monitored against KPIs.				
	IaaS supports all data in the landscape.				
	IaaS is managed with a single set of policies and rules.				
	IaaS services are built with interoperable design elements, enabling cross-cloud application and service design.				
	Virtualised infrastructure services are optimised to host and migrate resources to meet business objectives (i.e. dynamically select providers on lowest cost).				
	A cloud service broker allows selection from available services and platforms.				

Example Results



 Level fully accomplished
 Level partially accomplished

Keep in mind that the results shown here are **preliminary** and may change based on future observations.



		1	2	3	4	5
Operate IT	Operations					
	Software					
	Platform					
	Infrastructure					

