

# **The Role of Transparency and Trust in the Selection of Cloud Service Providers**

Thesis by

MOHAMMED IBRAHIM ALMANEA

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy at  
Newcastle University



School of Computing Science

Newcastle University

Newcastle upon Tyne

NE1 7RU

UK.

January 2015

## **Abstract**

Potential customers started to adopt cloud computing because of the promised benefits such as the flexibility of resources and most importantly cost reduction. In spite of the benefits that could flow from its adoption, cloud computing brings new challenges associated with its potential lack of transparency, trust and loss of controls. In the shadow of these challenges, the number of cloud service providers in the marketplace is growing, making the comparison and selection process very difficult for potential customers and requiring methods for selecting trustworthy and transparent providers. This thesis discusses the existing tools, methods and frameworks that promote the adoption of cloud computing models, and the selection of trustworthy cloud service providers. A set of customer assurance requirements has been proposed as a basis for comparative evaluation, and is applied to several popular tools (Cloud Security Alliance Security, Trust, and Assurance Registry (CSA STAR), CloudTrust Protocol (CTP), Complete, Auditable, and Reportable Approach (C.A.RE) and Cloud Provider Transparency Scorecard (CPTS)). In addition, a questionnaire-based survey has been developed and launched where by respondents evaluate the extent to which these tools have been used, and assess their usefulness. The majority of respondents agreed on the importance of using the tools to assist migration to the cloud and, although most respondents have not used the tools, those who have used them reported them to be helpful. It has been noticed that there might be a relationship between a tool's compliance to the proposed requirements and the popularity of using these tools, and these results should encourage cloud providers to address customers' assurance requirements.

Some previous studies have focused on comparing cloud providers based on trustworthiness measurement and others focused only on transparency measurement. In this thesis, a framework (called CloudAdvisor) is proposed that couples both of these features. CloudAdvisor aims to provide potential cloud customers with a way to assess trustworthiness based on the history of the cloud provider and to measure transparency based on the Cloud Controls Matrix (CCM) framework. The reason for choosing CCM is because it aims to promote transparency in cloud computing by adopting the best industry standards. The selection process is based on a set of assurance requirements that, if met by the cloud provider or if it has been considered in a tool, could bring assurance and confidence to cloud customers. Two possible approaches (Questionnaire-based and Simulation-based approach) are proposed in order to evaluate the CloudAdvisor framework.

## **Declaration**

I certify that no part of the material offered has been previously submitted by me for a degree or other qualification in this or any other University.

## **Published Work**

Part of the work presented in this thesis has been published as follows.

- I. Almana, M. I., “A Survey and Evaluation of the Existing Tools that Support Adoption of Cloud Computing and Selection of Trustworthy and Transparent Cloud Providers”, presented at the University of Salerno. 6<sup>th</sup> International Conference on Intelligent Networking and Collaborative Systems, Salerno, Italy. 2014

The paper was divided into two main parts. The first, discussed the existing tools and frameworks in the market that could encourage customers to adopt cloud computing and possibly select the trustworthy and transparent cloud service provider. This part of the paper has been written in Chapter 2, Section 2.5 – 2.8.

The second part of the paper discussed the assessment of tools in terms of their usage (popularity) by potential cloud customers, helpfulness towards searching and selection for the best cloud provider and their usage in the future. This part of the paper has been written in Chapter 6: Survey Questionnaire – Assessment of Tool’s Usefulness.

- II. Almana, M. I., “CloudAdvisor – A Framework Towards Assessing the Trustworthiness and Transparency of Cloud Providers”, presented at: UCC2014. 7<sup>th</sup> IEEE/ACM International Conference on Utility and Cloud Computing; 2014 Dec 8-11; London, UK

The accepted doctoral paper is part of this thesis. The details are presented in the methodology (Section 3.3.2) and the CloudAdvisor in (Section 7.5).

## **Acknowledgement**

I would like to thank my supervisor, Professor John Fitzgerald for his endless support, guidance, feedback and productive meetings throughout the past four years as a PhD student. He encouraged me to attend and participate in conferences that are related to my research field in cloud computing. I would like also to thank my thesis committee members Professor Aad van Moorsel and Dr. Paul Ezhilchelvan for their valued knowledge, suggestions and invaluable comments.

I am thankful to the University of Newcastle for providing the best and state of the art research facilities and make every process in the completion of my studies smooth and fun.

During my research Dr. Richard Payne and Dr. Carl Gamble were encouraging PhD students to become involved in the tech-chat group. It is a series of informal group meetings where PhD students and staff can discuss their work and research. It was a great chance for me to present my work and get feedback. It was also a great opportunity to practice my presentation skills for the preparation of conferences. Thank you to Professor Brian Randell and Dr. Richard Payne who attended the meeting. I also had valuable feedback for my accepted paper in Salerno, Italy.

I am grateful to my sponsors (Ministry of Higher and Education in Saudi Arabia) for granting me the scholarship and the opportunity to continue my studies in higher education for both my Master's degree in Computer Security and Resilience and my PhD in Computer Science.

Last but not least, I would like to express my deepest gratitude to my lovely family here in the UK and my parents and relatives in Saudi Arabia for their patience, endless support, prayers and encouragement throughout the past four years. I was, moreover, lucky to have been supported by my brother-in-law (Abdulaziz Alabdulhafez) and his family in Newcastle, they were great companions.

This thesis was proofread by [academicproofreading.com](http://academicproofreading.com)

# Contents

<b>ABSTRACT</b> .....	<b>II</b>
<b>DECLARATION</b> .....	<b>III</b>
<b>ACKNOWLEDGEMENT</b> .....	<b>IV</b>
<b>LIST OF FIGURES</b> .....	<b>VIII</b>
<b>LIST OF TABLES</b> .....	<b>X</b>
<b>TERMINOLOGY</b> .....	<b>XII</b>
<b>PART I</b> .....	<b>1</b>
<b>CHAPTER 1: INTRODUCTION</b> .....	<b>1</b>
1.1    MOTIVATION AND PROBLEM DEFINITION .....	2
1.1.1 <i>Motivation</i> .....	2
1.1.2 <i>Problem Definition</i> .....	3
1.2    AIMS, RESEARCH QUESTIONS AND HYPOTHESES.....	6
1.2.1 <i>Aims</i> .....	6
1.2.2 <i>Research Questions</i> .....	8
1.2.3 <i>Hypotheses</i> .....	10
1.3    CONTRIBUTION .....	11
1.4    THESIS STRUCTURE .....	13
<b>CHAPTER 2: BACKGROUND</b> .....	<b>14</b>
2.1    CLOUD COMPUTING AND COTS .....	14
2.2    CLOUD COMPUTING SECURITY AND TRANSPARENCY .....	17
2.3    BUILDING TRANSPARENCY AND TRUST .....	18
2.4    SELECTING CLOUD PROVIDERS.....	18
2.5    CUSTOMER ASSURANCE REQUIREMENTS.....	19
2.6    RELATED WORK .....	21
2.6.1 <i>Cloud Controls Matrix (CCM) Framework</i> .....	22
2.6.2 <i>Information Assurance Framework</i> .....	22
2.6.3 <i>Cloud Trust Protocol</i> .....	23
2.6.4 <i>CSA STAR</i> .....	23
2.6.5 <i>Cloud Provider Transparency Scorecard (CPTS)</i> .....	26
2.6.6 <i>Complete, Auditable, and Reportable Approach(C.A.RE)</i> .....	28
2.6.7 <i>CloudeAssurance</i> .....	29
2.6.8 <i>SMICloud Framework</i> .....	29
2.6.9 <i>CloudCmp Framework</i> .....	30
2.6.10 <i>CloudHarmony</i> .....	30
2.6.11 <i>Goal Question Metric (GQM) Approach</i> .....	31
2.7    PROVIDERS' REQUIREMENTS.....	32
2.8    COMPARISON BETWEEN THE TOOLS OF TRANSPARENCY .....	32
<b>CHAPTER 3: METHODOLOGY</b> .....	<b>34</b>
3.1    INTRODUCTION .....	34
3.2    OVERVIEW OF THE PROBLEM .....	34
3.3    METHODS .....	35
3.3.1 <i>Survey Questionnaire</i> .....	36

3.3.2	Scorecard.....	40
3.3.3	Goal Question Metric Approach – (GQM).....	45
<b>PART II</b>		<b>47</b>
<b>CHAPTER 4: CLOUD COMPUTING ADOPTION ISSUES AND THE TOOLS ENCOURAGING MIGRATION TO THE CLOUD</b>		<b>47</b>
4.1	INTRODUCTION .....	47
4.2	GOALS AND OBJECTIVES.....	49
4.3	TARGETED RESPONDENTS.....	51
4.4	SIGNIFICANCE OF THE PARTICIPANT'S POPULATION.....	52
4.5	METHODOLOGY .....	52
4.6	RELIABILITY OF DATA .....	54
4.7	QUESTIONNAIRE DESIGN .....	56
<b>CHAPTER 5: FACTORS AFFECTING CUSTOMER'S ADOPTION OF THE CLOUD – SURVEY RESULTS</b>		<b>60</b>
5.1	INTRODUCTION .....	60
5.2	RESPONDENTS' DEMOGRAPHIC RESULTS.....	61
5.3	ADOPTION OF CLOUD COMPUTING – DRIVERS AND CONSTRAINTS.....	64
5.3.1	<i>The Adopters</i> .....	64
5.3.2	<i>Adopters – a Comparison between sectors</i> .....	71
5.3.3	<i>Non-adopters</i> .....	77
5.3.4	<i>Non-adopters – a Comparison between sectors</i> .....	83
5.4	CONCLUSION .....	89
<b>CHAPTER 6: ASSESSMENT OF TOOLS' USEFULNESS – SURVEY RESULTS</b>		<b>92</b>
6.1	INTRODUCTION .....	92
6.2	ASSESSMENT OF TOOLS' IN GENERAL .....	92
6.3	<i>Non-Adopters Views on the Tools' Usefulness</i> .....	98
6.4	<i>Adopters Views on the Tools' Usefulness</i> .....	109
6.5	CONCLUSION .....	120
<b>PART III</b>		<b>128</b>
<b>CHAPTER 7: CLOUDADVISOR</b>		<b>128</b>
7.1	INTRODUCTION .....	128
7.2	CLOUDADVISOR REQUIREMENTS .....	129
7.3	RATIONALE FOR DEVELOPING CLOUDADVISOR.....	130
7.4	MOTIVATION .....	133
7.5	WORKFLOW OF THE CLOUDADVISOR .....	133
7.5.1	<i>Computing Trustworthiness Score – Adoption of Pauley's Methodology</i> .....	135
7.5.2	<i>Transparency Measurement – Adoption of CSA CCM Framework</i> .....	149
7.6	GENERIC SCORECARD TEMPLATE (GST).....	151
7.6.1	<i>Measurement Attributes of GST</i> .....	151
7.6.2	<i>Example of Measurement</i> .....	153
<b>CHAPTER 8: TOWARDS THE EVALUATION OF CLOUDADVISOR</b>		<b>160</b>
8.1	INTRODUCTION .....	160
8.2	EVALUATION OF CLOUDADVISOR PARAMETERS .....	161
8.3	EVALUATION CRITERIA AND REQUIREMENTS.....	162

8.4	POSSIBLE EVALUATION TECHNIQUES .....	166
8.4.1	<i>Questionnaire-based Survey</i> .....	166
8.4.2	<i>Simulation-Based Analysis</i> .....	167
8.5	COMPARISON OF EVALUATION TECHNIQUES .....	178
8.5.1	<i>Evaluation of Questionnaire-based approach</i> .....	179
8.5.2	<i>Evaluation of Simulation-based approach</i> .....	180
8.6	SELECTION OF EVALUATION TECHNIQUE.....	181
8.7	SIMULATION RESULTS .....	181
<b>PART IV .....</b>		<b>186</b>
<b>CHAPTER 9: CONCLUSION AND FUTURE WORK .....</b>		<b>186</b>
9.1	INTRODUCTION .....	186
9.2	SUMMARY AND LIMITATIONS .....	186
9.3	FUTURE WORK .....	193
<b>APPENDIX A .....</b>		<b>195</b>
<b>CLOUD COMPUTING ADOPTION ISSUES AND THE TOOLS ENCOURAGING MIGRATION ....</b>		<b>195</b>
A.1	SURVEY QUESTIONNAIRE TEMPLATE.....	195
A.2	WORKFLOW ANNOTATIONS .....	211
<b>APPENDIX B .....</b>		<b>212</b>
<b>CLOUD CONTROLS MATRIX FRAMEWORK .....</b>		<b>212</b>
B.1	CLOUD CONTROLS GROUPS .....	212
B.2	SIMULATION SCRIPT – TRUSTWORTHINESS AND TRANSPARENCY MEASUREMENT.....	216
<b>APPENDIX C .....</b>		<b>260</b>
<b>SIMULATION .....</b>		<b>260</b>
C.1	DATA AND RESULTS .....	260
<b>REFERENCES.....</b>		<b>279</b>

## List of Figures

Fig.1. CSA STAR workflow.....	24
Fig.2. Goal Question Metric (GQM) approach.....	31
Fig.3. Cloud computing adoption percentage. ....	64
Fig.4. Type of cloud service adopted.....	65
Fig.5. Respondents' selection of deployment models. ....	66
Fig.6. Justification of the enterprise's selection of deployment model. ....	67
Fig.7. Private vs. Hybrid adoption. ....	68
Fig.8. Respondents' selection of cloud provider. ....	69
Fig.9. Single CSP vs. multiple CSP based on cloud selection.....	69
Fig.10. Motivation behind adopting cloud computing.....	70
Fig.11. Sectors' adoption of delivery models.....	72
Fig.12. Sectors' adoption of the deployment models. ....	73
Fig.13. Comparing different working sectors based on the nature of the data. ....	74
Fig.14. Sectors' selection of the number of cloud providers.....	76
Fig.15. Non-adopters' influential role in adopting cloud computing. ....	77
Fig.16. Non-adopters likelihood for adopting cloud computing.....	78
Fig.17. Non-adopters' plan towards selecting type of cloud. ....	79
Fig.18. Factors encouraging cloud computing adoption.....	80
Fig.19. Factors affecting the adoption of cloud computing. ....	82
Fig.20. Sectors' likelihood of adopting cloud computing. ....	83
Fig.21. Sectors' adoption plan for selecting the type of cloud.....	84
Fig.22. Sectors' encouragement factors for adopting the cloud.....	85
Fig.23. Sectors adoption barriers. ....	87
Fig.24. Respondents' opinion on evaluating cloud providers' transparency.....	93
Fig.25. The percentage of using one of the transparency tools.....	93
Fig.26. CSA STAR usage percentage.....	94
Fig.27. CSA STAR usefulness.....	95
Fig.28. CTP usage percentage.....	95
Fig.29. CTP usefulness percentage. ....	96
Fig.30. CloudeAssurance usage percentage.....	97
Fig.31. CloudeAssurance usefulness percentage. ....	97
Fig.32. Sectors' opinion on using tools to evaluate providers' transparency.....	99
Fig.33. Sectors' likelihood of using the tools (non-adopters). ....	100
Fig.34. Sectors' usage percentage of CSA STAR. ....	100
Fig.35. CSA STAR helpfulness for sectors (non-adopters).....	101
Fig.36. Sectors' plan for using CSA STAR in the future (non-adopters). ....	102
Fig.37. Sectors' usage percentage of CTP (non-adopters).....	103
Fig.38. CTP helpfulness for sectors (non-adopters).....	104
Fig.39. Sectors' plan for using CTP in the future (non-adopters).....	104
Fig.40. Sectors' usage percentage of CloudeAssurance (non-adopters).....	106
Fig. 41. CloudeAssurance helpfulness for sectors (non-adopters).....	107
Fig.42. Sectors' plan for using CloudeAssurance in the future (non-adopters).....	107
Fig.43. Sectors' opinion on using tools to evaluate providers' transparency (adopters).....	110



Fig.44. Sectors' likelihood of using the tools (adopters).....	111
Fig.45. Sectors' usage percentage of CSA STAR (adopters).....	112
Fig.46. CSA STAR helpfulness for sectors (adopters).....	113
Fig.47. Sectors' plan for using CSA STAR in the future (non-adopters).....	114
Fig.48. Sectors' usage percentage of CTP (adopters).....	115
Fig.49. CTP helpfulness for sectors (adopters).....	115
Fig.50. Sectors' plan for using CTP in future (adopters).....	116
Fig.51. Sectors' usage percentage of CloudeAssurance (adopters).....	117
Fig.52. CloudeAssurance helpfulness for sectors (adopters).....	118
Fig.53. Sectors' usage percentage of CloudeAssurance (adopters).....	119
Fig.54. CloudAdvisor Workflow.....	134
Fig.55. CloudAdvisor evaluation - simulation-based analysis approach.....	168
Fig.56. Scenarios for cloud provider assessment.....	176
Figure 57. Comparing Cloud Providers' Trustworthiness Based on CloudAdvisor and CPTS.....	183
Figure 58. Transparency Results - A Comparison between Providers.....	184

## List of Tables

Table 1. Trustworthiness Assessment based on Business Factors .....	27
Table 2. Comparing Transparency Tools.....	33
Table 3. Generic Scorecard Template.....	45
Table 4. Respondents' Employment Status .....	61
Table 5. Respondents by Job Title .....	62
Table 6. Respondents by Level of Education .....	62
Table 7. Respondents by Years of Experience .....	62
Table 8. Respondents by Enterprise Size.....	63
Table 9. Respondents by Work Sector.....	63
Table 10. Respondents by Influence of Role .....	63
Table 11. Respondents' Selection of Single/Multiple Provider Based on Cloud Type.....	70
Table 12. Sectors' Ranking Based on Private, Public and Hybrid Clouds.....	73
Table 13. Sectors' Ranking Based on their Selection of Single/Multiple Provider.....	75
Table 14. Respondents' Influence in Adopting Cloud Computing .....	77
Table 15. Ranking Sectors Based on their Selection of the Cloud Adoption Barriers .....	87
Table 16. CloudeAssurance Usage Percentage (Non-Adopters) .....	105
Table 17. Sectors' plan for using CloudeAssurance in the future (non-adopters). .....	108
Table 18. Sectors' Concerns Toward the Use of CloudeAssurance.....	117
Table 19. The Most Used, Useful and Used Tool in the Future (Non-Adopters).....	123
Table 20. Ranking Sectors Based on their Usage of the Tools (Non-Adopters) .....	123
Table 21. Ranking Sectors Based on the Tools' Helpfulness (Non-adopters) .....	123
Table 22. Ranking Sectors Based on their Future Planned use of the Tools (Non-adopters).....	123
Table 23. Sectors' Concerns Towards Having a Tool for Evaluating Provider's Transparency .....	124
Table 24. Sectors' Concerns Towards Using CSA STAR (Adopters) .....	125
Table 25. Sectors' Concerns Towards Using CTP (Adopters).....	125
Table 26. Sectors' Concerns Towards Using CloudeAssurance (Adopters).....	126
Table 27. The Most Used, Useful and Used Tool in the Future(Adopters).....	126
Table 28. Ranking Sectors Based on their Usage of the Tools (Adopters).....	126
Table 29. Ranking Sectors Based on the Tools' Helpfulness (Adopters).....	126
Table 30. Ranking Sectors Based on their Planned Future Use of the Tools .....	127
Table 31. Improved Trustworthiness Attributes .....	136
Table 32. Computing Provider's Trustworthiness – Scenario 1 .....	140
Table 33. Computing Provider's Trustworthiness - Scenario 2.....	140
Table 34. Cloud Controls Matrix - Control Areas .....	149
Table 35. Control Group (Compliance) – Questions .....	150
Table 36. Generic Scorecard Template (GST) Attributes.....	151
Table 37. Example of IaaS Providers.....	153
Table 38. Example of Transparency Measurement - Cloud Provider 1.....	154
Table 39. Example of Transparency Measurement - Cloud Provider 2.....	156
Table 40. Example of Transparency Measurement - Cloud Provider 3.....	158
Table 41. CloudAdvisor Evaluation Matrix.....	167
Table 42. Comparison Between Evaluation Techniques .....	178
Table 43. Cloud Provider Transparency Scorecard - Trustworthiness Results.....	182

Table 44. CloudAdvisor's Trustworthiness Results .....	183
Table 45. Transparency Results (CloudAdvisor Vs. SCA).....	184
Table 46. Cloud Controls Matrix Groups .....	212
Table 47. Compliance Control Areas.....	212
Table 48. Data Governance Control Areas .....	212
Table 49. Facility Security Control Areas .....	213
Table 50. HR Control Areas .....	213
Table 51. Information Security Control Areas.....	214
Table 52. Legal Control Areas.....	214
Table 53. Operation Management Control Areas .....	215
Table 54. Risk Management Control Areas.....	215
Table 55. Release Management Control Areas.....	215
Table 56. Industry Standards Mapped to CCM .....	215

## Terminology

Word	Definition
Transparency	"Revealing enough information to enable reasonable strategic business decisions while respecting an organization's need for confidentiality"[13]
Transparent Security	"Appropriate disclosure of the governance aspects of security design, policies, and practices"[13]
Security Transparency	"The level of visibility into security policies and operations offered by the cloud service provider to the cloud customer"[14]
Trust	"An act of faith; confidence and reliance in something that's expected to behave or deliver as promised"[11]
Trustworthiness	"An exchange partner trustworthy when it is worthy of the trust of others. An exchange partner worthy of trust is one that will not exploit other's exchange vulnerabilities"[121]
Security Breach	"a breach of security or a loss of integrity that has a significant impact on the operation of electronic telecommunications networks and services"[122]
Privacy Breach	"A privacy breach is the result of an unauthorized access to, or collection, use or disclosure of personal information"[123]
DataLoss	"The result of unintentionally or accidentally deleting data, forgetting where it is stored, or exposure to an unauthorized party." [124]
Outage	"Is a period of time during which cloud services are unavailable" [125] " Unavailability or decrease in quality of service due to unexpected behaviour of that particular service, or an incident impacting consumers that results in a service not being delivered at a level they reasonably expected" [126]
Reputation	"Reputation is what is generally said or believed about a person's or thing's character or standing"[127]

## Part I

### Chapter 1: Introduction

The most widely known and used definition of cloud computing is that of the National Institute of Standards and Technology (NIST) which defines it as “a model for enabling ubiquities, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and service) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [1]. Cloud computing has been described as an ‘Internet Centric Software’ [2] which explains the cloud computing software model as “a shift from traditional single tenant approach to software development to that of a scalable, multi-tenant, multi-platform, multi-network, and global” [2]. There are three widely known delivery models offered by the cloud model. They are: Software as a Service (SaaS, e.g. Google Docs [3]); Platform as a Service (PaaS, e.g. Google Apps Engine [4]); and Infrastructure as a Service (IaaS, e.g. Amazon EC2 [5]). These are deployed on four types of model: Public, Private, Hybrid, and Community Clouds. [1].

Cloud computing leveraged by virtualization technologies is becoming a dominant computing model [6]. It aims to provide companies with the ability to utilize a tremendous capacity instantly without the need to invest in establishing a new infrastructure, training new employees, or buying a software license. Cloud computing utilizes virtualization to provide a secure, scalable, shared and manageable environment [7]. These potential benefits provided by the cloud computing model have attracted different working sectors including industry, academia, government, and even small to medium sized enterprises to adopt it. A survey of cloud computing revenues conducted by Gartner shows that the revenue of the cloud market in 2009 was \$58.6 billion, in 2010 it was \$64 billion, and by 2014 it is expected to reach \$148 billion [8]. The extent of this anticipated growth suggests that cloud computing is a promising paradigm.

## 1.1 Motivation and Problem Definition

Section (1.1.1) motivates the work presented in this thesis and Section (1.1.2) describes the problem that it aims to solve in Section (1.1.2).

### 1.1.1 Motivation

In spite of the potential benefits to be gained from cloud computing, it is important to assist cloud customers (e.g. IT managers and executives) to avoid making costly mistakes in their adoption of cloud computing. It has been said, “All Clouds are Not Created Equal” [15]. This has been a challenge to some cloud customers in making a correct or better informed decision when deciding to adopt cloud computing and, most importantly, when comparing the different cloud computing offerings of different competitive cloud providers [15]. Another significant challenge in the current cloud computing market is the selection of a trustworthy cloud service that is provided by several cloud providers that meets cloud customers’ requirements. [32]. In addition to the challenges that cloud customers might face when selecting a trustworthy cloud service provider, assessing the security compliance of the cloud provider [33], as well as the history of the cloud providers [15, 22], is of equivalent importance. A recent survey by CSA [28] and IEEE) [34] indicates that cloud computing is shaping the future of IT but the absence of a compliance environment is having a dramatic impact on cloud computing’s growth [35]. There are some attributes that are suggested to be important when selecting cloud providers, attributes that are associated with its history of breaches [15, 22]. Moreover, incident response has been regarded as an important requirement in cloud computing in order to foster transparency and confidence [36]

### 1.1.2 Problem Definition

With the emergence of the cloud computing paradigm, important issues have arisen which need to be addressed if cloud computing adoption is to widen. These issues are related to the societal and technological aspects articulated around the security of cloud computing. [9]. Customers adopting cloud computing models will be more concerned about their information being controlled by the cloud provider, especially if their information is sensitive. This is due to the lack of transparency, and to some extent the lack of control that potential cloud customers will perceive if they replace traditional models with cloud models. There have been some cases of cloud service providers being forced by request to hand over customers' data stored in the cloud. For example, the government forced Microsoft to hand emails over to them [108]. Thus, there is a possibility that governments might gain access to customers' information stored in servers within their jurisdictions. This raises some important questions. If something goes wrong, what will happen? If a breach of privacy occurs, will cloud providers notify their customers? Who should be accountable for the fault? [10].

Although there appears to be a broad acceptance of the potential benefits of adopting a cloud computing model, important challenges have been identified, including a lack of transparency, trust, loss of control over enterprise assets and vague security guarantees [11]. The lack of transparency of security and privacy practices, and deployed controls during the operation of cloud services, has been considered as a major issue in the risk lists [12]. What is more, if transparency does exist it is often an afterthought [13]. Given the challenges outlined above, it is important to assist customers in making a better informed decision on cloud adoption, particularly when comparing the services of competitive providers [15].

A significant challenge in the current market is the selection of a trustworthy provider that meets customers' security needs. Selecting a provider has been considered a problem for several reasons, including the diversity of the services, resources, technology, and service levels offered [16]. Information leakage from providers hosting customers' sensitive data is also a concern in provider selection [17], and has the potential to slow the adoption of cloud computing. From an academic viewpoint, some efforts have been made towards the security of cloud computing by means of techniques and tools developed for the purpose of fostering transparency between the provider and the customer [15]. While it has been argued that transparency is increasing, the lack of independent scoring tools is still an issue [18]. Efforts such as the Cloud Security Alliance Security, Trust, and Assurance Registry (STAR) [19]

appear to have helped primarily in establishing trust; they have not, however, supported customers in selecting a trustworthy provider through the use of a rating system [20]. There has been some work on support for the selection of cloud services by means of frameworks and tools [15, 19, 20, 21, 22, 23, 24, 25, 26], such as the Cloud Security Alliance Security, Trust, and Assurance Registry (CSA STAR), CloudeAssurance, CloudCmp, and SMICloud. These are presented in Section 2.5. Moreover, in order for the customer to obtain assurance in a cloud service, they should get sufficient and credible evidence from the providers [12]. As Khan and Malluhi [11] argue, more trust is required of the cloud, as it is usually used to store the most valuable information. Therefore, transparency is considered to be essential for cloud computing today. It is important to increase transparency between cloud providers and users before enterprises move their computing infrastructure to the cloud. Moreover, trust, as a societal aspect, could be a driver or a constraint for securing the cloud [9]. Several issues, such as ownership, control, prevention and security, can affect trust.

Sufficient transparency is seen as a prerequisite for trustworthy cloud services; the more valuable information is in the cloud, the more trust is required of it [12]. In other words, the more transparency, the more trust and vice versa. However, obtaining transparency from cloud providers is difficult. There are some challenges that are associated with transparency. They are presented in the following points. Transparency helps clients to determine a priori whether a cloud is trustworthy based on profiles and security assurances associated with a service. The reflection mechanism of a cloud provider's security profile will inform customers about that provider's strengths and weaknesses and reveal how their enterprise security policies would be addressed [11].

Some cloud providers are hesitant to disclose some relevant information to cloud customers. Studies suggest that this is due to several reasons:

- Cloud providers may expend so much effort answering cloud customers' requests that this detracts from the effort available to deliver their core services [3].



- Cloud providers are unaware of cloud customers' identity when responding to information requests, and so may feel there is a risk of losing proprietary information or exposing themselves to underhand exploits if they reveal certain information to unknown potential customers. If there is a public need for transparency then there is also a possibility of an adversary asking for information that might create an attack surface for exploiting this information and using it to attack other tenants that exist on the same cloud [13, 27]. The European Network Information Security Agency (ENISA) – an agency that acts as a switchboard providing information on good practices, advice and recommendations related to network and information security - point out that there is a strong need for cloud providers to deal with information requests in a clear and safe manner, mitigating the risk of misusing the information being given [3].
- Cloud customers need assurance that cloud providers are following sound security practices in mitigating risks facing both the cloud customer and providers. They need this in order to make better informed business decisions and to maintain or obtain security certifications. [3] Therefore, in response to these challenges, the ENISA have produced a standard checklist that provides a means by which cloud customers can accomplish the following:(1) assess cloud computing adoption risks; (2) compare different cloud providers; (3) obtain assurance from cloud providers, and also (4) reduces the assurance burden of cloud providers.

Moreover, the Cloud Security Alliance (CSA) [28] has developed a framework that will not compromise the cloud providers' security. The CSA is a member-driven organisation, chartered with promoting the use of best practices for providing security assurance within cloud computing. Their framework is based on the best security standards, such as ISO27001/2. Detailed information about the CSA framework is described in the literature review (Chapter 2).

## 1.2 Aims, Research Questions and Hypotheses

In this Section, we outline and provide a brief discussion of the aims, research questions and hypotheses that relates to the thesis.

### 1.2.1 Aims

The aims in this thesis are to:

- Explore cloud customers' adoption issues, such as the motivations and barriers towards cloud computing adoption. For example, concerning the barriers that potential cloud customers might face such as the lack of transparency, we investigate if it has been a major inhibitor for them to adopt cloud-computing solutions.
- Investigate if the CSA STAR [19], CloudeAssurance [15] and CTP [21] tools were helpful for potential cloud customers throughout the search of the right provider that meets their business requirements. In addition, if these tools will be part of the customers' plan to use them in the future to search for the right provider.

In order to achieve the above-mentioned aims we need to satisfy the following task:

- Conducting a survey questionnaire by using the popular online tool SurveyMonkey [29]. It aims to understand (1) cloud computing adoption constraints and drivers for potential customers and (2) the extent to which existing tools (e.g., CSA STAR registry, CTP and CloudeAssurance) have or have not encouraged organisations from different sectors to migrate to the cloud and select the appropriate cloud provider. Well-known factors related to the drivers and constraints of cloud adoption have been selected from the literature. In addition, newly distinguished factors have been added, such as the tools' impact on potential cloud customers in adopting cloud computing and selecting the appropriate cloud provider.

- Develop a framework (CloudAdvisor) that aims to provide customers with the capability to assess cloud providers' trustworthiness and transparency based on best industry standards, compare between several offerings, and select the best provider that meets their requirements. CloudAdvisor is based on the customer assurance requirements that have been identified in the literature (Chapter 2). Those requirements are very important for the development of any tool in order to increase customer's confidence. CloudAdvisor should be capable of:
  - Measuring cloud providers' trustworthiness based on the history of the provider.
  - Measuring cloud providers' level of transparency based on CSA's CCM [30] control areas.
  - Allowing providers to submit evidence that supports their claims on the CAIQ [31] template.
  - Monitoring the honesty of cloud providers' by having up-to-date evidence.

The measurement is performed using Pauley's method [22], which can be used to calculate the cloud providers' trustworthiness and transparency scores. An example of measuring trustworthiness is presented in Section 7.5.1 (Tables 30). In addition, an example of transparency measurement is presented in Section 7.6.2 (Tables 36, 37 and 38).

### 1.2.2 Research Questions

Some research questions that have been identified from the literature need to be answered. They are:

1. There are tools (i.e. CSA STAR, CloudeAssurance and CloudTrust Protocol) that have been developed specifically to foster transparency in cloud computing and help potential cloud customer to select the right cloud provider.

- Have these tools' been evaluated from the point of view of the users?

For example, if these tools have been used, were they helpful for them to find the best provider that meets their requirements?

- Were these tools considered an important factor or requirement for potential cloud customers to adopt cloud solutions?

For example, if these tools would bring confidence for potential customers because of their capabilities in measuring providers' transparency and trustworthiness.

2. Selection of a trustworthy cloud service provider

- How to measure cloud providers' trustworthiness?

For example, what are the parameters and formulae that have been used to define and calculate trustworthiness?

- Will the provider will offer an evidence that support his claims?

For example, if the provider claims that he has suffered from a security breach will he provide an evidence for it?

- How to monitor the evidence is up-to-date?

For example, if the type of evidence that is provided by the provider a certificate, is it up-to-date?

### 3. Selection of a transparent cloud service provider

- How can consumers trust that the security controls are satisfied, as claimed by the providers?

For example, asking providers to submit an evidence in a form of document that support their claims that they have implemented the security controls.

- Will the cloud provider maintain an up-to-date evidence that support his claims?

For example, some type of certifications that can be used as an evidence do have an expiry date such as ISO. Therefore, it is important to make sure the certificate is up-to-date if required.

- How to measure cloud providers' transparency?

For example, we need to identify the parameters and formulae that defines and calculates providers' transparency.

### 1.2.3 Hypotheses

In this section we set out our hypothesis regarding the adoption of cloud computing and the use of transparency tools. These hypotheses only relate to the first part of the thesis, which is the survey questionnaire. It has helped us to focus mainly on the problem of transparency in the context of cloud computing and the assessment of the tools from the point of view of the participants in the survey questionnaire.

Hypothesis “1”:

Lack of transparency is a major inhibiting factor for respondents who are planning to adopt cloud computing.

For example, from the results that have been collected we found out that lack of transparency has been ranked 4<sup>th</sup> amongst other reasons. 46% of respondents have agreed on the lack of transparency as a concern in cloud computing adoption.

Hypothesis“2”:

The tools of transparency such as CSA STAR registry, CTP and CloudeAssurance are of more help to respondents who have already adopted the cloud rather than helping non-adopters to search for an appropriate cloud service provider.

### 1.3 Contribution

The contributions made by this thesis are 4-fold:

1. The first contribution is to identify the customer assurance requirements that are necessary to bring confidence to cloud customers when selecting cloud providers. The requirements are listed and discussed in Chapter 2 (Section 2.5).
2. The second contribution is to identify the factors that affect cloud customers' adoption of cloud computing and evaluating the helpfulness of the existing tools in the market, such as CSA STAR, CloudeAssurance and CloudTrust, towards selecting cloud service providers; this is achieved through a survey questionnaire. Thirty-two questions were asked the participants and 177 responses were received. Detailed information is presented in Chapters 4, 5 and 6.
3. The third contribution is the development of the CloudAdvisor framework, which attempts to assist cloud customers in assessing cloud providers' trustworthiness and transparency, based on the predefined trust attributes, such as business factors, and the 11 security control domains defined by the CSA. The rationale behind the development of the CloudAdvisor is described in more detail in Section 7.3. Assessment of cloud providers' trustworthiness and transparency is based on existing methodologies, such as Pauley's methodology [22], and best practices developed by the CSA [28].

This is mainly achieved in two parts of the CloudAdvisor. The first part is to assess the cloud providers' trustworthiness based on some attributes defined by several literatures [15, 22], such as the history of breaches. Increasing the confidence of cloud customers towards cloud providers is important when selecting the best cloud provider. Therefore, Pauley's methodology has looked at other attributes and suggested that cloud customers should ask cloud providers some questions. For example, if they are a member of any cloud computing groups (i.e. ENISA [27], CSA [28], CloudAudit [37], Open Cloud Computing Interface [38], or other known cloud computing group), or if they have a history of breaches in their cloud computing service. However, Pauley's method lacks the evidence that should be provided by the cloud providers in order to support their claims of transparency.

The second part of the CloudAdvisor also needs to assess the transparency of the cloud provider by consolidating the current CSA framework: Cloud Controls Matrix (CCM) [30] and the Consensus Assessment Initiative Questionnaire (CAIQ) [31]. The transparency assessment is based on the scorecard mechanism. More details are described in the methodology (Chapter 3) and an example of how transparency is measured is presented in the CloudAdvisor (Chapter 7).

4. The fourth contribution is the development of simulation. The simulation can be used to evaluate how CloudAdvisor works compared to other frameworks such as Cloud Provider Transparency Scorecard (CPTS), CSA STAR and Security Compliance Assessment (SCA). The comparison is made based on the evaluation requirements that are highlight in Section 8.3. The results are presented in Section 8.7



## 1.4 Thesis Structure

This thesis consists of three parts.

Part I (Chapters 1-3). Chapter 1 provides a brief introduction to the challenges of trustworthiness and transparency in cloud service provision and outlines the motivation for the work reported here. Chapter 2 provides the necessary background and related work that is closely relevant to the thesis. The methodology is discussed in Chapter 3.

Part II (Chapters 4-6). Chapter 4 discusses the design of the survey questionnaire “Cloud Computing Adoption Issues and the Tools Encouraging Migration to the Cloud” that is needed to understand the factors affecting the adoption of cloud computing amongst different industry sectors, such as banks, telecommunications, governments, education, health care and information technology. It also demonstrates whether tools of transparency have been helpful for these industries when migrating to the cloud and selecting the right cloud service provider. The results are discussed in Chapters 5 and 6.

Part III (Chapters 7-8). Chapter 7 discusses the development of the CloudAdvisor framework, which aims to provide a mechanism for potential cloud customers to measure cloud providers’ trustworthiness and transparency. Chapter 8 presents two possible evaluation techniques for CloudAdvisor. The justification of selecting the convenient evaluation method is discussed.

Part IV (Chapter 9) provides an overall discussion of the strengths and limitations of the work reported in the thesis, and describe directions for future work.

## Chapter 2: Background

This chapter aims to put the work of the thesis in its wider context by giving a brief introduction to cloud computing concepts and commercial off-the-shelve (COTS) in (Section 2.1), and the issues of security and transparency in this setting (Section 2.2). Section 2.3 discusses the basis for building trust and transparency in the cloud. Section 2.4 presents the problem of cloud provider's selection and Section 2.5 proposes the criteria and requirements for cloud providers' selection. The related work is discussed in Section 2.6. Providers' requirements are presented in Section 2.7 and, finally, Section 2.8 presents a comparison between transparency tools.

### 2.1 Cloud Computing and COTS

The cloud computing model consists of five fundamental characteristics, three delivery models and four deployment models. Cloud computing is characterised by the following points [1]:

- *On-demand self-service*: The ability to provide computing resources such as server time and network storage as needed without communicating with the cloud service provider.
- *Broad network access*: Computing resources are accessible over the network through standard mechanisms that support the use of various thin and thick client platforms, such as mobile phones, tablets, laptops and workstations.
- *Resource pooling*: Using a multi-tenant model allows computing resources, such as storage, processing, memory and network bandwidth, to be pooled to serve multiple consumers. They are dynamically assigned and re-assigned depending on the consumers' demands. Consumers will not have control and knowledge of the definite location of the computing resources; however, they will be able to identify specific information such as the country, state, or data centre from abstraction high level.
- *Rapid elasticity*: Computing resources can be provisioned and released in a flexible manner in response to consumers' lower or higher demands for service.
- *Measured service*: Providing transparency for cloud service providers and consumers is needed when using resources such as processing, storage, bandwidth and active user accounts. Installing metering capability in to the cloud systems that can monitor, control and report resource usage can achieve this.

Three widely known delivery models are:

- Infrastructure as a Service (IaaS): This model depends entirely on the virtualization technology where cloud providers offer their consumers computing resources, such as network and storage in the form of internet-based services [8]. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications, and possibly limited control of selected networking components, for example host firewalls [1].
- Platform as a Service (PaaS): Cloud providers offer developers an environment where they can develop, deploy and manage their applications without the need to install any platforms or assisting tools [1].
- Software as a Service (SaaS): Cloud providers offer applications to the cloud consumers which are hosted on the cloud infrastructure without the need to install them over the users' machines [1].

These delivery services could be deployed on any of the four types of deployment model: Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud. Cloud providers make the Public Cloud available to the general public where as a Private Cloud refers to the operation of an organisation's infrastructure; the responsibility of managing the organisation's infrastructure may be done either by the organisation itself or by the cloud provider. The Community Cloud aims to allow several organisations to share a cloud infrastructure in order to support a specific community that has shared concerns. A combination of two or more types of cloud might be used for workload balancing among different clouds (this approach is called Hybrid Cloud), while each one of these clouds has its own characteristics [1].

Tremendous figures on cloud computing adoption have been predicted and reported by technology research firms, such as Gartner [39] and the International Data Corporation (IDC) [40], which reflects the potential growth of cloud computing adoption. For example, Gartner predicted a massive amount of money (\$7.6 billion) would be spent globally on cloud computing services encompassing IaaS, cloud management, security devices and PaaS in 2011. In 2016, spending projections are \$35.5 billion [41]. According to recent research reported by IDC, spending on public IT cloud services will reach \$47.4 billion in 2013 and is

expected to be more than \$107 billion in 2017. Over the 2013-2017 forecast period, public IT cloud services will have a compound annual growth rate (CAGR) of 23.5%, five times that of the industry over all. It is predicted that the SaaS model will still remain the largest public IT cloud service category, receiving 59.7% of the revenues in 2017 [42].

In order to differentiate between cloud computing and COTS, we first provide a definition of COTS and its purpose.

COTS is defined as "a Federal Acquisition Regulation (FAR) term for commercial items, including services available in the commercial marketplace that can be bought but used under government contract" [11].

COTS offer cost reduction advantage [11] as in cloud computing, however, it does not offer the flexibility that cloud computing do. For example, the provision of the delivery models (i.e. IaaS, PaaS and SaaS models) and the deployment models (i.e. Public, Private, Hybrid and Community Clouds) and other characteristics that have been introduced previously in Section 2.1. In addition, cloud computing is different from Commercial off-the-shelf (COTS) as it is defined as model but not as a product.

To the best of our knowledge, the issue of transparency has been promoted by the Cloud Security Alliance (CSA) organization with the advent of cloud computing and never been introduced in COTS. CSA has also attracted over 96 of providers to submit a self-assessment questionnaire that documents their security compliance in order to increase assurance amongst cloud customers when they decide to select a cloud provider. Therefore, the work in this thesis has been based on cloud computing rather than COTS.

## 2.2 Cloud Computing Security and Transparency

The security controls employed in cloud computing in general are similar to those applied in traditional IT settings. On the other hand, cloud computing may present diverse risks to organisations than a traditional environment does. This is due to the type of cloud models being utilized, the operational models and the technologies that are employed to set up cloud services. Moreover, in cloud computing the liability of the implementation of security controls is segregated between cloud providers and cloud consumers depending on the delivery models (i.e. SaaS, PaaS or IaaS) [43]. Cloud customers are losing the control to some extent when adopting cloud computing solutions. Therefore, transparency is needed where the potential for misplaced decisions and unfavourable results is tremendous, unless cloud providers are willing to disclose their security controls, and the degree to which they are enforced, and the customer knows which controls are required to maintain their security information. [43]

As discussed in Chapter 1, there is an argument as to whether transparency is improving or the lack of independent tools for measuring cloud providers' transparency is still an issue [18]. This brings the notion of "trust but verify" which indicates that cloud customers should trust their cloud providers. In return, cloud providers should furnish customers with the necessary tools to help them verify and monitor the security controls that are enforced by cloud providers [8]. Transparency is a demand that should be brought to the customer's attention when adopting cloud computing and they should avoid providers who refuse to disclose information related to security controls [44]. However, obtaining transparency from cloud providers is difficult for several reasons that were described in Section 1.1.

### **2.3 Building Transparency and Trust**

Industrial organisations such as the CSA and the Cloud Industry Forums have developed guidelines for transparency, self-certification, and accountability. Organisations and vendors that comply with these guidelines can count on a higher level of trust among businesses weighting vendor service offerings. Despite the fact that this approach of self-certification is still in its initial stages, it offers clear guidance by creating industry standard metrics that can illuminate decision makers and help perform comparative assessments of competing providers. For example, Mimecast has published its security controls in response to the standards set by the CSA and STAR in order to increase their transparency and trust amongst its customers. [45]. Cloud providers' transparency can be based on the CCM as it acts as a guide to the cloud customers to ask cloud providers about their security practices [46].

### **2.4 Selecting Cloud Providers**

Transparency and trust are essential components of any business relationship and they become especially important when choosing a CSP. There are some basic questions that cloud customer should ask the cloud provider. For example, how long has a cloud service provider been in business? [22, 45]. With the growing number of cloud service providers, customers are facing the challenge of selecting the best and most appropriate provider from numerous offers. Therefore, supporting customers in selecting trustworthy cloud providers, using trust and reputation concepts, has been considered one of the cloud computing challenges [47]. The concept of reputation is closely related to trustworthiness [113]. Reputation is defined as “The beliefs or opinions that are generally held about someone or something” [114]. Having said that, in this thesis, we will focus on the transparency and trustworthiness concepts and the reputation aspect will be considered as future work. One of the recommendations that could increase cloud providers' trustworthiness is to evaluate them based on fine-grained quality of service parameters together with consumers' feedback, recommendations, and further specific parameters related to the cloud computing environment.[47] Multiple parameters are important when selecting cloud providers, all of which need to be identified properly. Also, there is a need for mechanisms to measure those parameters and aggregate these measurements based on the customers' preference regarding the importance of the parameters [47].

Moreover, due to the vast diversity in the available cloud services, from the customer's point of view, it has become difficult to decide whose services they should use and what the basis for their selection should be. According to [24] there is no framework that can allow customers to evaluate cloud offerings and rank them based on their ability to meet the user's Quality of Service (QoS) requirements. The contribution of their framework is to create a competitive atmosphere among cloud providers in order to satisfy their Service Level agreements and improve their QoS.

An important issue is how to validate the cloud providers' claims of protecting the cloud customers' data. This can be achieved by incorporating trusted third party auditors where they will validate the statements of the cloud providers that he discloses. [45]. Another method for validating the cloud providers' claims is by providing the cloud customers with an approach for submitting their feedback [47].

Building a trustworthiness profile for cloud providers is important because it will provide a reflection mechanism of the cloud providers' security profile that will reveal the strengths and weakness within the cloud providers [11]. Measuring the trustworthiness of cloud providers is an important issue. Yet, it could be a challenge for potential customers when there is lack of tools [24, 46]. As transparency has been considered a prerequisite when selecting a cloud provider [45], a pre-assessment method for evaluating the cloud's trustworthiness would be essential for potential cloud customers.

## **2.5 Customer Assurance Requirements**

Although there are several tools in the market that have been created mainly to help customers in selecting the best provider to meet their security requirements, to the best of our knowledge there is no work that has considered evaluating them. Therefore, we postulate several requirements that need to be taken into consideration when evaluating the tools of transparency, including:

## **1. Obtaining a score of the provider's trustworthiness**

Trustworthiness is believed to be an important aspect in selection making [23]. It can be assessed based on a set of attributes such as years in business, history of breaches, outages, data loss and memberships [22]. The tools of transparency should be able to calculate a score for the cloud provider's trustworthiness.

## **2. Obtaining a score of the provider's transparency**

It has been observed that there is a lack of transparency in cloud computing [11, 12], and transparency has been considered as precondition for obtaining a trustworthy cloud service [12]. In order for the cloud customer to obtain assurance from the cloud service provider, the tools of transparency should be tested for their capability of assessing the cloud provider's transparency. Transparency is measured based on the CCM framework where a set of questions defined in each control area of the CCM framework is presented to the cloud provider for completion in order to obtain a score based on their answers.

## **3. Support of evidence**

In order to bring more assurance to the cloud customer, the providers are entitled to provide sufficient and credible evidence that supports their claims of trustworthiness and transparency [12, 59]. Bhensook has also emphasised the need for evidence, which confirms that providers are performing customer's requirements as expected [33]. Consequently, an evidence score will be calculated and assigned to each cloud provider.

## **4. Monitoring cloud provider's honesty**

Honesty has been regarded as one of the three trusting belief attributes that refer to a trustee's need (i.e. provider) to be honest and keep promises [23]. Therefore, it is not sufficient to know that the cloud provider has submitted evidence that supports its claims of trustworthiness and transparency. Some types of evidence such as certifications or memberships need to be kept up-to-date.



## **5. Adoption of the best industry standards**

An example of this would be the adoption of the CCM framework, which is intended to promote security transparency and documents the security controls that are applied in all of the delivery models (i.e. IaaS, PaaS and SaaS) [30]. This framework has been the base for several tools such as CloudeAssurance [15]. Therefore, it is an important assurance requirement to consider.

## **6. Comparing cloud providers' offerings**

With the growth of the cloud computing, several enterprises are providing various cloud services, and from the customer's point of view, it has been always a challenge to choose the right provider based on customers' requirements [24, 25, 26, 60]. In order to overcome this problem, several frameworks and tools have emerged to help customers to compare and select the provider [15, 24, 25, 26]. Therefore, examining which tool could accomplish this requirement is very important and could bring assurance to the cloud customer before or during the selection of the cloud provider.

### **2.6 Related Work**

There are several works that have been carried out in order to encourage transparency in cloud computing. Some of these works include the development of frameworks such as the CCM [30], developed by the CSA, and the Information Assurance Framework [48], developed by the ENISA. Other tools, such as the CTP, have been developed specifically in order to measure cloud providers' transparency [21]. This section explains the major work that has been conducted in the area of transparency encouragement in cloud computing environment, showing how our research will benefit from existing work in order to improve the decision making process for cloud customers.

### **2.6.1 Cloud Controls Matrix (CCM) Framework**

The CSA has developed a Cloud Controls Matrix (CCM) [30]; its purpose is to provide cloud customers with fundamental security principles that are aligned to the CSA guide 14 domains. Documenting the security controls that exist in all the delivery models, IaaS, PaaS and SaaS, has also been considered by the CSA. Consequently, they have developed the Consensus Assessments Initiatives Questionnaire (CAIQ) [31], which consists of over 140 questions articulated around 11 control areas, namely compliance, data governance, facility security, human resources, information security, legal, operations management, risk management, release management, resiliency and security architecture. It is intended to assist both the cloud customer and cloud auditor in assessing a potential cloud provider. One of the advantages of this framework is that it does not overwhelm the cloud providers with a myriad of questions provided by several cloud customers [27]. Providers need only to submit their responses in a Microsoft Excel sheet provided by the CSA.

### **2.6.2 Information Assurance Framework**

The ENISA has developed the Information Assurance Framework [48] in order to let cloud customers obtain assurance from cloud service providers that their information is sufficiently protected. The framework provides organisations with a set of questions that they might wish to ask cloud service providers. These are based on the security standards, such as those of International Organisation for Standardization (ISO) [49] and the National Institute of Standards and Technology (NIST) [50]. However, as Catteddu and Hogben [27] state, the questions act, as a minimal baseline and additional information might be needed to answer cloud customers' questions.

### **2.6.3 Cloud Trust Protocol**

An interesting work, which is considered one of the four initiatives related to the CSA, is called the Cloud Trust Protocol (CTP) [21]. It is a synchronous protocol that serves both cloud service providers and cloud customers. CTP serves as a mechanism to generate evidence-based confidence for the cloud service customers. It will provide customers with the ability to request and receive pieces of information when applying to providers. These pieces of information are related to compliance, security, privacy, integrity, and the operational security history of service elements being performed in the cloud. The CTP aims at providing cloud customers with true information. Consequently, better-informed decisions can be made when deciding to move data or perform computations in the cloud [11]. The protocol is based on a question and response pattern that is similar to that used in the other frameworks, such as the CAIQ and the Information Assurance Framework, both of which will be discussed later in this chapter. The main advantage of the CTP is that it will be available for all cloud providers and the user (i.e. Cloud Customers) ultimately controls it. Therefore, the CTP will provide the Transparency as a Service. However, according to Bhensook and Senivongse [33] the CTP can be more useful for existing customers with regards to building trust, rather than for prospective customers who are willing to choose between different cloud providers. CTP satisfies almost all of the customer assurance requirements presented in Section 2.5 except for the comparison requirement. It is important to provide a mechanism for customers to compare between different providers' offerings.

### **2.6.4 CSA STAR**

Another interesting approach for encouraging the transparency of the cloud providers has been introduced by the CSA, which has developed the CSA STAR registry system [19]. The CSA STAR system aims to document the security controls provided by various cloud computing offerings. The CSA STAR system is based on the CCM framework. The purpose of the framework is to provide cloud customers with fundamental security principles that are aligned with to the CSA guide 14 domains. Based on the CCM, the CSA have also developed the CAIQ questionnaire that documents the security controls that exist in all the delivery models, including IaaS, PaaS, and SaaS. The questionnaire sets out 140 questions that cloud customers or cloud auditors might wish to ask the cloud provider. The questions are articulated around 11 control areas.

One of the advantages of this framework is that it does not overwhelm cloud providers with the requests of the cloud customers. This framework simply lets the cloud providers submit their response to the CAIQ questionnaire using a simple method like an Excel sheet. Therefore, the cloud customers will be able to compare their security requirements with the cloud providers' security offerings. The architecture of the framework is described below. A definition of the shapes is presented in Appendix A.2

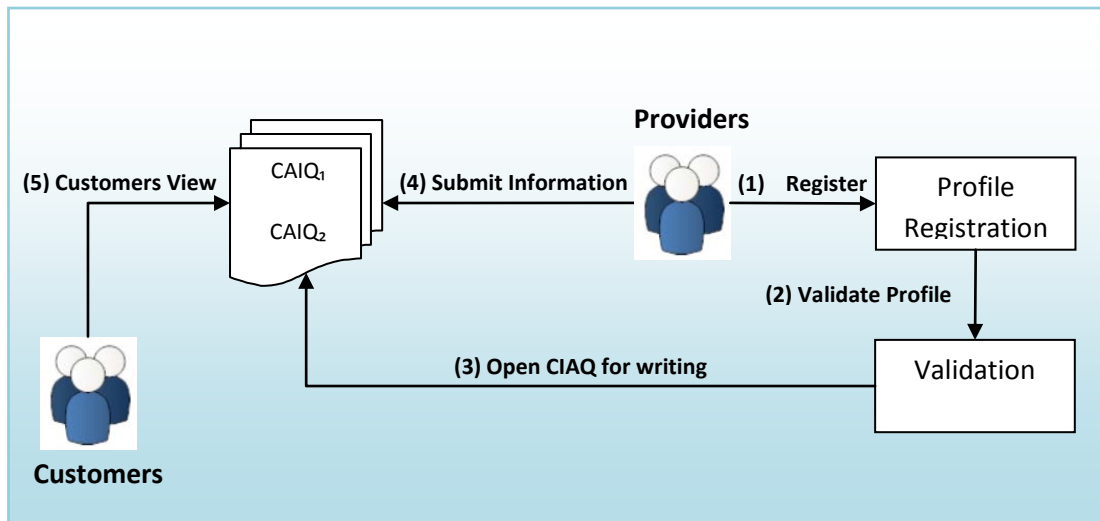


Fig.1. CSA STAR workflow

The workflow of the existing framework is described in the following points:

(1) **Registration step:** the cloud provider should provide the following details:

- Contact Name
- Email Contact
- Company Name
- Company Website
- Brief description about the cloud provider
- Company Logo

(2) The CSA will verify the authenticity of the submission by performing a basic check to make sure the application is complete.

(3) In case of successful validation, the CAIQ file will be displayed on the CSA STAR Registry website ready for cloud providers' submission.

(4) Cloud provider will write their response and it will be stored in the CAIQ repository file.

(5) The cloud customers will be able to open the CAIQ file and compare different cloud providers' offerings.

Cloud providers are also entitled to comply with the CSA rules. For example, after a successful submission, the cloud provider will be asked to update its security disclosure not less than once in a 12-month period. This is important to monitor the changes of the cloud providers' internal security controls and its procedures [51].

However, to some extent, the current framework lacks the following important features:

- It does not measure:
  - The trustworthiness of the cloud providers
  - The transparency of the cloud providers
  - The privacy or security risk score of the cloud providers
- To the best of our knowledge, the cloud customers have not tested it.
- To know which sector (i.e. governments, telecommunications, education, banks, Enterprises) has found the framework of the CSA is sufficiently appropriate to be adopted to search for cloud offering.

The CSA STAR is now based on three layers that are defined by the Open Certification Framework Working Group (OCFWG) [52].

- STAR-Self-Assessment: based on the CCM framework and the CAIQ questionnaire.
- STAR-Certification: At this level of assessment the cloud provider's security is assessed using the control areas that are defined in the CCM framework. Therefore, a score will be assigned to the cloud provider. STAR certification acts as a next level of assurance.
- STAR-Continuous: This is based on publishing the assessment results related to the security properties monitoring based on the CTP. This level of assurance will be completed by 2015.

The CSA has been, and remains, the inspiration upon which several researchers build their work, primarily based on both the CCM and the CAIQ [22, 33, 67]. The CSA has satisfied requirements (3 – 6), which relate to the support of evidence, certification, monitoring the honesty of the providers through attestation, and the adoption of best industry standards such as the CCM framework.

### **2.6.5 Cloud Provider Transparency Scorecard (CPTS)**

Pauley [22] has developed a scorecard that assesses the transparency of the cloud service provider across four dimensions, including security, privacy, auditability and service level agreements. Pauley's work is unique in that a pre-assessment has been performed on cloud service providers, based on several factors related to the provider themselves, including their business entity. Thus, a score from the pre-assessment phase is generated and assigned to the cloud provider as presented in Table 1. Based on this score and a compared threshold value, it will determine if the cloud provider is eligible for the post-assessment phase, where the transparency of the cloud provider will be assessed against a set of questions that are associated with the four dimensions. Although the CPTS acts as a guideline for how organisations can evaluate the cloud providers' transparency, its simplicity might not be effective for specific organisation's requirements. The reason for choosing the pre-assessment method is because it provides cloud customers with a background history of the cloud provider. Knowing historic problems, such as outages, breaches, data loss and other issues, is one of the important factors that should be included in the cloud providers' profile. Several business factors have been identified by Pauley that includes: (1) Years of Business, (2) Published Security or Privacy Breaches, (3) Published Outages, (4) Published Data Loss, (5) Profitable or Public (6) Similar Customers (7) Member of ENISA, CSA, CloudAudit, OCCI, or other cloud standard groups.

Table 1. Trustworthiness Assessment based on Business Factors

Business Factors	CP1	CP2	CP <sup>N</sup>
Number of years in business			<b>Total years</b>
<b>1</b> Number of years in business > 5?			0 ≤ 5, 1 ≥ 5
<b>2</b> Published security or privacy breaches?			0 = Y, 1 = N
<b>3</b> Published outages?			0 = Y, 1 = N
<b>4</b> Published data loss?			0 = Y, 1 = N
<b>5</b> Similar customers?			0 = N, 1 = Y
<b>6</b> Membership of Cloud Standard Groups			0 = N, 1 = Y
<b>7</b> Profitable or Public?			0 = N, 1 = Y
Pre-assessment total score			Total
Percentile score			Score/7

CPTS also satisfies three requirements (1, 2, and 5); these are trustworthiness, transparency measurement and the adoption of some industry standards that were taken from CSA and ENISA.

## 2.6.6 Complete, Auditable, and Reportable Approach(C.A.RE)

C.A.RE [14] provides a means by which cloud customers can determine how competently the cloud service provider adheres to a cloud customer's security. This has been achieved by assessing its completeness in addressing most, if not all, risks that a service may be exposed to. In other words, it lessens a cloud customer's risk of the insecurity of the cloud that they live in. Another advantage that C.A.RE claims is providing the cloud customer with a way of determining the overall trustworthiness of a cloud service provider through security metrics. Mutual auditability and multi-party trust parameters have been considered as the foundation of security assurance for the provided cloud service. The C.A.RE approach stands for and consists of three phases that would produce a trustworthy cloud service:

- **COMPLETE:** It is the existing evidence that is provided by the cloud providers in order to prove what security controls have been implemented and what security requirements are needed for the cloud customer. Three levels of assurance have been added in the COMPLETE phase, namely: SA.COM.1, SA.COM.2, and SA.COM.3. The first level shows that the cloud provider is not meeting the security requirements of the customer; SA.COM.2 shows that security requirements are partially met by the cloud provider and SA.COM.3 shows that the cloud provider has met the security requirements provided by the customer.
- **AUDITABLE:** This checks whether the cloud provider's security needs continuous monitoring and a well-established verification process. This is important because of the emerging changing threats. This phase consists of five levels of assurance related to the verification process performed during the auditability phase. The verification process is categorized as follows: SA.AUD.1, which is performed informally; SA.AUD.2, which is performed structurally; SA.AUD.3, which is structured and independent; SA.AUD.4, which is semi-complete and SA.AUD.5, which is complete.
- **REPORTABLE:** The last phase of the C.A.RE approach is related to the transparency between the cloud provider and customer. Sharing the information with the cloud customer will increase confidence. Therefore, two levels of assurance have been assigned to the cloud provider when it comes to this phase. The first is not transparent, as the information is not shared with the cloud customer. The second level is a transparent cloud provider where security information has been shared with the cloud customer.



The disadvantage of this approach is that it is hard to implement in practice. It possesses a challenge in finding two or more cloud service providers to provide an extensive detailing of their security configurations, the level of granularity of the audit conducted on that security, and so on. As an alternative solution, [14] performed a comparative study between the C.A.RE approach and the guidelines provided by the CSA, in which they found that C.A.RE is effective. In terms of this approach, satisfying the customer assurance requirements proposed in Section 2.5, the C.A.RE approach has satisfied five out of six requirements. The only drawback is that it did not consider adding a feature for the customers to perform a comparison between provider's offerings in order to make their selection process easy.

### **2.6.7 CloudeAssurance**

The CloudeAssurance is the first scoring system that has been developed using the current CSACCM [15]. It provides a provisional and validated score by consolidating all of the important cloud assurance metrics such as the cloud service provider's adoption of internationally accepted best practices and standards, scope of certifications, maturity levels, measurement against the Top 20 mitigating controls based on past security breaches, and even industry-specific compliance requirements like PCI-DSS [53], FedRAMP [54] and HIPAA [55]. Their strategy of choosing between competing offers provided by different cloud providers is based on the following factors: quality of certification, scope of certification, security maturity level, and history of breaches. However, their method of measuring the transparency of the cloud providers is not described since the CloudeAssurance is a commercial product that is sold to potential cloud customers.

### **2.6.8 SMICloud Framework**

An SMICloud framework [25] has been proposed in order to compare different cloud providers based on user's requirements using the analytical hierarchy process (AHP) approach [110]. The framework relies on utilizing the service measurement indexes that have been identified by the Cloud Service Measurement Index Consortium(CSMIC) [109]. The SMI framework focuses on a set of QoS attributes that are needed by customers such as: accountability, agility, assurance of service, cost, performance, security and privacy, and

stability. One of the advantages of the SMICloud framework is that it measures all the QoS attributes defined by CSMIC.

### **2.6.9 CloudCmp Framework**

Duke University and Microsoft Research aims to assist potential cloud customers in evaluating the performance and cost of the cloud providers, based on a set of metrics related to storage, memory, and network [26]. Therefore, they have developed a tool called CloudCmp that will help cloud customers to do this. They have conducted a study on major cloud providers in the market such as: Amazon AWS [111], Microsoft Azure [104], Google AppEngine [4] and Rackspace [98]. However, they have not performed an evaluation of the cloud providers based on other attributes, such as security, compliance and legal aspects.

### **2.6.10 CloudHarmony**

CloudHarmony is an online measurement tool that can be used to evaluate the cloud providers' performance [112]. It consists of four components, which are CloudSquare, CloudScores, CloudReports, and CloudMatch. CloudSquare can be used by cloud customers to search and compare between cloud providers based on attributes such as price, performance, geographical location and availability. CloudScores provide their customers with an access to benchmark metrics that help them to evaluate the performance of cloud services based on the CPU, memory, disk IO, and network. CloudReports is responsible for providing reports that contain analysis of the cloud services' performance and technical facts. CloudMatch allows cloud customers to perform tests on the speed of uploading and downloading large and small files and network latency on several services located in different geographical locations. It can be performed in Europe, the United States, Canada and Asia. Similar to the CloudCmp tool, CloudHarmony focuses on attributes that are related to performance, pricing and availability.

### 2.6.11 Goal Question Metric (GQM) Approach

Basili and Weiss developed the GQM approach in the 1980s [56] and it provides four fundamental benefits [57]:

1. Developing and understanding an organisation's application development practices and establishing appropriate baseline and benchmark levels.
2. Managing and assessing application development processes.
3. Evaluating the effectiveness of new software engineering processes.
4. Validating, assessing and implementing process and practice improvements.

In order to make the measurement effective it should be: (1) focused on specific goals, (2) applied to all life-cycle products, processes and resources and (3) interpreted based on characterization and understanding of the organisational context, environment and goals. A bottom-up approach cannot be considered in the GQM approach because several characteristics of the software need to be observed when measurement takes place; this includes, for example, time, number of defects, complexity, lines of codes, severity of failures, effort, productivity and defect density [58]. Therefore, the hierarchal structure of the GQM is presented in a top-down approach where the goals are first defined and then the questions that address the goals are stated. The last step in the hierarchy is the defining of the metrics where it will help to assess and measure the transparency level in a quantifiable way. Although the GQM approach was originally used to improve software products, the development process, and to define and evaluate goals for a particular project in a particular environment, the underlying concepts are generic and applicable in any measuring setting and it has been expanded to a larger context [56].

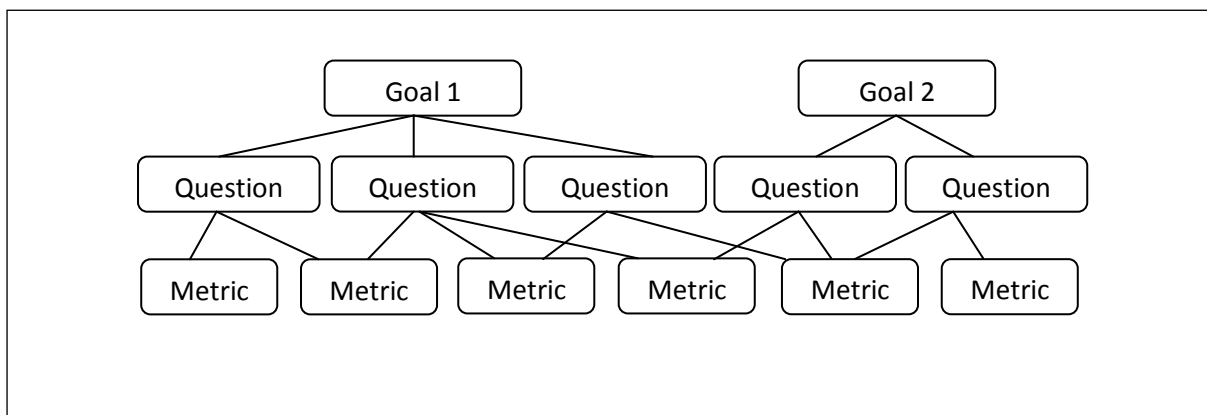


Fig.2. Goal Question Metric (GQM) approach

Bhensook and Senivongse [33] first adopted the GQM approach in an initial attempt to measure the security compliance of the cloud service providers. This is mainly done by utilizing the “CCM” framework, which consists of control groups that can be treated as the goals, which can be applied to the first layer of the GQM approach and the “CAIQ” questionnaire as the questions that can be mapped to the middle layer of the GQM approach. In the bottom layer, the metrics are defined in a quantifiable way, so measurement can be performed and a transparency score is assigned to the cloud provider.

## **2.7 Providers’ requirements**

The ENISA [27] has outlined some of the top recommendations for promoting assurance for cloud customers. At the same time, they have taken into consideration cloud customers’ obligations towards cloud providers when asking for information. This leads to an important requirement:

- Reducing the burden on the cloud providers

The ENISA has put important emphasis on reducing the burden on the cloud service provider. This is because several providers find that a large number of customers request audits of their infrastructure and policies. This can create a critically high burden on security personnel and it also increases the number of people with access to the infrastructure, which significantly increases the risk of attack due to the misuse of security-critical information, theft of critical or sensitive data. As a proposed solution to this problem, a CAIQ questionnaire, which has been developed by the CSA, can be adopted to provide cloud customers with a means of asking the providers relevant questions without compromising their infrastructure’s security and also will result in reducing the cloud provider’s burden of answering myriad questions.

## **2.8 Comparison between the tools of transparency**

Table 2 consists of two columns that aim to show each tool’s compliance to the customer’s assurance requirements. The first column contains the name of the tool, and the second column is divided into six-sub columns, each of which represents the following numbered assurance requirements:

- (1) Trustworthiness measurement
- (2) Transparency measurement
- (3) Support evidence
- (4) Keeping evidence up-to-date
- (5) Adoption of best industry standards
- (6) Comparison of performance between cloud offerings.

Table 2. Comparing Transparency Tools

Tool	Assurance requirements					
	1	2	3	4	5	6
CPTS	✓	✓	✗	✗	✓	✗
CSA STAR	✗	✗	✓	✓	✓	✗
C.A.RE	✗	✓	✓	✓	✓	✓
CTP	✓	✓	✓	✓	✓	✗

In this assessment, CSA STAR and CPTS satisfy the fewest of our requirements. Our view is that C.A.RE and CTP could, to some extent, meet cloud customers' expectations in delivering the needed information to them. The C.A.RE approach lacks from the start an important requirement, which is the capability to measure the cloud provider's trustworthiness. This requirement is very important to bring assurance to the cloud customer compared to the last requirement, which is the comparison of performance between cloud providers' offerings. To the best of our knowledge, the CTP lacks the comparison feature. This will lead cloud customers to some difficulties in selecting the right cloud provider.

After we have compared the tools of transparency, based on the proposed assurance requirements, this will lead us to try to answer the second research aim presented in Section 1.2.1. This related to the ways to help potential cloud customers to select the most trustworthy and transparent provider via the proposed CloudAdvisor framework that aims to satisfy all the customer assurance requirements.

## **Chapter 3: Methodology**

### **3.1 Introduction**

This chapter presents a brief overview of the research problem; it discusses and justifies the methods that helped in accomplishing the aims and objectives of the research.

### **3.2 Overview of the problem**

In spite of the potential benefits and revenues of adopting a cloud computing model, concerns have been expressed that it brings new challenges, including the potential lack of transparency and loss of control over cloud customers' assets [12]. Given these challenges there should be a good level of visibility into security policies and procedures offered by the cloud provider to the cloud customer [14]. This has led to other challenges that might face potential cloud computing customers. These challenges include making better-informed decisions on cloud adoption, particularly when comparing between cloud providers [15] and selecting a trustworthy and transparent cloud provider.

There should be a mechanism that helps cloud customers to select a trustworthy and transparent cloud provider that meets their security requirements. The following section will identify the research questions that have been considered as concerns for cloud customers when deciding to adopt cloud computing and selecting the right cloud provider.

### 3.3 Methods

A variety of methods have been explored in order to achieve the aims of the research problem. In this section, the methods will be discussed thoroughly and the selection of the approach is made and justified.

There are three typical methods that can be used to conduct the research [61]. In brief, they are a case study, survey and an experiment. The case study requires detailed information about a single case or a small number of related cases, whereas surveys aim to collect data and identify patterns from a group of people or organisations in a consistent manner. The last approach - conducting an experiment - usually starts with some requirements, such as (1) a definition of the hypothesis (2) measuring the effects of planned change in one variable to another and (3) it is applied to a sample of people from a known population.

The case study and experiment approach are not used in this research; this is because the type of research questions that are addressed here cannot be applied to them. The applicability of the methods depends on the nature of the research questions [61]. For example, it is more convenient to answer the first research question using the survey method, as it requires the data collection from a large group of people from different organisations. Therefore, the first aim of the thesis will be conducted using the survey method.

### 3.3.1 Survey Questionnaire

A survey questionnaire is required that aims to understand cloud computing adoption constraints and drivers, the tools and framework that provide assistance for the respondents in migrating to the cloud, the selection of the most trustworthy and transparent cloud provider and evaluating the CCM framework. Structured questionnaires can be conducted using a variety of data collection methods. Questionnaires can be conducted in several forms. It includes face-to-face interviews, telephone, email or electronic survey questionnaires that can be completed online using internet-based applications [62]. In this thesis, a survey questionnaire has been developed in order to answer the research questions 2 – 4. The survey questionnaire was developed using the popular SurveyMonkey web application tool. It was founded in 1999 and it is considered as a SaaS cloud model. It provides capabilities such as data collection and data analysis. The survey questionnaire that has been developed included three different types of questions:

- Behavioural
- Attitudinal
- Classification

Behavioural questions are designed to record facts but not opinions, finding out what people of enterprises do. For example, asking the participant the following questions: Have you used the CSA STAR registry tool? Or, will you use the CSA STAR registry in the future?

Attitudinal questions are designed to record the participants' opinions of products or services. For example, using positioning statements to ask for participants' agreement or disagreement on a statement. A typical question would be, how helpful did you find the CSA STAR registry in encouraging you to use cloud computing solutions?

Classification questions are designed to collect data in order to group the respondents' information and see how they differ from each other. For example, questions that are related to their employment status, level of education, geographical location, scale of enterprise or company and industry domain.



In order to be effective, the following seven principles have been adopted in designing the survey questionnaire:

1. Deciding what information is needed.
2. Rough listing of the questions.
3. Refining the questions' phrasing.
4. Developing the response format.
5. Putting questions into appropriate sequence.
6. Finalising the layout of the questionnaire.
7. Pre-test and revision of the questionnaire (Piloting and Revising).

#### *Deciding what information is needed*

In order to know what information is needed, objectives of the study should be ready and clear. In this step, the objectives of the survey questionnaire are highlighted in Chapter 4 (Survey Questionnaire – design).

#### *Rough listing of the questions*

Making a list of all possible questions that could be included in the questionnaire. The aim is have a comprehensive set of questions, although at this stage they may not be well phrased.

#### *Refining the questions' phrasing*

In order to collect good quality data, that answers the research questions, the comprehensive list of questions have to be well phrased. Several sessions were conducted with the supervisor, producing several drafts of the questionnaire, in order to make sure that the questions are not biased and that they are clear and meaningful.

### *Developing the response format*

There are several response formats that can be used in order answer the questions correctly. These include open-ended questions, close-ended questions and optional formatting. Two types of response questions format have been used when developing the survey questionnaire. For example, the close-ended format uses multiple choices and drop-down menus and optional formatting can be used to add a field for additional comments. The last type of format, the open-ended question, asks the participant to write a comment text in a single text box or multiple text to represent their answer.

### *Putting questions in a logical sequence*

There should be a flow and logic to the questionnaire. The SurveyMonkey questionnaire has the capabilities to create logical questions that can lead the participant smoothly through the questions without any confusion. Logical questioning means that participants are prompted to respond to different sets of questions depending on their previous answers. In the survey questionnaire there are 10 logical questions that aim to lead the participant to answer a certain number of questions related to the survey's research questions.

### *Finalising the layout of the questionnaire*

The questionnaire layout should be clearly introduced with instructions for the participant [63]. The survey questionnaire that has been developed includes what is called the "Participant Information" sheet. It provides a brief introduction for the participant by stating the purpose of the study, the type of questions that need to be answered related to the research questions and the expected time needed to complete the survey. Most importantly, it assures the anonymity of the responses.

### *Pre-test and revise (Piloting Study)*

Before launching the survey questionnaire, it is important to test the questionnaire by performing a pilot study. The purpose of the pilot study is not to collect data but to make sure the questionnaire introduction and instructions are clear and that there are no ambiguities in the questions.

Prior to the launching of the survey questionnaire in 2012, the pilot study was sent on the 6<sup>th</sup> of August 2012 to [cs-all@ncl.ac.uk](mailto:cs-all@ncl.ac.uk). A list includes both academic staff and PhD students from the computing school. The pilot study has received three responses. One response has given us a solid feedback towards improving the clarity of the questions and some terms used to define cloud computing and its characteristics. The remaining two responses have not shown any concerns related to the questions of the survey questionnaire. The received feedback was positive and helpful in making the survey questionnaire live and ready to be sent out.

The survey questionnaire was distributed electronically using a Newcastle's University email account. The mailing list was created manually by searching for the email accounts of universities, telecommunication companies, governments, banks, healthcare and IT websites. All of these potential candidates were invited to participate and a good number of responses were received from some sectors, such as IT, universities and telecommunication companies. There were very few positive responses from banks and the healthcare sector. In order to maximise the number of responses, LinkedIn [64] was used to send the survey questionnaire invitation. LinkedIn is a business-oriented social networking service that was launched in 2006. It has helped to gain more responses by sending invitations to a variety of professional groups related to cloud computing. This includes groups such as, "Cloud Computing Community", "Cloud Computing", "Cloud Computing and Virtualization", "Cloud Computing, SaaS, and Virtualization", "Cloud Security Alliance", "Saudi Banks" and "Trusted Cloud Initiative". Moreover, a scientific trip to Saudi Arabia was approved by Newcastle University in order to collect data from several sectors, such as governments, IT, telecommunication and education sectors. This helped to gain more responses from organisations within Saudi Arabia. The design of the survey questionnaire is described in Chapter 4 and the results are presented and discussed in Chapters 5 and 6.

The second aim of the research is to develop a framework "CloudAdvisor" that helps potential cloud customers to select a trustworthy and transparent cloud service provider. The framework focuses on two components that are very important to accomplish when it comes to selecting a cloud provider. These components are the trustworthiness and transparency of the cloud provider. [22, 33] have made substantial efforts towards achieving the trustworthiness and transparency of cloud providers. The former focuses only on assessing the cloud providers' transparency, based on the GQM approach, while the latter focuses on

two components by developing a scorecard that provides scores for the cloud providers based on yes and no answers. The GQM and Scorecard approach are defined and described thoroughly in the subsequent sections and the selection of the methodology is justified.

### 3.3.2 Scorecard

Pauley’s method has been adopted in order to measure cloud providers’ trustworthiness and transparency. The method relies on developing a scorecard that aims to provide cloud providers with questions that can assess the providers’ trustworthiness. Trustworthiness is measured on business factors that are defined by Pauley. These include factors such as the number of years in business, security and privacy breaches, outages, data losses and membership of cloud standard groups. Based on these factors, several questions were developed in the form of yes and no answers. The questions were formed based on fundamental areas defined by the CSA, the National Institute of Standards and Technology (NIST), and the ENISA. In this thesis, Pauley’s method will be conducted using the exact factors. Having said that, the approach lacks important requirements that are very important to address, such as the support of evidence. It has been emphasised that there is a need for evidence that confirms that providers are performing customers’ requirements as expected [33]. Another requirement that complements the previous one is monitoring the honesty of the provider. Therefore, Pauley’s approach will be improved to include the abovementioned requirements.

The following equations will describe how the trustworthiness score is calculated and assigned to the cloud provider based on Pauley’s approach. More details about this method are described in Chapter 7 (CloudAdvisor).

$$Security\ Breach_{score} = \begin{cases} 1 & \text{if } sb = 0 \\ 1 - 0.sb & \text{if } sb \geq 1 \text{ and } sb \leq 9 \\ 0 & \text{if } sb \geq 10 \end{cases} \quad (1)$$

$SecurityBreach_{score}$  is the security breach score that will be assigned to provider. Three possible scores are calculated depending on the number of security breaches. For instance, a 0 score is assigned to the provider if the number of security breaches exceeds 10 breaches in a year. A score of 1 is assigned to the provider if he does not suffer from

any breaches, or a score  $(1 - 0.sb)$  is assigned to the provider provided that the number of security breaches is between 1 and 9.  $sb$  is the number of security breaches incidents.

$$Privacy\ Breach_{score} = \begin{cases} 1 & \text{if } pb = 0 \\ 1 - 0.pb & \text{if } pb \geq 1 \text{ and } pb \leq 9 \\ 0 & \text{if } pb \geq 10 \end{cases} \quad (2)$$

$PrivacyBreach_{score}$  is the privacy breach score that will be assigned to provider. Three possible scores are calculated depending on the number of privacy breaches. For instance, a 0 score is assigned to the provider if the number of privacy breaches exceeds 10 breaches in a year. A score of 1 is assigned to the provider if he does not suffer from any breaches, or a score  $(1 - 0.pb)$  is assigned to the provider provided that the number of privacy breaches is between 1 and 9.  $pb$  is the number of privacy breaches incidents.

$$Membership_{score} = \begin{cases} 0 & \text{if } m = 0 \\ 1.m & \text{if } m \geq 1 \text{ and } m \leq 9 \end{cases} \quad (3)$$

$Membership_{score}$  is the membership score that will be assigned to the provider. Two possible scores are calculated depending on the number of memberships that cloud providers holds. For example, a score of 0 is assigned to the provider if he does not hold any membership with any cloud computing group. A score of  $1.m$  is assigned to the cloud provider who holds membership ranging from 1 to 9.  $m$  is the number of memberships.

$$DataLoss_{score} = \begin{cases} 1 & \text{if } l = 0 \\ 1 - 0.l & \text{if } l \geq 1 \text{ and } l \leq 9 \\ 0 & \text{if } l \geq 10 \end{cases} \quad (4)$$

$Data\ Loss_{score}$  is the Data Loss score that will be assigned to provider. Three possible scores are calculated depending on the number of Data Loss incidents. For instance, a 0 score is assigned to the provider if the number of incidents exceeds 10 in a year. A score of 1 is assigned to the provider if he does not suffer from any incidents, or a score  $(1 - 0.l)$  is assigned to the provider provided that the number of incidents is between 1 and 9 is the number of Data Loss incidents.

$$Outages_{Score} = \begin{cases} 1 & \text{if } O = 0 \\ 1 - 0.O & \text{if } O \geq 1 \text{ and } O \leq 9 \\ 0 & \text{if } O \geq 10 \end{cases} \quad (5)$$

$Outages_{score}$  is the Outages score that will be assigned to provider. Three possible scores are calculated depending on the number of Outages incidents. For instance, a 0 score is assigned to the provider if the number of incidents exceeds 10 in a year. A score of 1 is assigned to the provider if he does not suffer from any incidents, or a score  $(1 - 0.O)$  is assigned to the provider provided that the number of incidents is between 1 and 9.  $O$  is the number of outages incidents.

$$Years\ in\ Business_{Score} = \begin{cases} 1 & \text{if } y > 5 \\ 0.8 & \text{if } y = 5 \\ 0.6 & \text{if } y = 4 \\ 0.4 & \text{if } y = 2 \\ 0.2 & \text{if } y = 1 \\ 0 & \text{if } y < 1 \end{cases} \quad (6)$$

Equation (6) shows different scores assigned to the cloud provider depending on the number of years in business that the cloud provider has been.

The following equations will measure provider's transparency, based on their claims of evidence submission for each factor (Security, Privacy, Data loss, Outages and Membership).

$$\text{if } sb \geq 1 \text{ then } T_{Security} = \left\{ \frac{\sum_{i=1}^e \text{Published Evidence}}{\sum_{i=1}^{sb} \text{Security Breach}} \right\} \quad (2)$$

Where  $T_{security}$  is the transparency score of the security breach factor that the provider will be assigned. The transparency is measured by dividing the number of published evidence related to the security breach factor by the number of security breach incidents that have occurred to the provider.

$$\text{if } pb \geq 1 \text{ then } T_{Privacy} = \left\{ \frac{\sum_{i=1}^e \text{Published Evidence}}{\sum_{i=1}^{pb} \text{Privacy Breach}} \right\} \quad (2)$$

Where  $T_{privacy}$  is the transparency score of the privacy breach factor that the provider will be assigned. Transparency is measured by dividing the number of published evidence related to the privacy breach factor by the number of privacy

breach incidents that have occurred to the provider.

$$if\ l \geq 1\ then\ T_{DataLoss} = \left\{ \frac{\sum_{i=1}^e Published\ Evidence}{\sum_{i=1}^l DataLoss} \right\} \quad (3)$$

Where  $T_{data\ loss}$  is the transparency score of the data loss factor that the provider will be assigned. The transparency is measured by dividing the number of published evidence related to the data loss factor by the number of data loss incidents that have occurred to the provider.

$$if\ 0 \geq 1\ then\ T_{Outage} = \left\{ \frac{\sum_{i=1}^e Published\ Evidence}{\sum_{i=1}^o Outages} \right\} \quad (4)$$

Where  $T_{outage}$  is the transparency score of the outage factor that the provider will be assigned. The transparency is measured by dividing the number of published evidence related to the outage factor by the number of outages that have occurred to the provider.

$$if\ m \geq 1\ then\ T_{members\ hip} = \left\{ \frac{\sum_{i=1}^e Published\ Evidence}{\sum_{i=1}^m Membership} \right\} \quad (5)$$

Where  $T_{Membership}$  is the transparency score of the membership factor that the provider will be assigned. The transparency is measured by dividing the number of published evidence related to the membership factor by the number of memberships that providers have.

After describing how the provider's trustworthiness is measured based on the provider's history, the transparency measurement requirement is also very important to consider before cloud customers commit to an agreement with a provider. There are two possible methods to measure transparency. The first is to use the same approach that has been used to measure trustworthiness. In this thesis, transparency is also measured using a scorecard. The second approach that can be used to measure transparency is the GQM approach, which is described in Section 3.5.3.

The transparency of the cloud provider will be measured based on the well-formed CSA CCM framework. As it has been discussed in the literature, the CCM framework

consists of 11 control groups namely compliance, data governance, facility security, human resources, information security, legal, operations management, risk management, release management, resiliency and security architecture. Each control group consists of several questions. Providers' transparency is measured based on 202 questions that are aligned to 11 control areas that exists in CCM. These questions are claimed to be of interest to both customers and auditors [16]. The CAIQ questionnaire, which includes the 202 questions, will be used as they are mapped to several industry-accepted security standards, regulations and controls framework. In order to get the score of the provider for each question existing in the CAIQ, a generic scorecard template (GST) is attached to each question that exists in the control areas. Customers can assign weights to each control group depending on its importance to them. The following equations describe the process of transparency measurement.

$$\left[ CP_{Transparency} = \frac{Score_{CG}}{Number\ of\ CG} \right] \quad (3)$$

Where  $CP_{Transparency}$  is the cloud provider's transparency score, it is calculated by dividing the total score of control groups by the total number of control groups.

$$\left[ Score_{CG} = \frac{Score_{CID}}{Number\ of\ CID} \right] \quad (2)$$

Where  $Score_{CG}$  is the total score of control groups, it is calculated by dividing the total score of questions by the total number of questions in the control group.

$$\left[ Score_{CID} = \frac{CP_{response} + CP_{comment} + CP_{Evidence} + CP_{publis\ hed} + CP_{Auditing}}{Number\ of\ attribute} \right] \quad (3)$$

Where  $Score_{CID}$  is the score of the question that has been answered by the provider, it is calculated by dividing the score of each answer of the attributes by the number of attributes which is 5.

An example of how transparency is measured is explained in Chapter 6 (CloudAdvisor – framework towards assessing cloud provider's trustworthiness and transparency).



Table 3. Generic Scorecard Template

<i>Generic Scorecard Template</i>	
<b>Attributes</b>	<b>Score</b>
Response	$Response_{score} = \begin{bmatrix} 1 \text{ if Yes} \\ 0 \text{ if No} \end{bmatrix}$
Comments	$Comments_{score} = \begin{bmatrix} 1 \text{ if Commented} \\ 0 \text{ if Not} \end{bmatrix}$
Evidence	$Evidence_{score} = \begin{bmatrix} 1 \text{ if Submitted} \\ 0 \text{ if Not} \end{bmatrix}$
Published	$Published_{score} = \begin{bmatrix} 1 \text{ if Published} \\ 0 \text{ if Not} \end{bmatrix}$
Audited	$Auditing_{score} = \begin{bmatrix} 1 \text{ if Not expired} \\ 0 \text{ if Expired} \end{bmatrix}$

### 3.3.3 Goal Question Metric Approach – (GQM)

Measuring the security compliance of the cloud provider is an important question, as it will help to create a secure and trusted cloud service. However, security compliance can be difficult to demonstrate from the cloud provider. Therefore, a well-designed security metric can be useful for cloud providers to quantify and objectively demonstrate their security compliance [65], provide security assurance [66] and motivate the creation of a trustworthy cloud ecosystem [67]. Security metrics can be used for decision support, particularly in assessment, monitoring and prediction. Security measurement targets can include a technical system, service, product, an organisation, its processes and resources [68]. Good metrics should be specific, measurable, attainable, repeatable and time-dependant (SMART) [69].

As an example, the Common Assurance Maturity Model (CAMM) [70] explores metrics and measurements by proposing to quantify the level of assessment required to achieve greater confidence. CAMM considers two principles: the first, objective metrics, can be used to obtain scores from different components that can be composed to model the security level of a cloud provider [71]. Until now, the CAMM have not issued additional information regarding the cloud metrics. The CSA Metrics Work Group (MWG), which complements the CSA CCM, has developed security metrics that are needed to evaluate

CCM's requirements. The CSA MWG has created a template that characterises each metric with attributes, and also proposes their first 10 metrics covering approximately 25 of CCM's control areas. There are other security metrics that are defined by NIST [72] and CIS) [73] that are not specific to the cloud but they can be applied to the cloud because of its flexibility.

There are several frameworks or methods that are useful for deriving security metrics, such as the GQM approach [56] and NIST [74]. Chapter 2 described the GQM approach developed by Basili and Weiss in the 1980s, as a mechanism of measurement. It starts at the top level by defining the goals and then presents questions, the answers to which will try to achieve the goals. The last step is defining the metrics, which provides a quantifiable way of measurement [56]. The GQM approach is widely accepted in the industry for several reasons [57]. One of these is that the approach can be applied to different organisations and environments. Another reason is that since the nature of the GQM is a top-down approach, the organisational directions and goals are easily aligned. [75]. An extensive literature review and evaluation of the frameworks and methods for deriving the metrics has been conducted by [76].

However due to the difficulties of defining a metrics, such as the need for team work and the progress work on defining specific cloud metrics for the CCM control areas, the GQM approach will not be adopted. Another approach, which is developed by [22], can be used as a guideline for assessing the cloud providers' transparency. However, Pauley's methodology has been criticised by [33, 77] in that it was not created for the purpose of evaluating threats and does not take into consideration subjectivity and uncertainty when conducting the evaluation. In addition to this, it does not demonstrate the quality of evidence provided by the cloud provider. Having said that, since part of our research focuses only on scoring cloud providers' levels of transparency, and the pattern of the questions placed on the CAIQ template are based on "Yes/No" response, we consider this approach to be convenient. The question is how to validate the claims of the cloud service providers that exist in the CAIQ. [67]

## Part II

### Chapter 4: Cloud Computing Adoption Issues and the Tools Encouraging Migration to the Cloud

#### 4.1 Introduction

Several authors have discussed cloud computing adoption issues, such as [78, 79, 80], and many survey questionnaires have been conducted and published to address this subject. For example, the ENISA published a survey questionnaire in 2009 targeting small and medium sized enterprises. They aimed to understand the possible engagement of SME enterprises in adopting cloud computing and the reasons behind adoption. 74 responses from 19 countries were collected; the findings of their survey were used to provide support for the creation of a use case scenario called “An SME Perspective on Cloud Computing” [81]. A different survey questionnaire sponsored by Mimecast delivered SaaS-based enterprise email management including archiving, discovery, continuity, security and policy. They examined the perception and adoption of cloud computing among 565 respondents in the U.S. and Canada. The findings suggested that security concerns and integration of existing infrastructure are the biggest roadblocks for cloud adoption, while cost reduction remains the main driver of cloud adoption. Moreover, some industries have shown quicker movement than others. The top three cloud computing adopters were the technology (53%), financial services (40%), and legal (37%) sectors [82]. Findings of another survey conducted by the Department of Information Technologies at Prague University, targeting 600 Czech organisations, showed that the main motivation for cloud computing adoption was cost reduction (26% of the respondents). Whereas, the cloud computing barriers shows that security constitutes only 14% of the respondents’ concerns and dependence on external providers constitutes 17% of respondents’ concerns [83].

Several surveys have been conducted in Europe and North America researching how businesses are approaching and perceiving cloud computing technology [84, 85]. There is also increasing evidence that the benefits of cloud computing do not apply equally to all companies and that new (start-up) companies are the prime candidates for cloud computing. This is because such companies can best take advantage of rapid deployment and the elasticity of cloud infrastructure [85]. The survey designed for this thesis is different in that it targets multiple types of enterprises, including micro, small, medium and large, and is

globally distributed. It will also include Saudi Arabia, as there are several studies that have been conducted in the United States and Europe [84, 85] and only a very few have considered Saudi Arabia. Including Saudi Arabia in the survey questionnaire is very important as according to the IDC, the Middle East could be the next major market to adopt cloud computing. Saudi Arabia's total projected spending on cloud delivery is set to increase by 34.86% in 2012, with long term spending to expand at a compound annual growth rate of 49.70% between 2012 and 2016. [86] Hamza Naqshbandi, a senior research analyst for IT services with IDC Saudi Arabia said, "Organisations across the kingdom have traditionally preferred to manage their IT operations internally, however, there has been growing interest in outsourcing models, with organisations increasingly using hosting and managed service. This growing adoption of outsourcing services is seen as a first step toward moving to a cloud-based model, as companies become more comfortable with the concept of remote services delivery". The level of adoption of cloud computing in Saudi Arabia is affected by several factors, such as educational level and job domain [87].

The survey aims to analyse the participants' responses in terms of their adoption of the cloud and use of transparency tools such as CSA STAR registry, CTP and CloudeAssurance. Most of these tools rely on the CCM framework developed by the CSA. The effectiveness of the CCM framework is a very important research question. In Chapter 7, a framework "CloudAdvisor" has been defined, and part of it relies on the CCM framework. Therefore, evaluating the effectiveness of the CCM, in terms of its helpfulness and future use, will be a part of the survey questionnaire.

The structure of this chapter is as follows: Section 4.2 highlights the survey questionnaire goals and objectives and Section 4.3 explains the targeted audience. In Section 4.4, the significance of the participants' population is explained. The research methodology is discussed in Section 4.5 and the design of the survey questionnaire is discussed in Section 4.6. The survey results are explained in both Chapter 5 and 6. The survey questionnaire template containing the questions is presented in the Appendix (A.1).

## 4.2 Goals and Objectives

The survey aims to gather information from the participants in order to achieve the following goals and objectives:

- **Cloud Computing Adopters – Analysis objectives**
  - Adoption level of the respondents.
  - Analysing cloud adopters' selection of the delivery service.
  - Analysing cloud adopters' selection of the deployment model.
  - Analysing cloud adopters' justification for their selection of the deployment model based on the classification of the application and data.
  - Comparing between private and hybrid adoption rates based on the classification of the applications and data.
  - Analysing the cloud adopters' selection of the number of cloud service providers.
  - Comparing between single and multiple providers based on the type of cloud adopted.
  - Studying and analysing the factors that have encouraged respondents in adopting cloud computing.
  - Comparison between different sectors in terms of their selection of the delivery and deployment models of the cloud, the classification of the data and application being hosted and the selection of number of cloud providers that are offering their services.

- **Cloud Computing Non-adopters – Analysis Objectives**
  - Analysing the respondents’ likelihood of adopting cloud computing.
  - Analysing the respondents’ selection of the type of service in case of planning for cloud computing adoption.
  - The factors that could encourage respondents to adopt cloud computing.
  - The barriers that dissuade respondents from adopting cloud computing.
  - Performing a comparison between the sectors based on their likelihood of adopting the cloud.
  - Performing a comparison between the sectors based on their selection of the type of the service when planning to adopt cloud computing.
  - Sectors’ comparison based on their selection of the factors that encourage their decision to adopt cloud computing.
  - Sectors’ comparison based on their selection of the barriers that affect their decision to adopt cloud computing.
  
- **Tools for Transparency Assessment**
  - The respondents will independently assess the tools of transparency, such as CSA STAR, CTP and CloudeAssurance. The purpose of the assessment is to investigate the tools in terms of the following criteria:
    - Usage
    - Helpfulness
    - Future Usage
  - Assessing the tools of transparency from the point of view of both adopters and non-adopters across different sectors, such as IT, education, governments, healthcare, telecommunications and banks. The tools will be assessed according to their usage, usefulness and future usage.

- **Respondents' demographic data**

Demographic information can provide important information about certain populations: [88].

- Employment status
- Job title
- Level of education
- Years of experience
- Scale of enterprise
- Enterprise's working sector
- Respondent's role and influence

### **4.3 Targeted Respondents**

The aim of the survey was to study the factors that affect customers' adoption of cloud computing, and the extent to which existing tools and frameworks for transparency have or have not encouraged potential cloud customers from different sectors to migrate to the cloud. Correspondingly, targeted respondents were chosen from both the technical and business sides of organisations, in an effort to encompass those who have an understanding of the technology and technological requirements for organisations, as well as those with experience in understanding business goals and the procurement and funding of IT projects. The respondents were offered a set of role descriptions from which to choose, or they could provide a free text description. The following section thoroughly explains the conducted method of designing the survey questionnaire.

#### **4.4 Significance of the Participant's Population**

The population size that has been targeted in the survey questionnaire is large, as it has been distributed through LinkedIn to several groups. However, knowing the sample size (i.e. the number of completed responses) is important to gain confidence in the results. In order to know the right sample size three parameters need to be taken into consideration. They are population size, confidence level, and the margin of error. We assume the population size would be 500, the confidence level is 95% and the margin of error is 10%. Calculating the sample size will give us 81 responses that need to be received. In our study, we received 87 responses, which are considered significant compared to the sample size.

#### **4.5 Methodology**

The survey was launched in early October 2012, with the intention of collecting responses over the course of 2 years. The reason for choosing 2 year's period was that the survey would be conducted in several countries and across multiple industrial sectors, including education, banks, governments, information technology and healthcare. The questionnaire was designed using online survey tools in order to study the factors that affect customers' adoption of cloud computing, and the extent to which existing tools and frameworks for transparency have or have not encouraged potential cloud customers from different sectors to migrate to the cloud.

The online survey was both effective and convenient. It was effective as it broadened the accessibility and reach of respondents, and was convenient in that it did not require an immediate response from the respondent, allowing each respondent to complete the questionnaire at their own pace. A mailing list for respondents was created, the survey was posted online and invitations to participate were sent to create a mailing list. The mailing list was created using a variety of groups that specialise in cloud computing security and transparency, such as CSA, CSA STAR Support Group, Cloud Computing, SaaS and Virtualization. The survey questionnaire participant information sheet was sent to the abovementioned groups via LinkedIn [64]. In addition, the mailing list was created and collected from the websites of banks, education, healthcare, telecommunication, government and IT sectors.



Quality of the collected data is an important factor in this study. Therefore, the aim was to send the survey questionnaire to a respondent who could influence the organisation's decision towards adopting, or not adopting, cloud computing technology. In order to get this quality of data, a question was presented to the respondent asking them to indicate whether, in their own opinion, their role could influence the enterprise's decisions regarding adopting a cloud computing solution. It is also recommended that questionnaires should be piloted before they are distributed to the targeted respondents [62]. This is mainly important in order to detect any errors in the questions and have them corrected prior to the main survey. In addition, it will maximise the response rate and minimise the error rate on answers [89]. We have conducted a pilot survey before the survey's distribution and it was sent to the staff and PhD students of Newcastle University. The feedback that has been received was valuable. It has corrected the questions that were not clear enough to the reader.

## 4.6 Reliability of Data

The risk of receiving automated responses filled by a program or multiple responses filled by the participant is possible. For instance, a software bot can generate automated responses in order to fill in the questionnaire several times with various inputs.

In addition, about the multiple responses problem this could happen when:

- The participant disable the web browser's cookies and this will lead to multiple access to the questionnaire. The participant has the control of disabling or enabling the cookies.
- SurveyMonkey response format is set to "Multiple Responses per Computer". However, in our case the response format is already set to "Single Response per Computer".

In order to solve the above-mentioned problems, SurveyMonkey provides three possible solutions that could protect against automated and multiple responses.

The first is to create a password to the survey questionnaire's WebLink. This solution would prevent from receiving automated responses filled by bots. However, might not work against receiving multiple responses filled by the participant. This is mainly because the participant, which will give him an access to the questionnaire multiple times, might disable Cookies.

The Web Link collector has advantages and disadvantages. The main advantage is in reaching large number of respondents and responses. The disadvantage of using the Web Link collector is that it could lead in having multiple responses from one computer.

Having said that, this can be solved by using Cookies that are enabled in the browser, which will prevent the respondent from answering the questionnaire twice. The Cookies on web browser are enabled by default. In case the respondent manually disable the cookies, SurveyMonkey does have the capability to record

the IP address of the respondent's answer in order to track it and then delete the repeated answer.

The first solution has been used but without setting a password, this is because of the risk of respondents leaving a questionnaire partly completed, forgetting their password and not going to the trouble of requesting a new one, and hence failing to return.

The second solution uses an Email invitation collector that will create a unique link for each respondent. This solution is a prevention mechanism against bots as it can be only used by the legitimate participant that received the invitation and cannot be used anyone else.

The third approach is to use open-ended questions at the start of the survey. The third approach will act CAPTCHA. A prevention mechanism from bots where it will identify whether the one behind the computer is human or a bot.

What has been done is that, the survey questionnaire was distributed using three methods (1) Web Link collector (2) Email Link Collector and (3) Open-ended questions in order to prevent or minimise the possibility of receiving illegitimate responses.

WebLink method was used when distributing the survey through social media such as LinkedIn. The Email Link method was used when sending the survey questionnaire to the list of emails that have been gathered from the respondents' web portals.

## 4.7 Questionnaire Design

The structure of the survey questionnaire was explained to the respondent through the “participant information sheet”, which contained brief information related to the purpose of the study, the likely time it would take to complete the survey and the anonymity statement that guaranteed the anonymity of the respondents.

The online survey questionnaire had two sections. The first section aimed at gathering information on cloud computing adoption drivers and constraints for enterprises. The levels of cloud computing adoption can vary according to the type of organisation, industry sector, and geographical location [83, 90]. The first nine questions posted in this section aimed at understanding the respondents’ employment status, level of education, experience in IT, the size and nature of their enterprise, the geographical location of the respondent’s enterprise, their role in their enterprise’s decision making and their familiarity with cloud computing solutions. This was important because personnel at different levels of management, and with different levels of involvement in IT decisions, may have different understanding of technology and its impact on the organisation [46]. The geographical location of the enterprise is affected by legislation and compliance issues. The organisation size is also important as it affects how different systems and SLAs are managed.

The respondent answered a logic question relating to their prior usage of cloud computing solutions. If the respondent indicated that they have used a cloud service solution, this section then presented five questions that aimed to analyse the selection of deployment model (e.g. IaaS, PaaS or SaaS models), the type of cloud that was chosen for delivering the respondents’ services (for example, whether it was a public, private or hybrid cloud), and the reason for selecting the type of cloud model. Justification could be obtained from a further question that related to the type of data and applications being hosted in the cloud. As choosing the right service model depends upon the information sensitivity and client’s requirements, for example, healthcare SaaS, clients required more security and privacy mechanisms to trust cloud computing because they are outsourcing their data and infrastructure to the cloud. [91] Moreover, it ascertained if the respondents had relied on a single cloud provider to deliver their service or whether they used different cloud providers to fulfil their requirements. The last question in this section aimed to understand the reasons for adopting cloud computing solutions. It highlighted some of the reasons that could be presented to the respondent, which are the elimination of the up-front investment, the increased reliability through redundancy,

the higher flexibility of resource allocation and de-allocation, the ability to pay for the use of computing resources and the tools for selecting the cloud service provider's offerings.

If the respondent answered "No" to the logic question on prior use of cloud service solution, four questions were presented in order to analyse the constraints on the adoption of cloud computing solutions. The first question began by assessing the likelihood of the respondents towards adopting cloud computing using the "Likert scale". There is a comment box that has been created by the tool in order to analyse the respondent's comments concerning the likelihood of their adopting the cloud. For instance, if the respondent chose to say that they are less likely, or never, considering the adoption of the cloud computing solution, then it's worthwhile to know the reason for that. The three remaining questions that were considered in the survey included the choice of deployment model that the respondent expressed their opinion on, when planning to adopt cloud solutions, the possible motivations that could encourage them to adopt the cloud technology, in addition to the barriers that might inhibit their organisation from adopting the cloud computing. To cite some of the barriers to adopting the cloud computing solutions that [46,81, 82, 83, 90] identify, are isolation failure in a multi-tenant environment, data lock-in, lack of security guarantees, legal considerations, lack of transparency, malicious insiders, business continuity and data confidentiality and auditability.

The second section of the questionnaire aimed at understanding which of the market's existing tools or frameworks of transparency have or have not helped participants in: adopting cloud computing solutions, selecting the cloud service provider that matches their business security requirements, identifying which tools have mostly helped or not in making informed decisions and obtaining feedback from the participants in the use of transparency tools to evaluate and select the cloud service from different providers.

During the design of Section 2, the questions were developed to analyse the participants' responses. The objectives of this section were to establish:

- The importance of transparency tools in evaluating the cloud service provider's transparency
- The likelihood of using transparency tools for the purpose of evaluating the cloud service provider.
- The familiarity of the transparency tools and whether they have been used recently.

- The helpfulness of the transparency tools.
- The willingness to use the transparency tool again in the future.

Eleven questions were presented to the participant to cover the above scenarios. The first logical question asked the participant's opinion about the importance of having a tool that would help in evaluating the cloud service provider's transparency, and whether it would encourage the respondent to make a decision about moving to the cloud. The logical question allows three possible answers (yes, no and don't know). The respondent then continued to answer the remaining ten questions depending on the obtained answer.

If the response was "no", the respondent would not be able to continue answering the remaining questions. However, the logical question was set up to solicit the respondent's reason for not agreeing to use the tools for evaluating the provider's transparency, by allowing a free-text comment. We could envisage that this question should not exclude the participant from answering the other questions. This is because it is important to know whether they could have used these or other tools, even if they don't agree to use them for the purpose of evaluating a provider's transparency and migrating to the cloud. Having said that, it is easy to modify the logical question so that future respondents can answer the remaining questions related to the assessment of tool's usage and usefulness. However, due to the time left for the submission of the thesis, and the expected number of responses that will be gathered for a period of seven months, it was better to make the modification as a future work. In addition, the survey results showed that 11% of the respondents did not agree to use the tools, which might not be significant compared to the 89% who did.

If the response was "yes" or "don't know", the assessment of the likelihood of the respondent's using tools for evaluating the provider's transparency was done through a rating structured question that includes "strongly disagree", "disagree", "undecided", "agree" and "strongly agree". In order to further analyse the respondent's choice, an option was provided to give feedback when expressing disagreement with using the tools for the purpose of evaluation.

The remaining nine questions were grouped into three sets. The first set presented three questions to the participant in order to assess their response towards the usage of the CSA STAR registry, its helpfulness, and to examine their interest in using the CSA STAR in the future to search for the right cloud service provider. The first question was based on a "yes" and "no" response pattern, asking the respondent if they had used the CSA STAR when

searching for a cloud service offer. The second was a rating question type that asked the respondent to categorise the degree of helpfulness as “not helpful”, “a little helpful”, “undecided”, “helpful” and “very helpful”. Again, a comment field allowed free text discussion of the possible reasons, if their opinion on the helpfulness of the CSA STAR registry was low.

The second set presented three questions asking respondents to evaluate the CTP in terms of its usage, usefulness and the likelihood of using it in the future to search for a cloud service offering. The final set also contained three questions, which asked respondents to evaluate the CloudeAssurance’s helpfulness in searching for the right provider, whether it had been used to search for a cloud provider and/or would be used in the future.

When designing the survey questionnaire, we have taken into consideration the customers’ point of view. The customers’ assurance requirements that have been identified in the literature (Chapter 2) could bring assurance to the customers providing that the existing tools, such as CloudeAssurance, CTP and CSA STAR, would satisfy them.

## **Chapter 5: Factors Affecting Customer’s Adoption of the Cloud – Survey Results**

### **5.1 Introduction**

In October 2012, a survey questionnaire “Cloud Computing Adoption Issues and the Tools Encouraging Migration to the Cloud” (<https://www.surveymonkey.com/s/GCYORRG>) was developed and distributed globally, using the popular online tool SurveyMonkey. Over 2 years, the total number of responses received from various countries is 177. The number of completed responses is 99 responses. The aim of the questionnaire was to gather information from potential cloud customers working in different sectors, such as information technology, healthcare, banks, telecommunications, governments and education, for investigating the adoption constraints and drivers of cloud solutions. The second part of the survey related to assessing the importance and usefulness of tools in migrating to cloud computing solutions and selecting the right cloud service provider, such as CSA STAR, CTP and CloudeAssurance. The reason for selecting these tools is that they adopt CCM, the best industry-accepted security standards, that promote security transparency in cloud computing [92]. In this section the analysis of the survey is presented. The findings from the data collected are presented together with their analysis.

This chapter discusses the results of the first part of the survey questionnaire. The results of cloud computing adoption issues and drivers from the point of view of the adopters and non-adopters are presented in Section 5.3.1 and Section 5.3.3. A comparison between sectors is presented for groups of respondents who have or have not adopted the cloud in Section 5.3.2 and Section 5.3.4. The conclusion is set out in Section 5.4. The results of the second part of the survey are described and discussed in Chapter 6.



## 5.2 Respondents' demographic results

There is a huge difference concerning the responses that have been received from the participants. The largest proportion of responses came from Saudi Arabia (51.7%), followed by United States (7.9%) and United Kingdom (7.8%). Having great difference in responses could be justified by the scientific trip that has been conducted in Saudi Arabia, which has given us flexibility to reach the participants and receive their responses.

The following tables will present the respondent's employment status, job title, level of education, years of experience, working sector, enterprise size and influential role.

- Respondents' Employment Status

Responses received from participants who are not employed or business owners or independent researchers have been excluded from the survey questionnaire. They have been excluded because the level of adoption of cloud computing could be affected by several factors, one of which is the job domain [87]. Table 4 shows the percentages of the respondents' employment status.

Table 4. Respondents' Employment Status

<b>Respondents' Employment Status</b>	<b>Percentage</b>	<b>Count</b>
Employed	87.9%	87
Not Employed	10.1%	10
Other (Business owner and Postdoc Research Scholar)	2.0%	2

- Respondents' Job title

Table 5. Respondents by Job Title

<b>Respondents Job Title</b>	<b>Percentage</b>	<b>Count</b>
Software Engineers	1.20%	1
Software Analysts	1.20%	1
System Engineers	1.20%	1
VP	1.20%	1
Database Analysts	1.20%	1
Systems Programmers	1.20%	1
Systems Administrators	1.20%	1
Quality Assurance	1.20%	1
Network Engineers	1.20%	1
Software development manager	1.20%	1
Web Developers	1.20%	1
Database Administrators	1.20%	1
CTO	2.41%	2
Director	2.41%	2
Technical Consultants	4.82%	4
Project Manager	4.82%	4
Software Developers	4.82%	4
CIO	4.82%	4
IT Consultant	6.02%	6
Security Specialist	7.23%	7
IT Director	9.64%	9
Manager	12.05%	10
Others	26.51%	23

- Respondents' Level of Education

Table 6. Respondents by Level of Education

<b>Respondents' Level of Education</b>	<b>Percentage</b>	<b>Count</b>
Bachelor's degree	38.27%	31
Master's degree	40.74%	38
Doctoral degree	17.28%	15
Professional degree	2.47%	2
Other	1.23%	1

- Respondents' Years of Experience in IT

Table 7. Respondents by Years of Experience

<b>Respondents' Years of Experience</b>	<b>Percentage</b>	<b>Count</b>
1-5	16.05%	13
6-15	55.56%	47
16-30	27.16%	26
Over 30	1.23%	1

- Respondents' Enterprise Size

Table 8. Respondents by Enterprise Size

<b>Respondents' Enterprise Size</b>	<b>Percentage</b>	<b>Count</b>
< 10 Micro	3.70%	4
< 50 Small	9.88%	9
< 250 Medium	18.52%	15
> 250 Large	67.90%	59

- Respondents' Working Sector

Table 9. Respondents by Work Sector

<b>Respondents' Working Sectors</b>	<b>Percentage</b>	<b>Count</b>
Information Technology	29.63%	27
Telecommunications	9.88%	8
Education	23.46%	20
Government	22.22%	18
Healthcare	2.47%	2
Banks	4.94%	4
Others	7.41%	8

- The Respondents' Influential Role in the Enterprise

Table 10. Respondents by Influence of Role

<b>Respondents' Roles' Influence</b>	<b>Percentage</b>	<b>Count</b>
Yes	70.0%	61
No	30.0%	26

### 5.3 Adoption of Cloud Computing – Drivers and Constraints

#### 5.3.1 The Adopters

This section presents the results from the questionnaire concerning of the level of adoption of cloud computing. Figure 1 shows the level of adoption, with 52 respondents (60%) stating that they are using cloud computing solutions, whereas 35 respondents (40%) reported that they are not using cloud solutions. The results and analysis of the lack of adoption are presented later in this section. As indicated in Table 10 (presented in Section 5.2), the majority of respondents (69.0%, 58 respondents) indicated that they have influence on their enterprise’s decision regarding the adoption of cloud computing solution. This might suggest that a respondent with an influential role on the enterprise could be considered as an important factor towards adopting cloud computing technology.

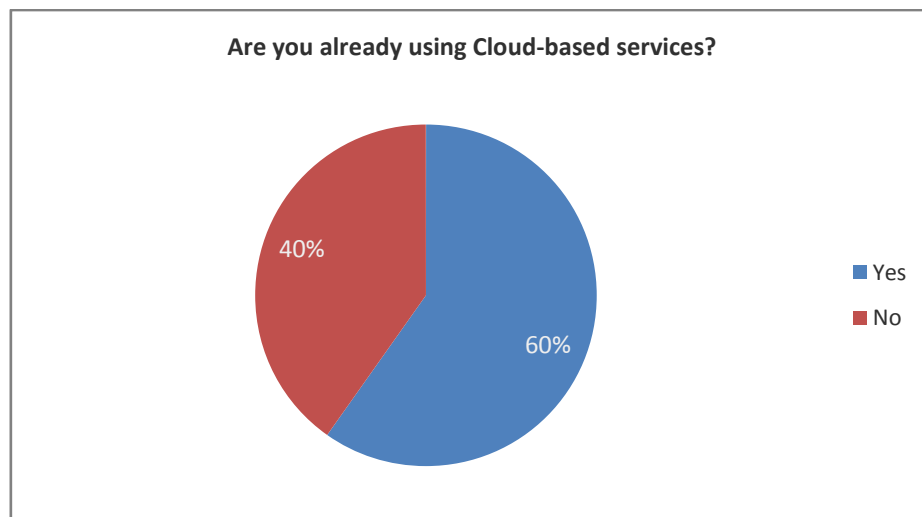


Fig.3. Cloud computing adoption percentage.

The type of cloud delivery model chosen by the adopters of cloud computing were as follows: 71% (SaaS), 53% (PaaS), 45% (IaaS) and 16% (others). In this sample, SaaS is still the dominant model [35, 84]. Moreover, it has been suggested that the SaaS model is the reason for market growth [93]. Our findings comply with another study's results [35]. The reason for choosing the SaaS model might be because of the promise of benefits, such as improved operational efficiency and reduced costs [84].

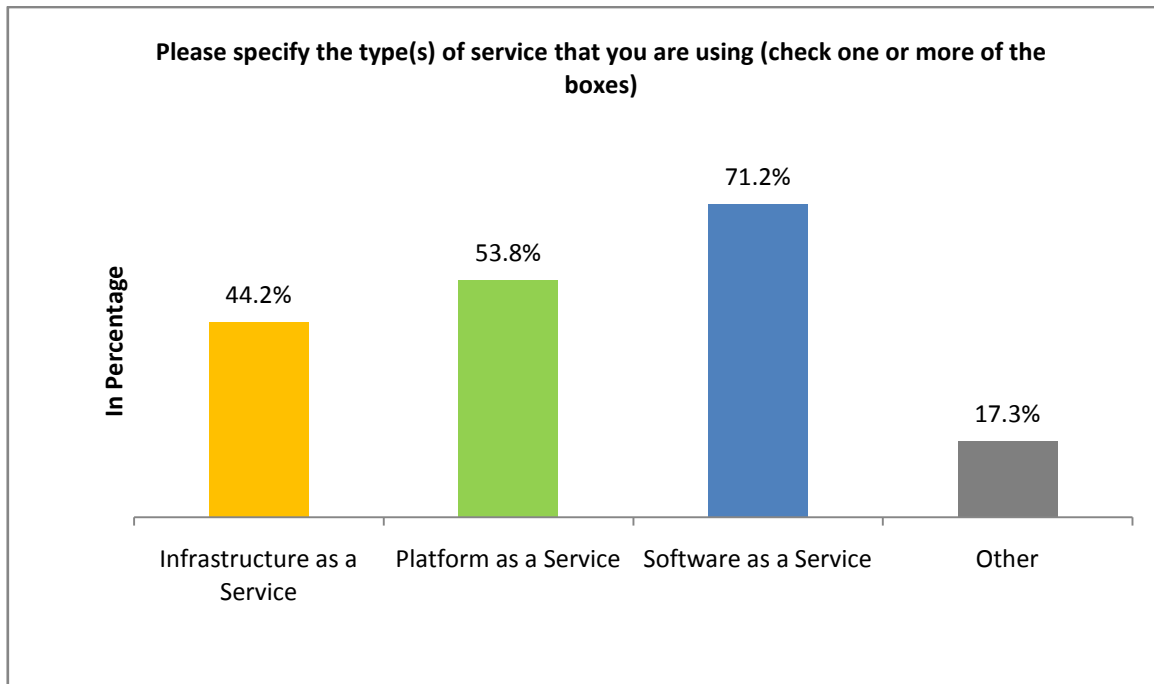


Fig.4. Type of cloud service adopted.

Figure 5 shows the respondents' selection of the cloud's deployment model (Public, Private and Hybrid) that is mainly used to host the cloud delivery models, such as SaaS, PaaS and IaaS. (36% of the respondents have selected the private cloud to outsource their work. Public and hybrid clouds share the same number of responses (29%). Within the remaining 6% of respondents, one, working in a governmental sector in Singapore, stated that they have used all types of delivery models (SaaS, PaaS and IaaS) and all types of deployment models (Public, Private and Hybrid), and this decision was based on the organisation's needs and the classification of data. The others mentioned that they were cloud service providers who expressed their opinion of adopting cloud computing as an opportunity to make partnerships.

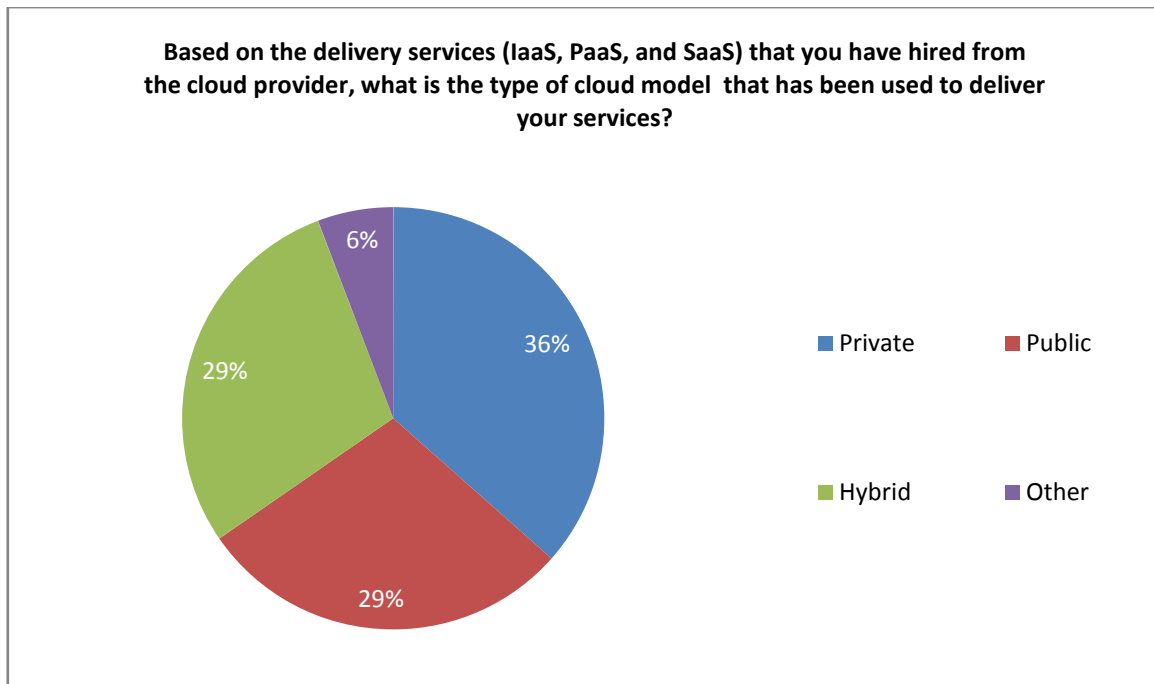


Fig.5. Respondents' selection of deployment models.

We have queried the respondents' reasons for their selection of the type of clouds for hosting their applications and data. The results were based on asking the respondents' for the nature of the data and applications that would be hosted in the cloud. The classification of the data and applications includes: non-mission critical application and data, mission-critical applications and data, non-mission and mission critical applications and data, and the last classification was left open for other reasons that the respondents might think about. Figure 6 shows the results with 33% of respondents stating that their enterprise's data and application are sensitive. The category "Non-mission-critical applications and data" and "Mission and Non-mission-critical applications and data" both comes in second with 25%. The remaining 17% have mentioned different opinions on their selection of the type of the cloud. These include the following:

- Sub client data sensitivity
- High availability for ram for Ansys Software
- Depending on the needs and the classification level
- Cost
- Exploration of options for our customers
- Using Office 365 to host student emails

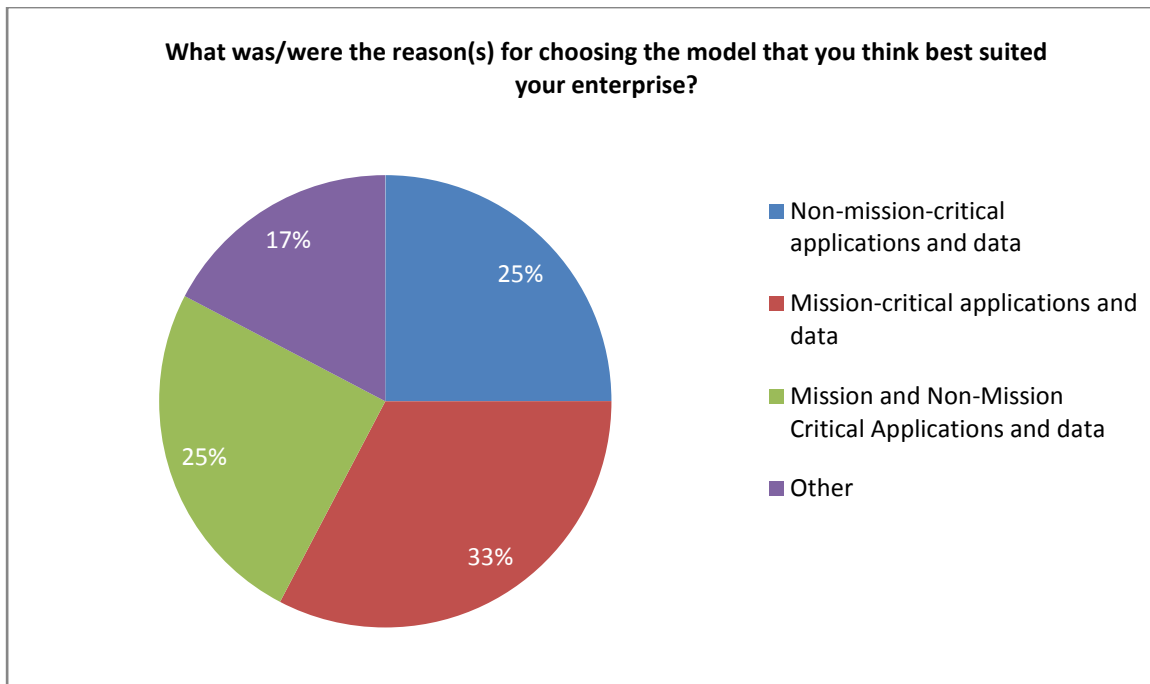


Fig.6. Justification of the enterprise's selection of deployment model.

From Figures 5 and 6, we can envisage that the classification of the data and applications of the enterprise can have an effect on the selection of the type of cloud (public, private or hybrid). It is claimed that choosing a public cloud offers benefits to the enterprises, such as cutting costs of investing in new infrastructure, and shifting risks to the cloud service provider. However, they lack fine-grained controls over the data, network and security settings [94] and are more vulnerable to attacks [92], whereas the private cloud offers a higher degree of control over performance, reliability and security. They have, however, been criticised for being similar to traditional data centres that do not provide the benefits of cost reduction. The hybrid cloud is much more flexible compared to the others where it tries to alleviate the limitations of both approaches. It provides tighter control and security over data and applications. However choosing the hybrid cloud should entitle the enterprise to select carefully which part of the data and applications are being shifted to public or private clouds [94].

We have compared the results of those who have adopted the private and hybrid cloud for mission-critical and non-mission critical applications and data. It can be noticed from Figure 7 that the classification of data and applications has affected the respondents' selection of the type of cloud. For example, 70% of the respondents have chosen a private cloud to host their mission-critical applications and data, whereas this percentage reduced by 40% to only 30% of respondents adopting the same cloud where they have stated that they possess both

mission and non-mission critical applications and data. Vice versa, there was an increase of about 10% of respondents adopting the hybrid cloud rising from 45.5% to 54.50%, depending on the classification of the data and applications.

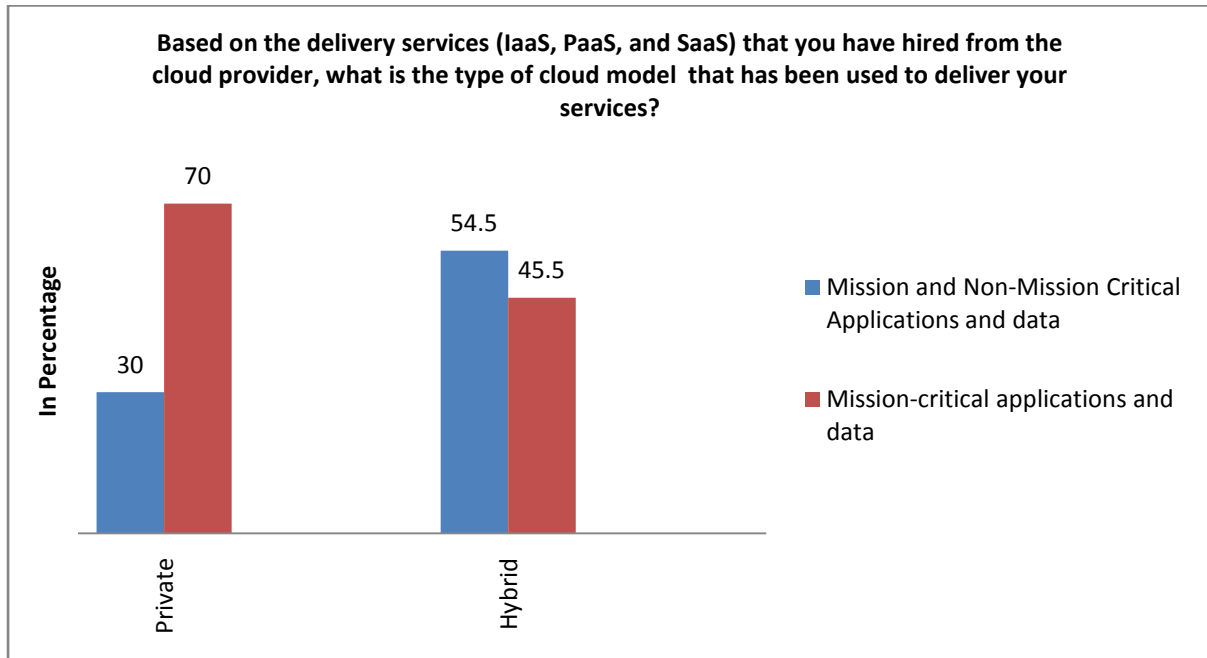


Fig.7. Private vs. Hybrid adoption.

Figure 8 shows the results of the respondents who have used single and multiple cloud service providers in order to host their application or data. 54% have preferred to choose several cloud providers to receive different cloud services that meet their business requirements. 46% of the respondents have used a single cloud provider. The selection of either a single cloud provider or multiple cloud providers might depend on the type of cloud and the classification of the applications and data. With regards to the type of cloud, the public cloud is more vulnerable to both technical and business risks, such as outages and other service failures, and so the respondents might have preferred to consider a multi-vendor strategy [95]. We will try to interpret the respondents' selection based on the type of the cloud model that has been selected and the classification of the applications and the data. Moreover, in general, we will show the results of the sectors who used single and multiple cloud providers.



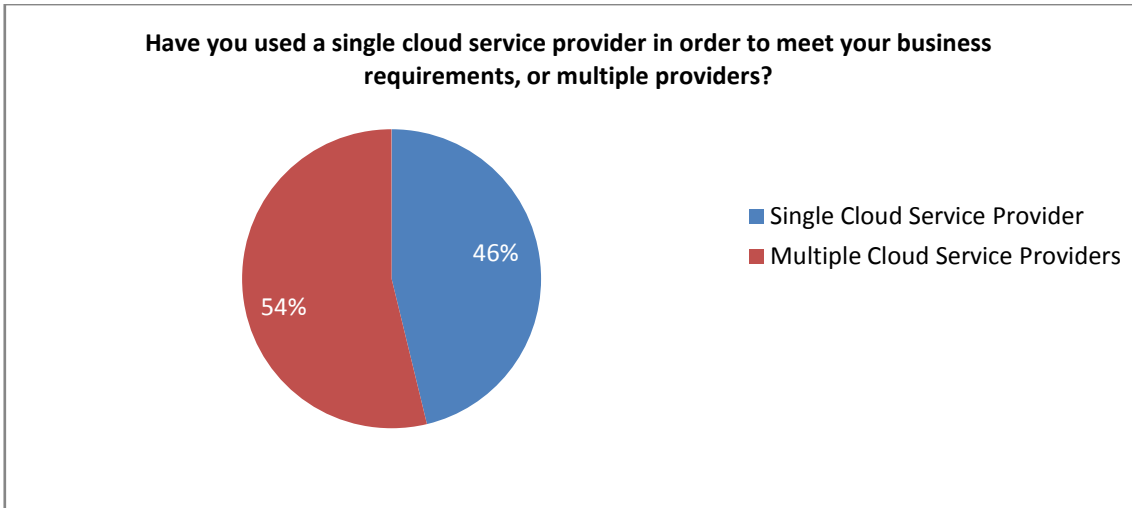


Fig.8. Respondents' selection of cloud provider.

Figure 9 shows a comparison between the respondents' selection of either a single or multiple cloud providers, based on their prior selection of the type of the cloud. It can be seen from the Figure below that the single cloud provider is highly selected (52%) in private clouds and it is reduced by 22% when the public cloud is selected. This could confirm that one of the factors, such as the type of data and applications being hosted in the cloud, could have an effect on the selection of the number of cloud providers.

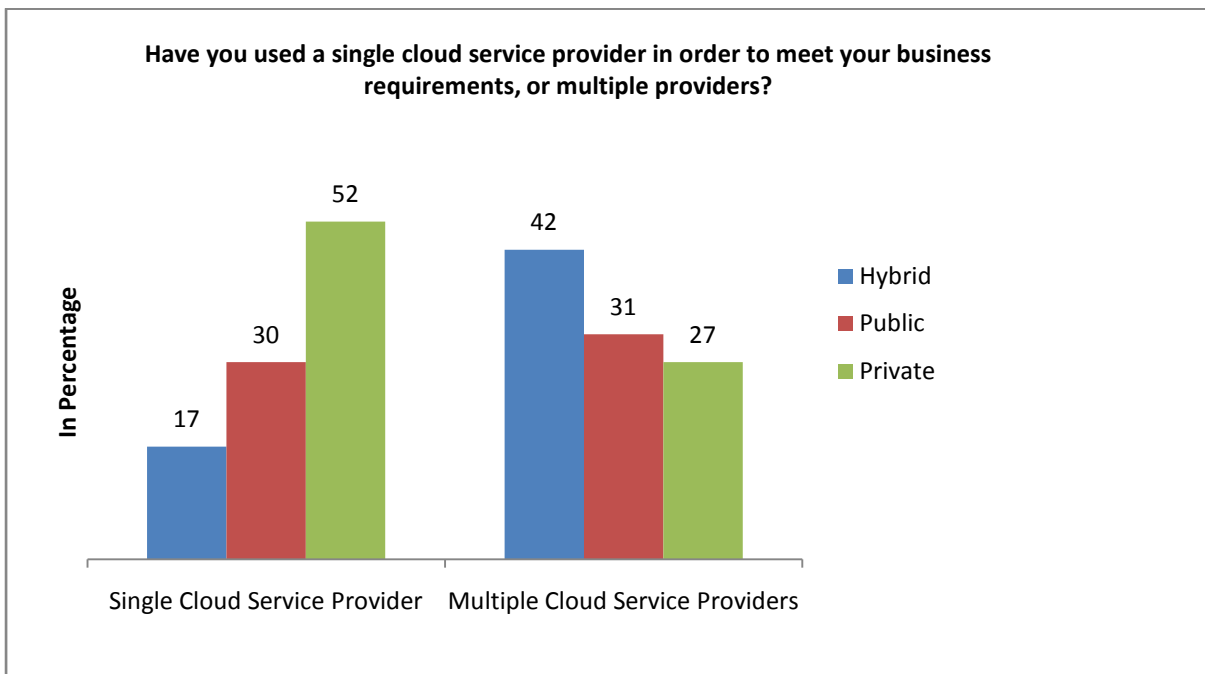


Fig.9. Single CSP vs. multiple CSP based on cloud selection.

Table 11. Respondents' Selection of Single/Multiple Provider Based on Cloud Type

<b>Have you used a single cloud service provider in order to meet your business requirements, or multiple providers?</b>					
<b>Based on the delivery services (IaaS, PaaS, and SaaS) that you have hired from the cloud provider, what is the type of cloud model that has been used to deliver your services?</b>					
<b>Answer Options</b>	<b>Private</b>	<b>Public</b>	<b>Hybrid</b>	<b>Response Percentage</b>	<b>Response Count</b>
Single Cloud Service Provider	13	8	4	50%	25
Multiple Cloud Service Providers	7	7	11	50%	25
<i>answered question</i>					<b>50</b>
<i>skipped question</i>					<b>0</b>

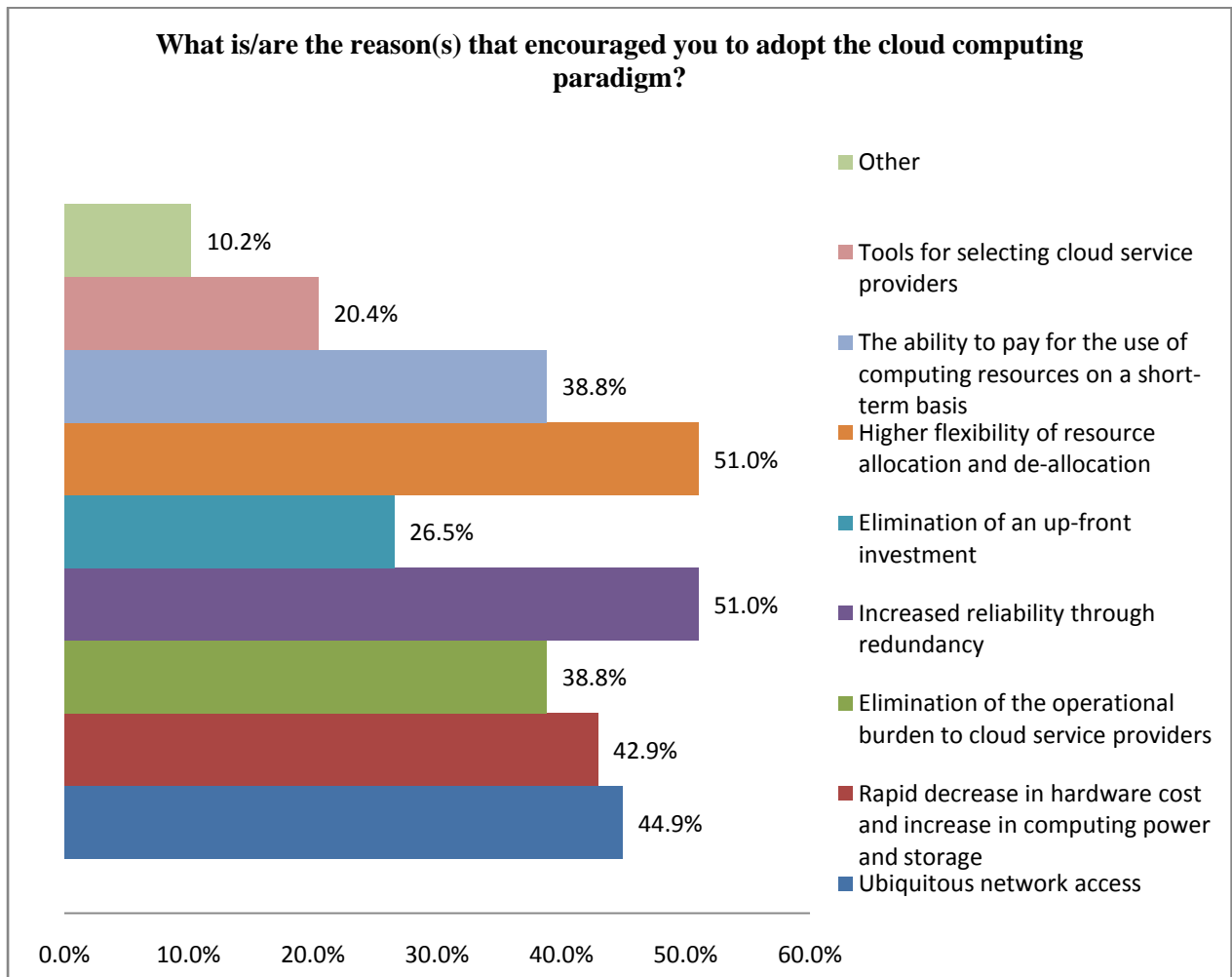


Fig.10. Motivation behind adopting cloud computing.

There are several factors (presented in Figure 10), which have also been identified in the literature that might encourage cloud customers to adopt cloud computing solutions. From

the survey results we found out that the respondents who currently use cloud computing mentioned that the top two joint factors (51%) were the higher flexibility of resource allocation and de-allocation and the increased reliability through redundancy. Following this, approximately 45% of the respondents stated that the ability to access the services from anywhere and anytime was an influential factor in their decision. The rapid decrease in hardware costs and the increasing computer power was ranked in third place (42.9%), despite the fact that several surveys have suggested that the cost factor usually comes in first place when adopting the cloud [85, 96, 97, 98]. Paying for the computing resources and the elimination of the operational burden to cloud providers was jointly selected with 38.8%. About 27% of the respondents emphasised the benefit of eliminating the upfront investment. The tools for selecting cloud providers was the least influential factor (20.4%) in the decision to adopt cloud computing. There are other reasons that had encouraged the respondents from adopting the cloud; this includes lower costs in general and one of the respondents was encouraged by having better user experience than prior solution.

### **5.3.2 Adopters – a Comparison between sectors**

We compare now the adoption of the delivery models, such as IaaS, PaaS and SaaS, amongst different sectors in either industry or academia including banks, healthcare, government, education (such as universities), telecommunications and information technology enterprises.

The adoption level of the SaaS model is the highest amongst the models and it accounted for 83% of adoptions in both the education and governmental sectors, followed by the IT domain at 76%. The adoption level of the PaaS model is the lowest with both telecommunications and banks sectors accounting for 40% and 33% respectively. With regards to the PaaS model, it can be noticed that it is the second preferable model in almost all the sectors: governments (67%), telecommunications (60%), IT (59%) and education (58%), with the exception of the banking sector where the PaaS adoption level is 33%. The IaaS model can be regarded as the least adopted delivery model, compared to SaaS and PaaS. The percentages are as follows: banks (67%), IT (59%), education (42%), governments (33%) and telecommunications (20%).

Overall, the Figure below shows that the dominant model for the banking sector is the IaaS model. Education, governmental and IT enterprises tend to use the SaaS model.

Telecommunication companies are more likely to adopt the PaaS model and the healthcare sector preferred to choose between either the PaaS or SaaS models.

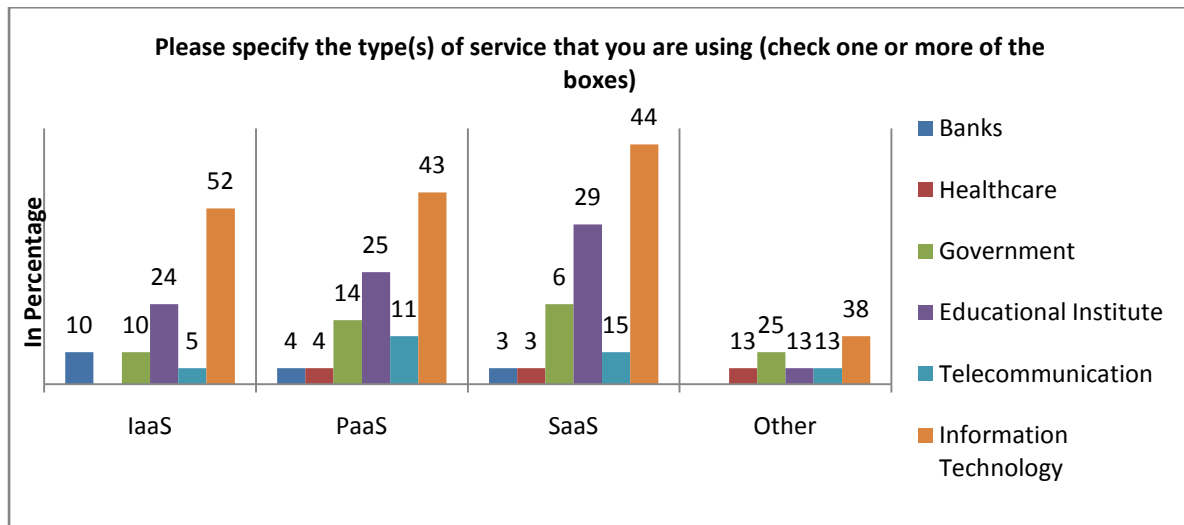


Fig.11. Sectors' adoption of delivery models.

Figure 12 shows a comparison between several working sectors based on their adoption on the type of cloud. The healthcare sector has not been included in the chart because of no responses were received in that domain. It can be noticed from the chart below that the preferences on the type of the cloud vary from one sector to another. However, 40% of the respondents representing various working sectors, preferred to choose the private cloud. The public and hybrid clouds are jointly chosen, representing two thirds of the respondents' sample. Several factors can affect the sectors' adoption of the deployment models. That includes the nature of the data and applications and the size of the enterprise.

Generally the chart shows that the IT sector is the highest adopter of cloud computing technology in each deployment model. Education comes second, then governmental and telecommunication companies. The banks are the least likely sector to adopt the cloud in this survey. It is worth mentioning that banks choose the private cloud as their deployment model. This might be due to the customer sensitive data that the bank holds. We are also keen to know if the banking sector intends to use a single or multiple cloud providers. This is an important question as the banks might also see redundancy as an important factor in saving critical data from being lost from outages.

The following Table shows the ranking of each sector in adopting each deployment model.

Table 12. Sectors' Ranking Based on Private, Public and Hybrid Clouds

Ranking	Ranking in private cloud	Ranking in public cloud	Ranking in hybrid cloud
1	IT	IT	IT
2	Edu.	Edu.	Edu.
3	Gov.	Tele.	Gov.
4	Banks	Gov.	Tele.
5	Tele.	Banks	Banks

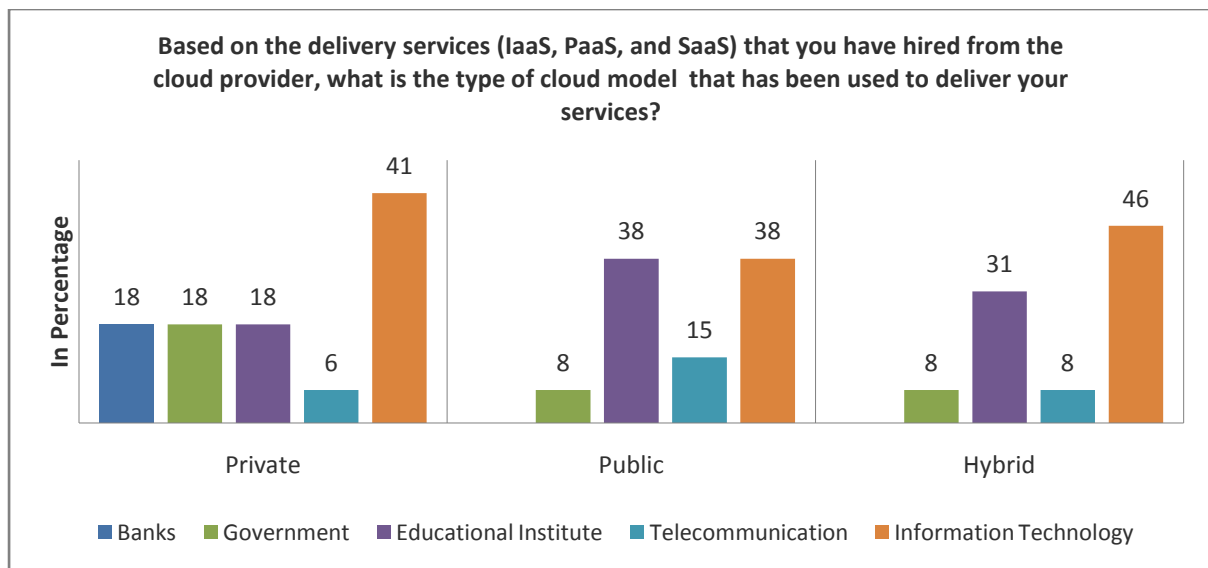


Fig.12. Sectors' adoption of the deployment models.

As shown in Figure 13, the banking sector is the only domain that hosts mission-critical applications and data and this confirm the reason for its choosing private clouds to host their sensitive application and data, rather than relying on public or hybrid clouds. We aim to know, to some extent, the nature of the data that different working sectors have. Therefore, the data has been classified into three categories; it includes non-mission-critical applications and data, mission-critical applications and data and combined mission and non-mission critical applications and data.

The respondents to the first category were from the IT sector (40%), followed by the governmental domain (30%), education (20%) and, to a far lesser extent, the telecommunication sector (10%). The bank sector proves that their data and applications are critical. In the second category, the education responses were 11% higher, indicating that the type of data or applications that they hold is sensitive. The number of responses from the IT

sector is reduced by 15% in the second category, compared with the first, and the figure for the governmental sector is lowered to 17%. The banks sectors' responses were 100% for mission-critical applications and data. The last category, which is a combination of both the sensitive and non-sensitive data and applications, shows that the IT sector has the highest take-up in this category with 62%, when compared to other categories. The education sector was lower by 8% in the second category and greater by 3% from the first category.

So, the responses that we have received indicate that IT companies are holding both sensitive and non sensitive data and applications and is confirmed in Figure 10, which demonstrates their preference for the selection of both private and hybrid clouds. With regards to the education sector, the best selection so far is the category: mission-critical applications and data. Despite the nature of the data that the education sector holds, their selection of the public cloud is still the highest, followed by hybrid and private cloud. The responses from the telecommunication sectors show that they mostly hold mission and non-mission critical data and applications rather than non-sensitive data on itself. The governmental sector mostly uses on-mission-critical applications and data and, despite this, they have adopted the private cloud more than any other type of clouds. This can be justified by the use of the G-Cloud [99].

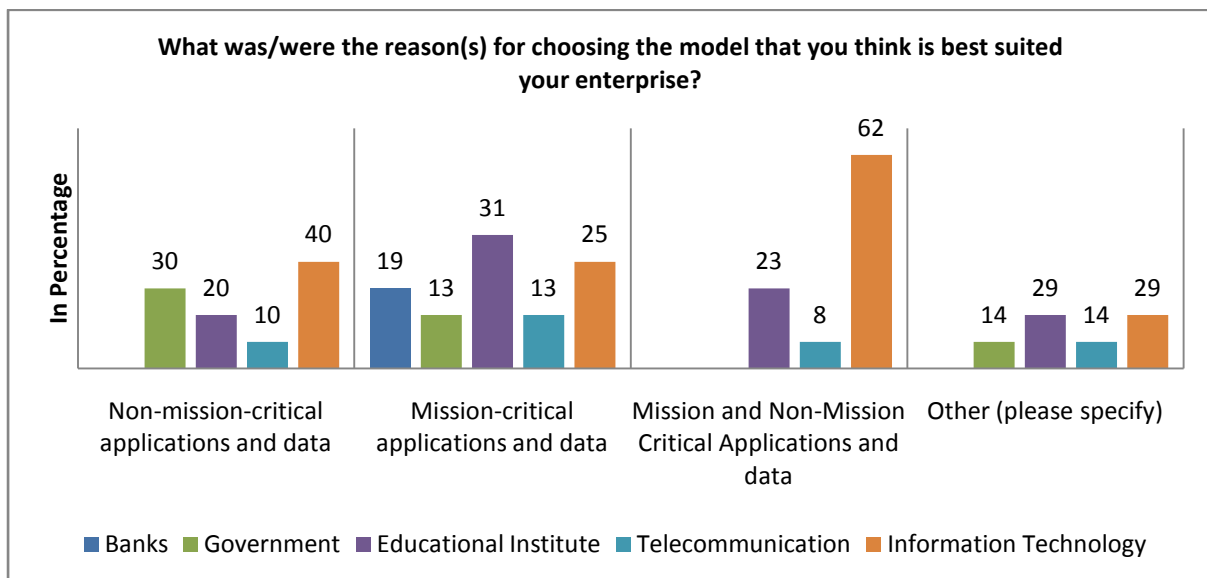


Fig.13. Comparing different working sectors based on the nature of the data.

Figure 14 shows the selection of either single or multiple cloud providers for each working domain. There is a variance in the selection of the number of cloud service providers within the sectors. However, the average is that 51% of the respondents' have chosen to select multiple cloud service providers, closely followed by 49% in the selection of a single cloud service provider. With regards to the selection of multiple cloud service providers, the IT sector is the highest amongst the others receiving 46%, followed by 21% in the education sector, and the governmental and telecommunications sectors are equal at 13%. The banking sector is least likely to adopt the multi-vendor strategy at only 8%.

With respect to the selection of a single cloud service provider, the IT and education sectors are still the highest amongst others, despite the IT's sector decrease (by 14% from multiple provider's selection), whereas the education sector have shown more interest in selecting a single provider and increased by 11%. The governmental sector received a slight increase of 14% from the multiple provider selection. The banks and telecommunications sectors are more attracted to selecting single cloud service provider, rather than relying on multiple providers. It can be seen that there has been a decrease of 4% and 3% in the telecommunications and banks respectively. The healthcare sector is interested in selecting a single provider and none of the respondents have considered choosing more than one cloud provider to host their data or applications.

Table 13. Sectors' Ranking Based on their Selection of Single/Multiple Provider

Ranking	Single CSP		Multiple CSP	
	1	IT	32%	IT
2	Edu.	32%	Edu.	21%
3	Gov.	14%	Gov.	13%
4	Tele.	9%	Tele.	13%
5	Healthcare	9%	Banks	8%
6	Banks	5%	Healthcare	0%

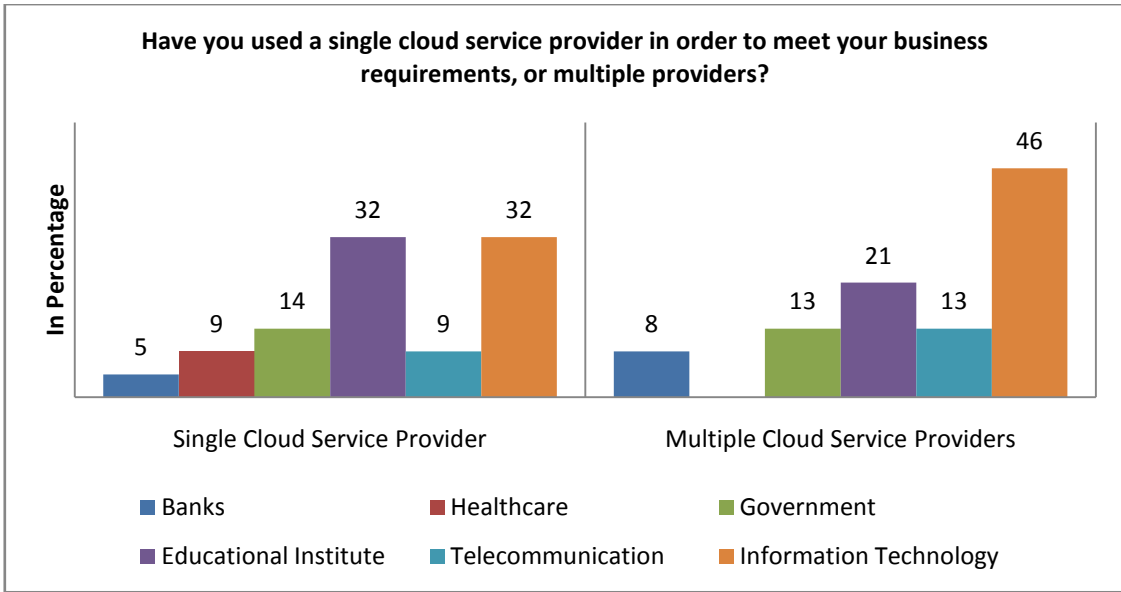


Fig.14. Sectors' selection of the number of cloud providers.



### 5.3.3 Non-adopters

In this section, we describe the results of the respondents who have not adopted cloud computing technology and seek to know the reasons for this. Table 14 shows the results of the respondents' influential role in adopting cloud computing technology. Figure 15 shows that the number of non-adopters rests at 40%, despite the majority of respondents, about 69%, claiming to have an influential role in their enterprise's decisions to adopt new technology, such as cloud computing. It is worth investigating the reasons behind their unwillingness to adopt the cloud.

Table 14. Respondents' Influence in Adopting Cloud Computing

<b>Does your role influence your enterprise's decision whether to adopt or not adopt cloud computing solution?</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Yes	69%	24
No	31%	11
<i>answered question</i>		<b>35</b>
<i>skipped question</i>		<b>0</b>

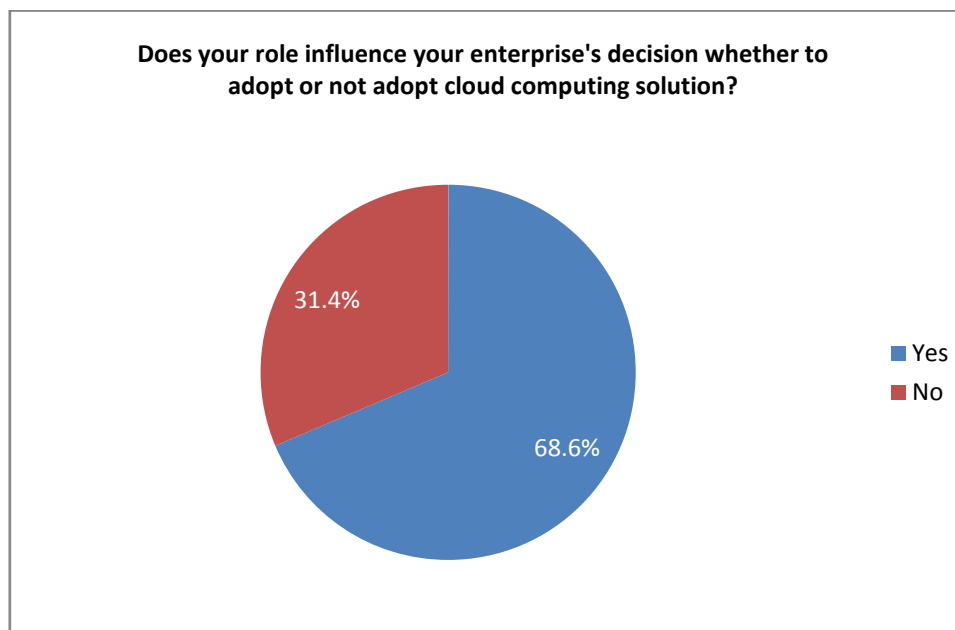


Fig.15. Non-adopters' influential role in adopting cloud computing.

As illustrated in Figure 16, 32% of respondents indicated that they are likely to adopt cloud computing solutions, 25% were less likely to adopt them due to several reasons provided by different sectors in the comments field in the survey. One reason given from a respondent in the governmental sector was that they had security concerns. From the point of view of the banking sector, they mentioned that they are less likely to adopt the cloud for regulatory reasons. Another opinion from the education sector is that they stated that security was a major concern in adopting the cloud. About the same percentage, around 21% of the respondents had no opinion on whether to adopt or not adopt cloud solutions in the future. The “more likely” category has received a considerable amount of responses showing respondents’ interest in adopting the cloud in the future according to their enterprise plans.

Only 4% of respondents reported no interest in adopting cloud computing. This was restricted to the education sector, and they have selected several reasons for not adopting cloud computing, which includes the lack of security guarantees, lack of transparency towards delivered services to the customers and data confidentiality and auditability.

The average rating of the likelihood for adopting cloud computing is 3.36 out of 5.0. This represents 67.2% (non-adopters sample size) expressing their interest in adopting cloud computing in the future. As Figure 15 showed, 68.6% of respondents have an influential role in making decision and this could have been the reason for receiving a higher percentage from the non-adopters sample size towards considering cloud computing adoption.

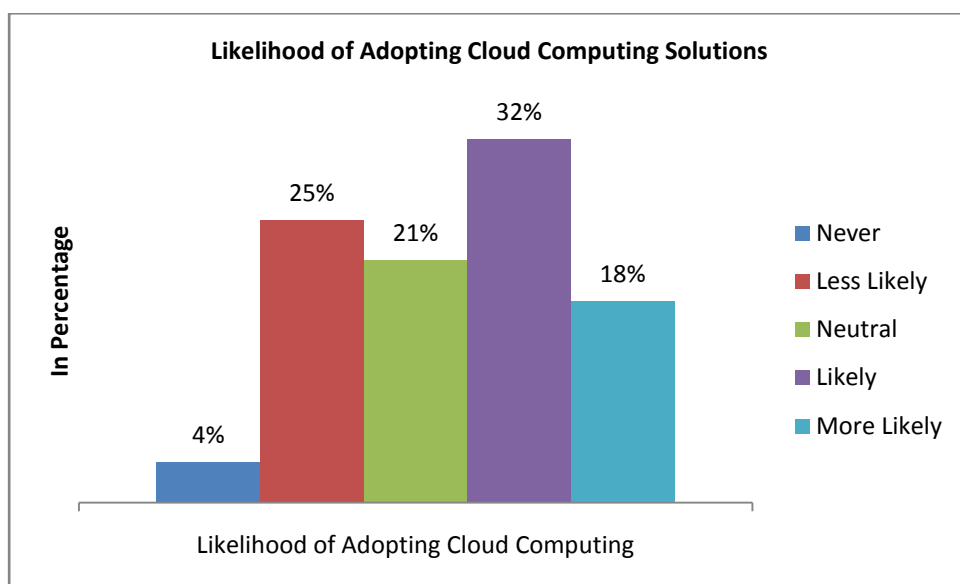


Fig.16. Non-adopters likelihood for adopting cloud computing.

We now describe the results of the respondents who are not adopting cloud computing and planning to select the type of cloud that meets their enterprise requirements. Figure 17 shows that the private cloud is the most popular delivery model (35.7%) that is being considered for adoption, followed by the hybrid cloud at about 36%. With respect to the public cloud, it has been always the least favourite type of cloud for the respondents, from the point of view of adopters and non-adopters, receiving 17.9%. About a quarter of the respondents have not yet decided which type of the cloud they would use when adopting cloud computing. They indicated that this is for several reasons, including the lack of control over IT assets, which has been expressed as a concern by respondents in both education and governmental sectors.

Some responses from the government sector have added the lack of security guarantees from the cloud providers, isolation failure in multi-tenant environments, data confidentiality and auditability, and unclear of the liabilities on SLAs. Respondents from the banking sector emphasised various concerns, such as the lack of security guarantees from the cloud service providers, legal considerations, lack of transparency about cloud providers' security and privacy towards cloud customers' delivered services, data confidentiality and the auditability issue. The respondents from the IT sector shared some of these concerns, such as the lack of security guarantees offered by cloud providers; data confidentiality and auditability has been the most common concern in almost all of the working sectors.

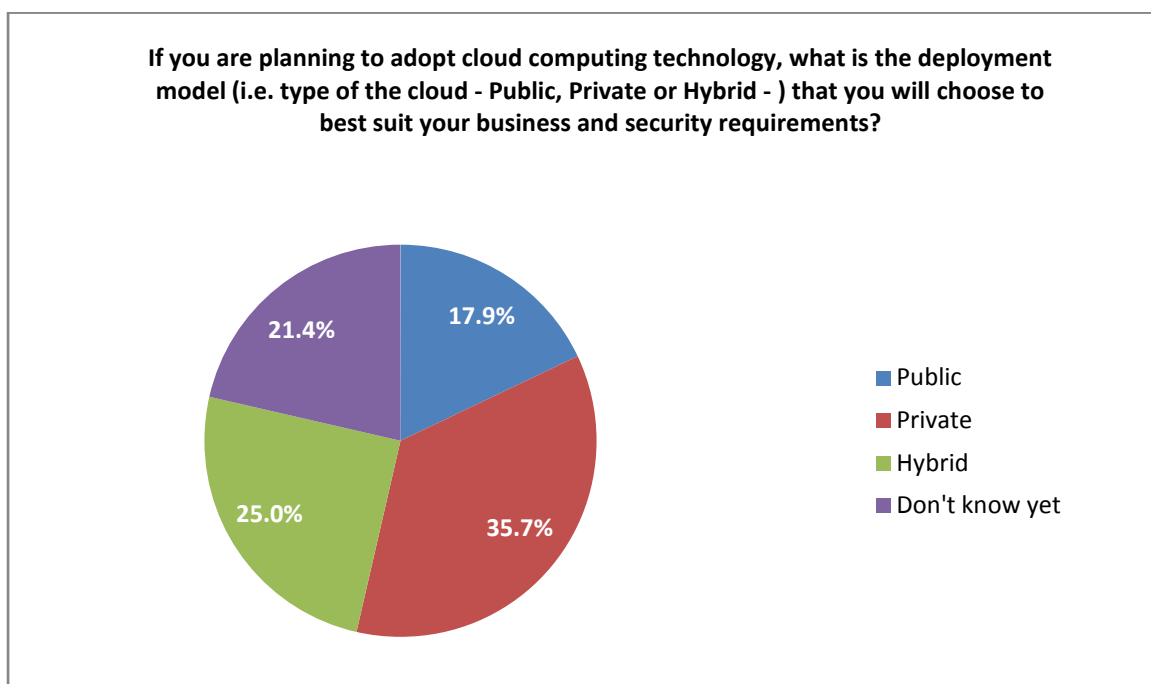


Fig.17. Non-adopters' plan towards selecting type of cloud.

It is important to understand the factors that could affect the adoption of cloud computing and also the constraints behind their lack of adoption. As shown in Figure 18, 57% of respondents acknowledged “ubiquitous network access” as the highest factor that could motivate customers to migrate to the cloud, followed by 54% for both cost reduction and flexibility of resources. Elimination of the operational burden has been ranked third amongst the factors at 45%. The reliability of the cloud service providers based on redundancy received 43%. The three factors that received the lowest percentages were for the elimination of the up-front investment (31%), the ability to pay for the use of computing resources on a short-term basis (20%) and tools for selecting cloud service provider (11%). Despite our aim to investigate whether such tools of transparency will help potential customers to migrate to the cloud, the lowest score was given to this factor. It is worth investigating whether those who have been encouraged to adopt cloud computing, or who have already adopted it, consider such tools to have helped them. As this questions forms a part of our study, this subject will be explored later in Chapter 6.

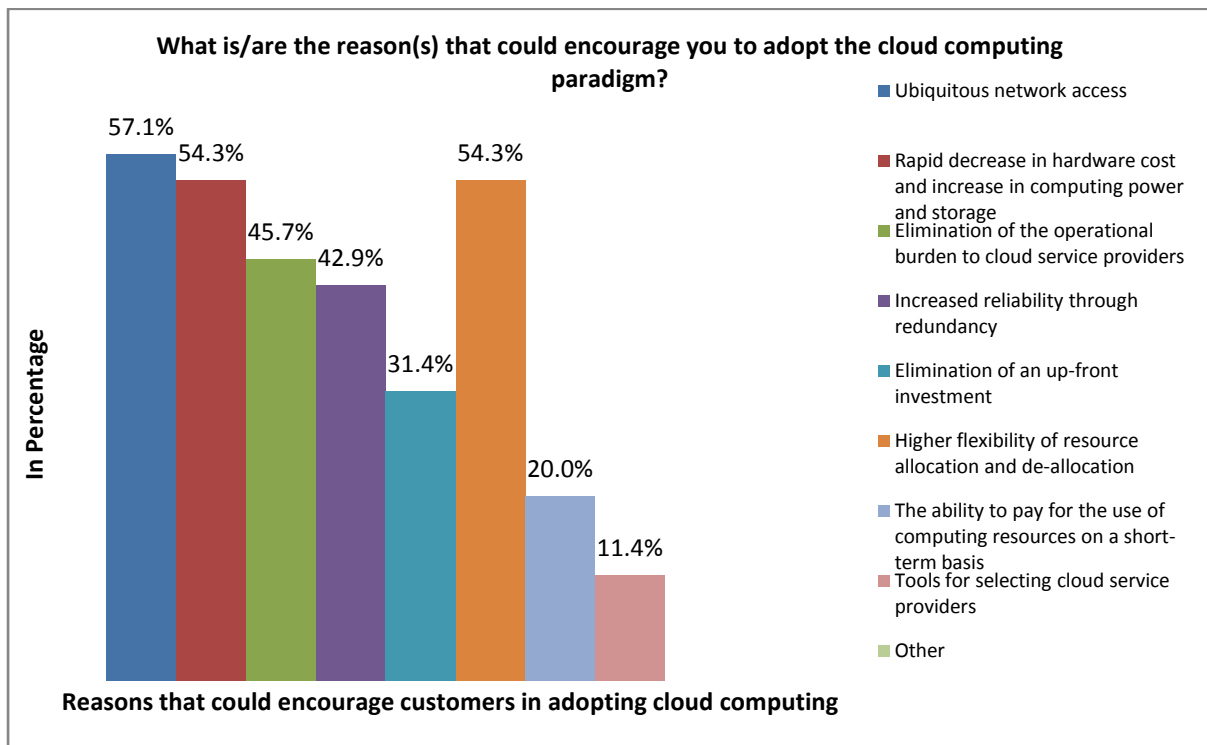


Fig.18. Factors encouraging cloud computing adoption.

Previously we presented the results of the respondents with respect to factors that could encourage migration to the cloud. The following Figure presents the respondents' results, with regards to their selection of the factors that are likely to inhibit their organisations from adopting cloud computing. The security issue has been the most influential factor (68.6%) that respondents indicated would affect adoption of cloud computing. This is consistent with the findings of several studies conducted by [100] that security remains the highest factor affecting adoption of cloud computing. Legal issues have been ranked secondly with 57.1% and this figure coincides with that of another study [100]. This is followed by data confidentiality and auditability factors which received 54.3% of the responses. The lack of transparency has received good feedback from the respondents, at about 46%, which also supports the literature. About 43% of the respondents reported the lack of clarity on the liabilities on service level agreements as having been an issue when migrating to the cloud. Respondents cited the fear of data lock-in (31.4%), lack of control over IT assets (25.7%) and malicious insiders (25.7%) respectively. The lowest three barriers to cloud computing adoption, with respect to the respondents, were the lack of compliance of cloud service providers (22.9%), business continuity and availability (14.3%), and isolation failure (11.4%). There is another factor that has been found interesting to mention representing, accounting for 5.7% of the responses. It includes the lack of full data control, and a given example is the deletion of a file from all hosting servers.

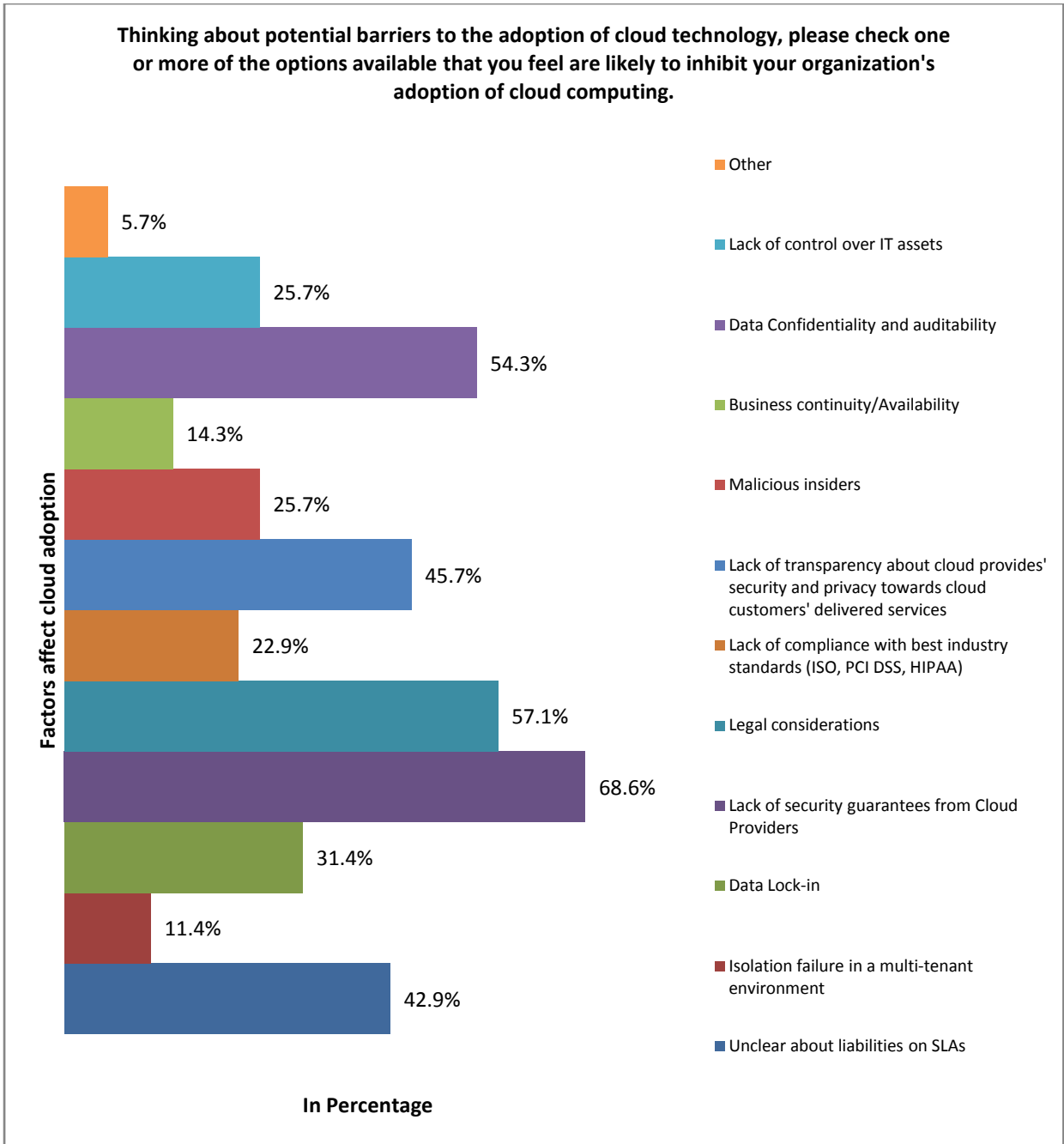


Fig.19. Factors affecting the adoption of cloud computing.

### 5.3.4 Non-adopters – a Comparison between sectors

We have presented the results of the non-adopters in general. In this section we compare the results on a sector basis, in order to further understand the reasons behind respondents' non-adoption. First of all, we will look at the average rating for the sectors' willingness to adopt cloud computing technology. Figure 20 shows the likelihood of each sector's adoption of cloud computing. The telecommunication sector has a full score of five, despite the limited number of responses that were received from this sector. The governmental sector is ranked secondly with a score of 3.73, closely followed by the education sector 3.25. Scoring below 3 is the IT sector, which received a score of 2.67. The least amongst others is the banking sector, which has received an average rating score of 2; this could be due to the sensitive nature of the data that banks hosts.

Overall, the average rating score of all sectors is 3.33, which represents a good percentage about 67% of the respondents being likely to adopt cloud computing. We asked the respondents to leave feedback if they answered "less likely" or "never", in order to know their reasons for not adopting the cloud. They all expressed security as a major issue in adopting cloud computing with the exception of the banking sectors where regulatory reasons are the main issue for them.

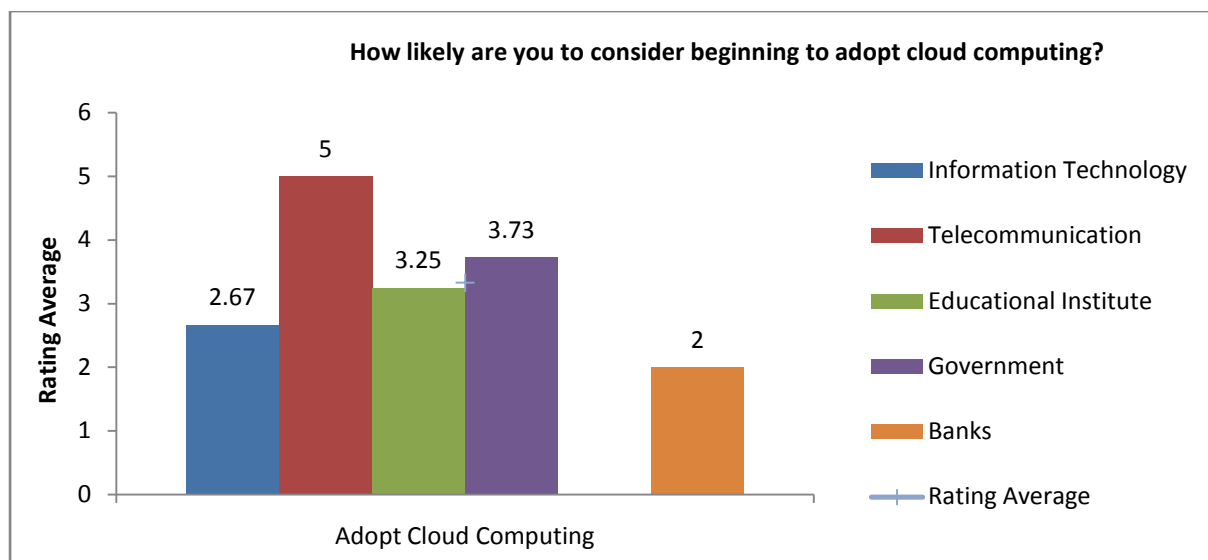


Fig.20. Sectors' likelihood of adopting cloud computing.

Figure 21 shows us that the favourite deployment model for the sectors in general is the private cloud, achieving 37% of the responses; the hybrid cloud comes second with 22.2% and the same percentage respondents from various sectors have not yet decided which deployment model they would select. This reluctance could be due to several reasons, such as the lack of control over IT assets, legal considerations and security issues. The least popular deployment model is the public cloud, receiving only 18.5% of respondents. With regards to the selection of the public cloud, the governmental sector figure accounts for 40% of the responses, followed by information technology, education and the banking sector, all of which receive equivalent percentages of 20%. The respondents' selection of the private cloud is categorised as follows: the governmental sector shares the same percentage of the public cloud percentage (40%), the responses from the IT sector shows more interest in the private cloud than the public and it is greater by 20%. Respondents from education sector have shown interest in both private and public clouds, sharing the same figure of 20%; this is 47% higher than for the hybrid cloud. The governmental sector has shown less interest in the hybrid cloud, compared to the public and private cloud, which has decreased by 20%. About 22.2% of the respondents did not indicate what type of cloud solution they would choose to adopt.

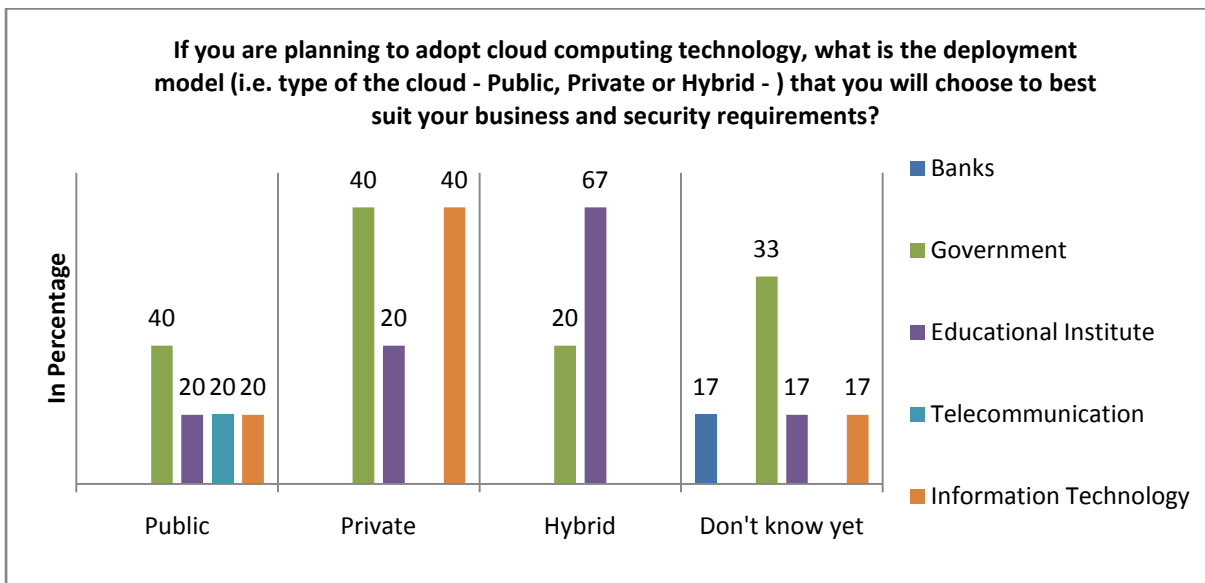


Fig.21. Sectors' adoption plan for selecting the type of cloud



Figure 22 shows that the majority of respondents have selected three main drivers for cloud computing adoption: ease of accessibility (59.4%), cost savings (56.3%), and flexibility in the provision of scalable resources (50%). These results are to some extent similar to another study conducted by KPMG in 2010, which indicated that scalability and cost reduction were the main drivers that encourage adoption of cloud computing [100]. As indicated in Figure 22, the remaining percentages of other factors from respondents are: the elimination of the operational burden and the increased reliability through redundancy (43.8%), elimination of an up-front investment (31.3%) and paying for the computing resources based on short-term basis (18.8%). The tools for selecting the right cloud service provider do not appear to be a main factor in cloud computing adoption (9.4%).

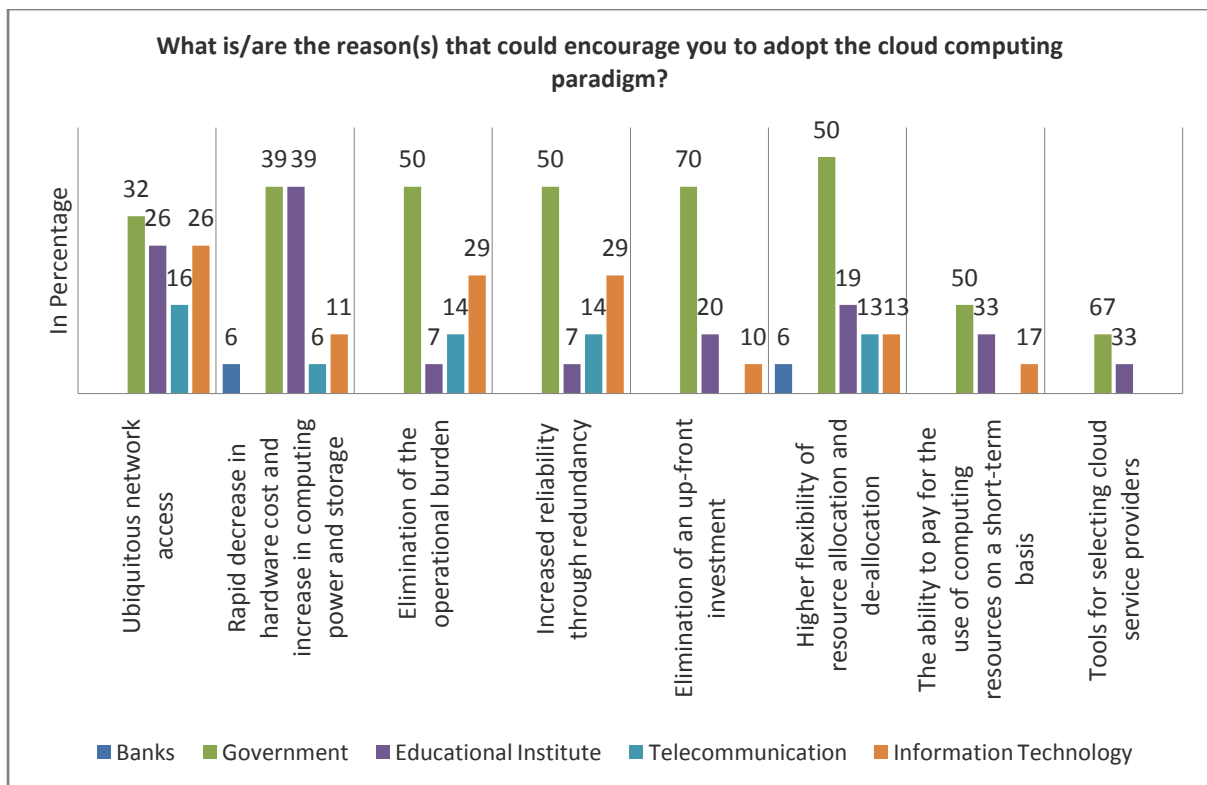


Fig.22. Sectors' encouragement factors for adopting the cloud.

The governmental sector has seen almost all of the factors provided in the survey as major drivers to their adopting the cloud. Only two factors do not appear to be attractive to this sector, which are the ability to pay for the computing resources in the short-term and the tools that help them to select cloud service providers. However, compared to the other sectors the respondents from the governmental sector received higher percentages on those two factors. The education sector sees the ease of accessibility and cost reduction as the main drivers for their adoption. In spite of the wide range of factors that are presented to the respondents in the survey, two factors appear to have attracted the banking sector to consider migrating to the cloud: the rapid decrease in hardware cost, and the higher flexibility of resource allocation and de-allocation. Unfortunately the healthcare sector was not represented among the responses received. Respondents within the IT sector suggest that the elimination of the operational burden and the reliability based on redundancy are the main drivers, followed closely by the ease of accessibility that cloud computing provides.

The respondents were offered several factors that might be considered as potential barriers for customers when adopting cloud computing. They are presented in Figure 23. These include the lack of clarity of liabilities in SLAs, isolation failure in a multi-tenant environment, data lock-in, lack of security guarantees from cloud service providers, legal considerations, lack of transparency from cloud service providers, malicious insiders, business continuity, data confidentiality and auditability and lack of controls over IT assets. The response percentage received in each factor for combined sectors is as follows: the top main factors are the lack of security guarantees (68.8%), followed by legal considerations and data confidentiality and auditability (56.3%).

The lack of transparency, which this thesis considers to be an important research problem, scored a considerable number of responses from the sectors. 40.6% of the responses have been given to the lack of transparency; the lack of clarity factor also shared 40.6% of responses. This could suggest that the lack of transparency could lead to another complication for the customer in the form of unknown liabilities. Datalock-in has been rated as one of the cloud computing risks identified by 34.4% of the respondents. The lack of compliance, control over IT assets and malicious insiders gained the same attention across all sectors with 25%. The two factors with the lowest proportion of respondents are isolation failure and business continuity, receiving 12.5% and 15.6% respectively. Despite the fact that isolation failure is considered as one of the top security risks in cloud computing, it has been

emphasised that attacks on resource sharing are very difficult to achieve and rarely occurs [27].

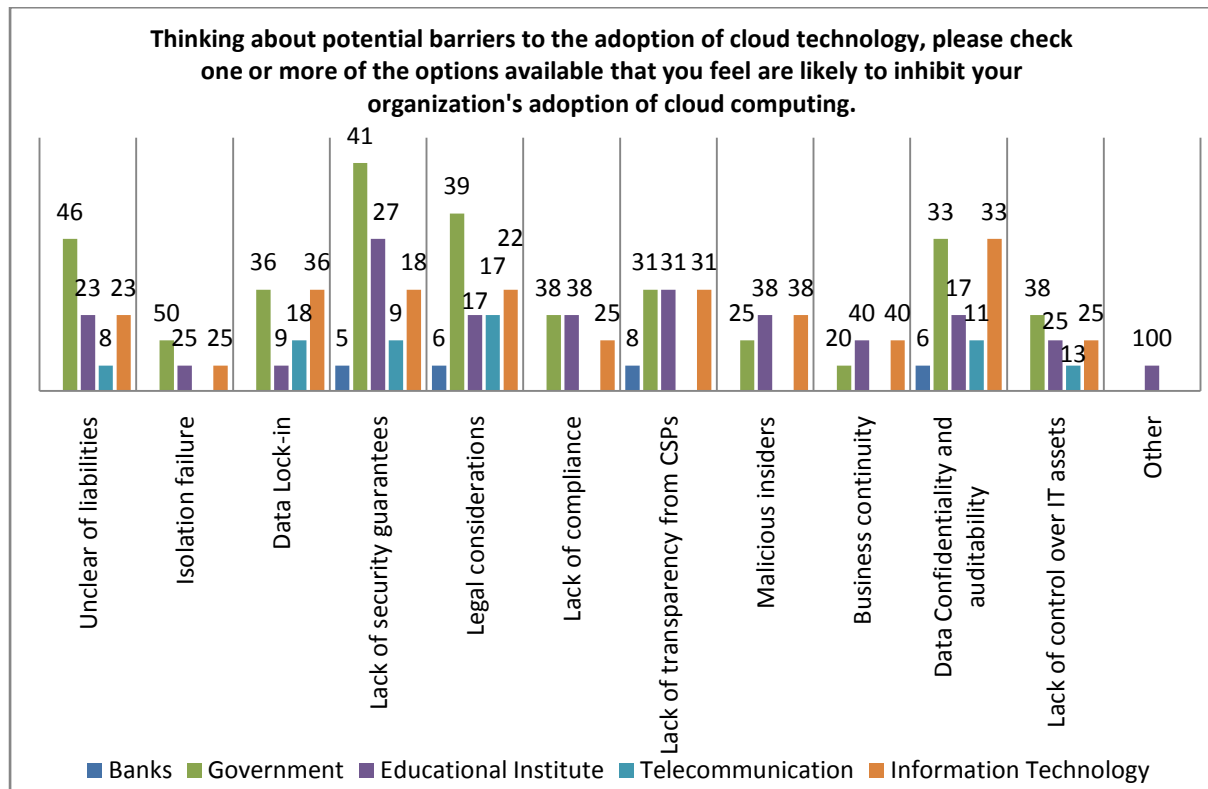


Fig.23. Sectors adoption barriers.

Table 15 ranks each sector based on the selection of the potential barriers from the set provided in the survey. After this, the main factors that were considered to be a major issue for the sectors are highlighted.

Table 15. Ranking Sectors Based on their Selection of the Cloud Adoption Barriers

Factors	Sectors Ranking				
	1	2	3	4	5
<b>Unclear about liabilities on SLAs</b>	Government	Education & IT	Telecommunication	.	
<b>Isolation failure</b>	Government	Education & IT			
<b>Data Lock-in</b>	Government & IT	Telecommunication	Education		
<b>Lack of security guarantees</b>	Government	Education	IT	Telecommunication	Banks
<b>Legal considerations</b>	Government	IT.	Education & Telecommunication		Banks
<b>Lack of compliance</b>	Government & Education	IT.			
<b>Lack of transparency</b>	Government, Education & IT	Banks			
<b>Malicious insiders</b>	Education & IT.	Government			
<b>Business continuity</b>	Education & IT.	Government			
<b>Data confidentiality</b>	Government & IT.	Education	Telecommunication	Banks	
<b>Lack of control over IT assets</b>	Government	Education & IT.	Telecommunication		

It can be observed from the above Table that the government sector is ranked first in almost all of the factors, with the exception of the fear of malicious insiders and business continuity. These are considered to be secondary in cloud adoption concerns. The government sector selected the main barriers for their adoption of cloud computing as being the lack of clarity over liabilities (46%), lack of security guarantees (41%), legal considerations (39%), data lock-in (36%), data confidentiality (33%) and lack of transparency (31%). Respondents from the education sector chose business continuity (40%) and both the lack of compliance and malicious insiders (38%) as the main inhibiting factors when deciding to migrate to the cloud. Out of eleven factors, the IT sector selected five main constraints to their adoption of cloud computing. The constraints are: business continuity (40%), malicious insiders (38%), data lock-in (36%), data confidentiality (33%) and the lack of transparency offered by the providers (31%). According to the results obtained from survey, based on this question, the main considerations for the telecommunication sector is data lock-in (18%), followed closely by the legal issues (17%). With respect to the banking sector, the lack of transparency (8% compared to other sectors) given by the providers appears to be a major issue when considering adopting cloud solutions. Other factors, such as data confidentiality, legal considerations and the lack of security guarantees have the least impact on cloud computing adoption, with each receiving 6%.

## 5.4 Conclusion

The aim of the survey was to gather information from participants (IT, education, government, telecommunication, healthcare and banks) in order to understand their cloud computing adoption constraints and drivers. The second part of the survey (the results and conclusions are presented in Chapter 6) aimed to assess tools of transparency (e.g., CSA STAR registry, CTP and CloudeAssurance) in terms of its usage, usefulness and future usage for searching and selecting the right cloud service provider. The tools that have been chosen are the CSA STAR registry, CTP and the CloudeAssurance as they provide best industry standards for potential cloud computing customers. In this section, we draw our conclusions by highlighting the important findings of the survey questionnaire results.

The delivery model SaaS is still the dominant model, according to our results. This result is also supported by the literature found in [35, 42, 84]

Most of the respondents have selected the private cloud as their deployment model. This can be justified due to the data and applications that the respondents' organisations hold. The findings have also shown that the respondents are almost equal in their selection of single and multi-providers; the average rate of the respondents' selection has shown that multiple-cloud providers are better when comparing between the three types of clouds and in terms of the respondents' selection of the number of providers. Most of the respondents preferred to choose a single cloud provider when they are planning to choose private cloud, and selecting multiple cloud providers is better for the respondents who are planning to use a public or hybrid cloud. This is because public cloud is most likely to be vulnerable to technical and business risks, such as outages and service failures. The most encouraging factors that pushed the respondents towards adopting cloud computing were related to cost reduction, increased reliability and ubiquitous network access.

We conducted a comparison between the sectors in terms of their selection of the type of delivery services (i.e., IaaS, PaaS and SaaS). Among our respondents, IaaS is the dominant model in the banking sector; the SaaS model is mostly preferred in education, IT and governmental sectors; the PaaS model is most convenient for telecommunication companies. The healthcare sector mostly selected PaaS and SaaS. Among the responses, the private cloud is the most selected deployment model across all sectors because of the nature of the data. The IT sector is the top adopter for each of the deployment models (private, public and hybrid). Education comes next, but this sector is seen to be interested in public and hybrid

cloud more than private deployment. The adoption of cloud computing is likely to be less in governments, telecommunications and banks than other sectors, as is shown in the survey sample. Selection of the number of cloud providers differs from sector to sector. IT and telecommunication enterprises prefer using multiple providers rather than a single cloud provider. On the other hand, most of the respondents from within education and healthcare have used a single cloud provider more than multiple providers. Some of the respondents from governments and banks were attracted to both single and multiple providers' offerings.

From the point of view of non-adopters, Telecommunication is the domain with the largest proportion of likely adopters, followed by government and education, then the IT and banking sectors. Only a few have not shown any interest in adopting cloud computing for several concerns, which include the lack of security guarantees, the lack of transparency towards delivered services to the customers and data confidentiality and auditability. The influential role of the respondents themselves could have been one of the factors that have led to the higher percentage of the respondents who likely to adopt cloud computing.

The private cloud is still the most selected deployment model among both respondents who have and have not adopted cloud solutions. The IT and governmental sectors prefer private cloud and the education sector sees the hybrid cloud as best choice for them to adopt. Respondents from the telecommunications sector have chosen the public cloud model. There are several factors that discourage respondents from adopting cloud computing. These factors are the lack of security guarantees, legal considerations and data confidentiality and auditability. Those are the most common factors that affect the adoption of cloud computing for almost all of the sectors in the response set. The government sector respondents selected the lack of clarity of liabilities, lack of security guarantees and legal considerations as the main barriers to their adoption of cloud computing. The education sector chose business continuity and lack of compliance as the main inhibiting factors to adoption. The IT sector selected five major factors, which in their opinion, affected their adoption of cloud computing. These are business continuity, malicious insiders, data lock-in, data confidentiality and the lack of transparency. Respondents from the telecommunications domain were concerned with data lock-in and legal issues. Responses from the banking sector have supported our claim that the lack of transparency is the major issue in cloud computing adoption. That is true only from the point of view of one sector as the IT sector considers it as a barrier but not their ultimate one.

Factors such as broad network access, cost reduction and flexibility of resource allocation and de-allocation have also been drivers for respondents who wish to adopt cloud computing. Respondents from the education sector considered the ease of accessibility and cost reduction as main motivations for their adoption. The banking sector's respondents were attracted by the benefits of cost reduction and the higher flexibility of allocation and de-allocation. With respect to the IT sector, the elimination of the operational burden and the reliability based on redundancy were reported as main drivers. When designing the survey questionnaire, it has been assumed that "tools for selecting cloud service providers" would be a major factor in helping respondents to adopt cloud computing. However, the results have suggested that, for most of the respondents, this factor is not significantly important. Only two sectors (government and education) reported that a tool for selecting cloud providers is an important factor.

## **Chapter 6: Assessment of Tools' Usefulness – Survey Results**

### **6.1 Introduction**

This is the second part of the survey questionnaire, which aims to assess the helpfulness of tools, such as CSA STAR, CTP and CloudeAssurance, in terms of their usage when searching for the right cloud provider and whether they will be used in the future. This chapter discusses the results of the tools' assessment in general in Section 6.2. The results from the point of view of non-adopters are explained in Section 6.3, Section 6.4 presents the adopters' point of view of the tools and Section 6.5 presents a summary and the main findings.

### **6.2 Assessment of Tools' In General**

Figure 23 shows cloud customers' responses to the question seeking their opinion on the usefulness of the tools in evaluating providers' transparency and whether they will help them adopt cloud computing technology. Around 72% of the responses acknowledged the usefulness of having a tool, while approximately 17% said they did not know if such tools would encourage them to migrate to the cloud, or evaluate cloud providers' transparency. The remainder did not rely on these tools to migrate to the cloud. While some respondents' comments about these tools are available, due to the space limitation, we can highlight only most common feedback which is: "It would be nice if I trusted the tool, but probably I wouldn't be convinced the tool gives 100% trustworthy results".



**Q14 Do you think having a tool for evaluating the transparency of the cloud providers is important and it will encourage you to migrate to the cloud?**

Answered: 87 Skipped: 10

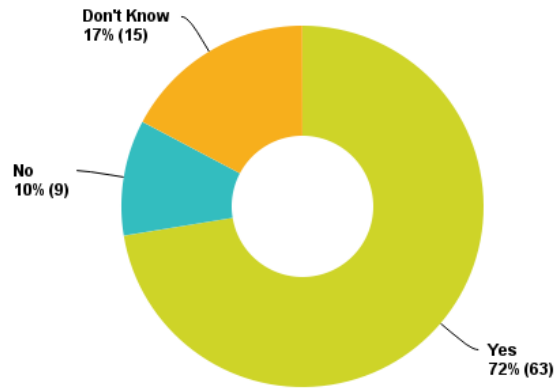


Fig.24. Respondents' opinion on evaluating cloud providers' transparency.

Navigating through the survey questionnaire, several questions related to the usage of existing tools in the market. Figure25 shows a considerable number of respondents who have used one of the three tools covered by this survey (CSA STAR, CTP and CloudeAssurance). In fact, the rest, who represent over two third of the responses, might have used different tools other than these three.

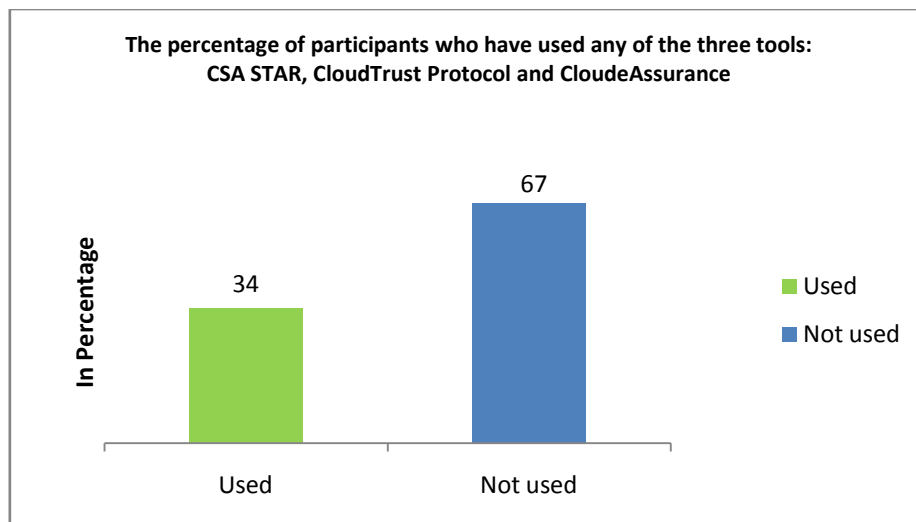


Fig.25. The percentage of using one of the transparency tools.

Figure 26 shows the results for the first question, which is related to the usage of CSA STAR registry. Most of the participants had not used the CSA STAR. On the other hand, about 14.1% of the participants had used it.

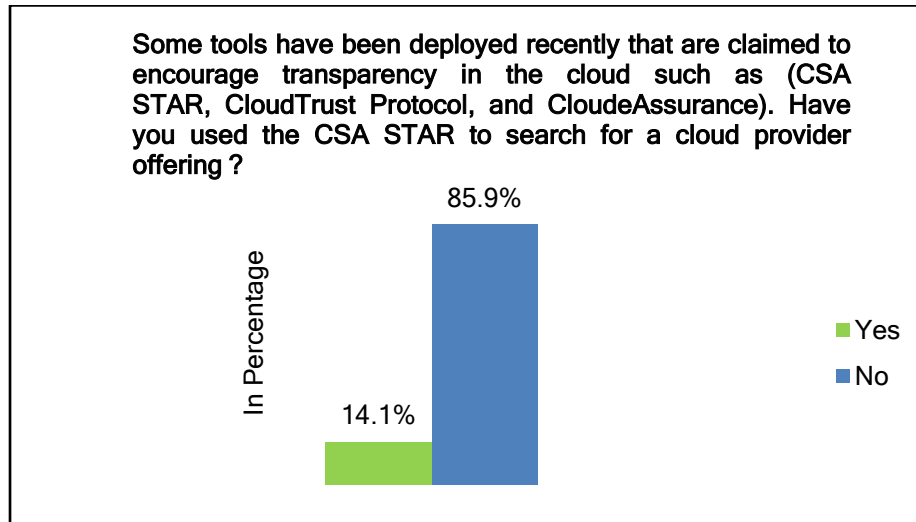


Fig.26. CSA STAR usage percentage.

Figure 27 shows the usefulness of the CSA STAR registry for the participants who had used it. 25% of respondents stated that the CSA STAR was a significant help in adopting cloud computing solutions, provided by the cloud providers. Half of the respondents have chosen the category “helpful” when rating the tool. In contrast, one of the participants expressed his opinion that CSA STAR did not help them greatly, due to some difficulties in comparing the cloud computing offering provided by the cloud providers in the CSA STAR registry. One of the respondents did not express any opinion about the CSA STAR. From another point of view, one of the respondents stated that it was not helpful at all, without mentioning any reasons. The results suggest that the usage of the CSA STAR tool and its usefulness is not significant. This can be related to the customers’ assurance requirements, stated previously in Chapter 2, whereby the CSA STAR has not fulfilled almost all of the requirements.

**Q17 How helpful did you find the CSA STAR in encouraging you to use cloud computing solutions?**

Answered: 12 Skipped: 85

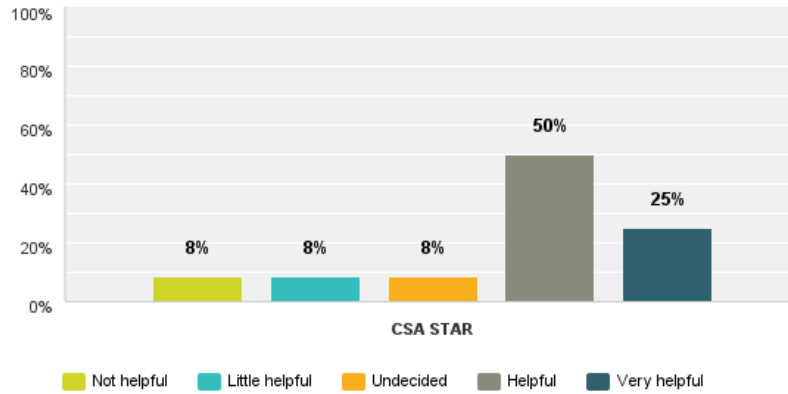


Fig.27. CSA STAR usefulness.

With regards to the CTP usage percentage, Figure 28 shows that the majority of the respondents had not used it. One of the given reasons was that they were not familiar with the tool. Yet, 15.4% of those had used the tool, which represents the highest percentage of the three tools.

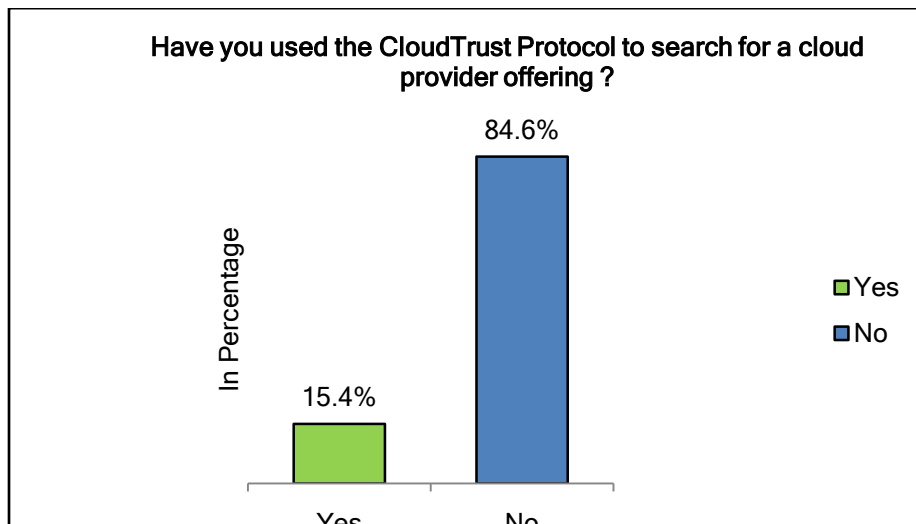


Fig.28. CTP usage percentage.

Figure 29 shows a wide range of opinions with regards to the usefulness of the CTP. Seven of the respondents agreed on the usefulness of the CTP, while only one of the respondents stated that the tool was not helpful, without giving any reason that could help in the analysis of the usefulness. The rest (about one third) choose not to decide. It seems that the CTP is more popular (in terms of usage) than the other tools named in the questionnaire. This could prove the importance of fulfilling the customer’s assurance requirements as the CTP meets five out of six requirements that were discussed before transparency measurement, trustworthy measurement, support of evidence, keeping evidence up-to-date and the adoption of best industry standards. This might reflect the potential cloud customers’ interest in achieving these requirements.

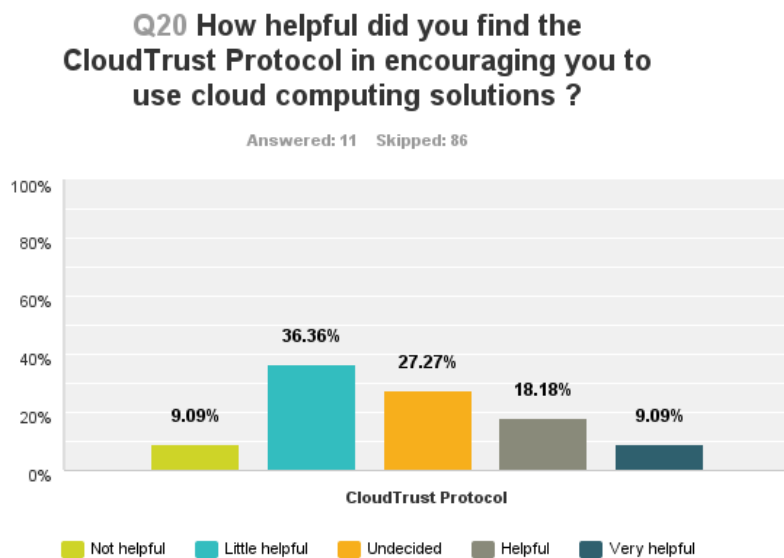


Fig.29. CTP usefulness percentage.

Finally, in the assessment of the CloudeAssurance usage and usefulness in evaluating the cloud provider’s transparency, Figure 29 shows that 86% of the respondents had not used the CloudeAssurance. CloudeAssurance and CTP have exactly the same usage percentage. The reason for this limited usage could be that they are commercial tools that you have to pay for. Moreover, some of the respondents from the government sector stated that they are using the G-Cloud [99] framework, which is dedicated to the U.K.’s government sector. Another reason that has been drawn from the survey is that some have said they are not familiar with the CloudeAssurance.

### Q22 Have you used the CloudeAssurance to search for a cloud provider offering?

Answered: 78 Skipped: 19

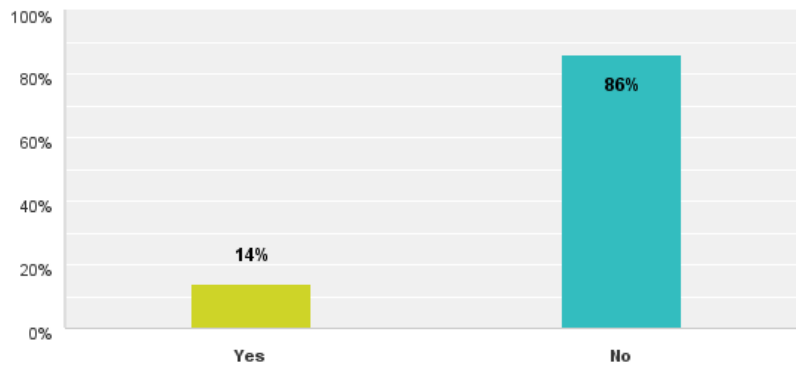


Fig.30. CloudeAssurance usage percentage.

With regards to the assessment of usefulness, Figure 31 shows that all respondents expressed their opinion on its usefulness. 60% of the respondents said the tool was helpful in assessing the cloud providers and providing a clear scoring scheme. With regards to other participants, they share the benefits of the tool but they differed in opinion as to the degree or level of helpfulness. As the CloudeAssurance is distinguished by having the rating feature, which cannot be found in other tools yet, this could explain its obtaining the highest results for usefulness tool in this questionnaire.

### Q23 How helpful did you find the CloudeAssurance in encouraging you to use cloud computing solutions?

Answered: 11 Skipped: 86

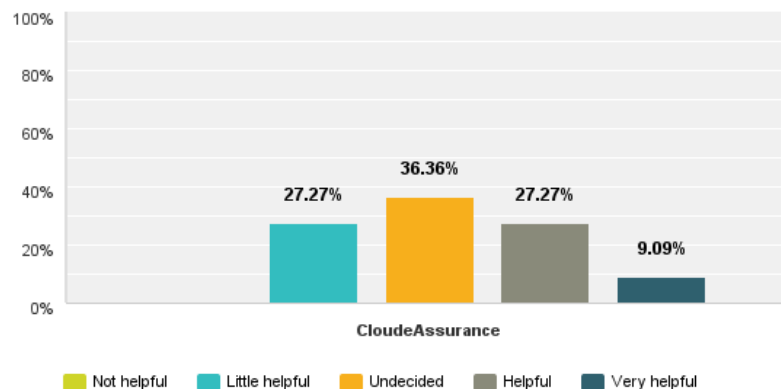


Fig.31. CloudeAssurance usefulness percentage.

### **6.3 Non-Adopters Views on the Tools' Usefulness**

This section presents the results of the respondents who are not adopting cloud computing. The objective is to know whether such tools of transparency have or have not helped various sectors in migrating to the cloud, evaluating the transparency of cloud service providers, assessing sectors' usage of the tools, and whether they will use it in the future to search for a cloud service provider. We asked the respondents a question about having a tool for the purpose of evaluating cloud providers' transparency and whether this might encourage them to migrate to the cloud.

The results from the different sectors' point of view are presented in Figure 32. More than two thirds(65.6%) of the total respondents agreed on using the tools to evaluate cloud providers' transparency and they found them to be a very important step in moving to the cloud. Only a few (9.4%) of the respondents did not agree about using tools. The other quarter of the respondents did not know whether having a tool would help them to migrate to the cloud or not. We believe that there are several reasons that have a direct or indirect impact on the respondents' answers to this question. These are, specifically, the influential of their own role and the trustworthiness of the tools provided in the market.

50% of the respondents who answered, "Did not know" were not in influential roles within their organisation. The remaining 50% were reluctant to use the tools because, from the point of view of one technical consultant at a governmental sector, they already used the gCloud framework and, he added, that they would use the external tools available on the market depending on how their accreditors view the internal system of the tools. Another opinion, from a respondent in the government sector at CIO level, mentioned that the tools do not provide clear defined requirements to be viewed. Some of the respondents (an IT consultant and a manager from the IT and government sector) have not agreed on the importance of having tools for evaluating the cloud providers' transparency. They have, however, emphasised the importance of having cloud providers' transparency evaluated.

The governmental sector has agreed on the importance of using the tools for evaluating cloud providers' transparency (38%), followed by the education sector (33%), the IT sector (19%) and the telecommunication sector (10%). Two sectors have not agreed on using the tools. They are banks (33%) and IT (67%) that voted not to use the tools. Despite

the governmental sector's high degree of agreement to using the evaluation tools, the other 50% of them selected "Don't Know". In the light of these results, it can be suggested that the influential role of the respondent, trustworthiness of the tools and clear defined requirements are important factors to consider in the survey.

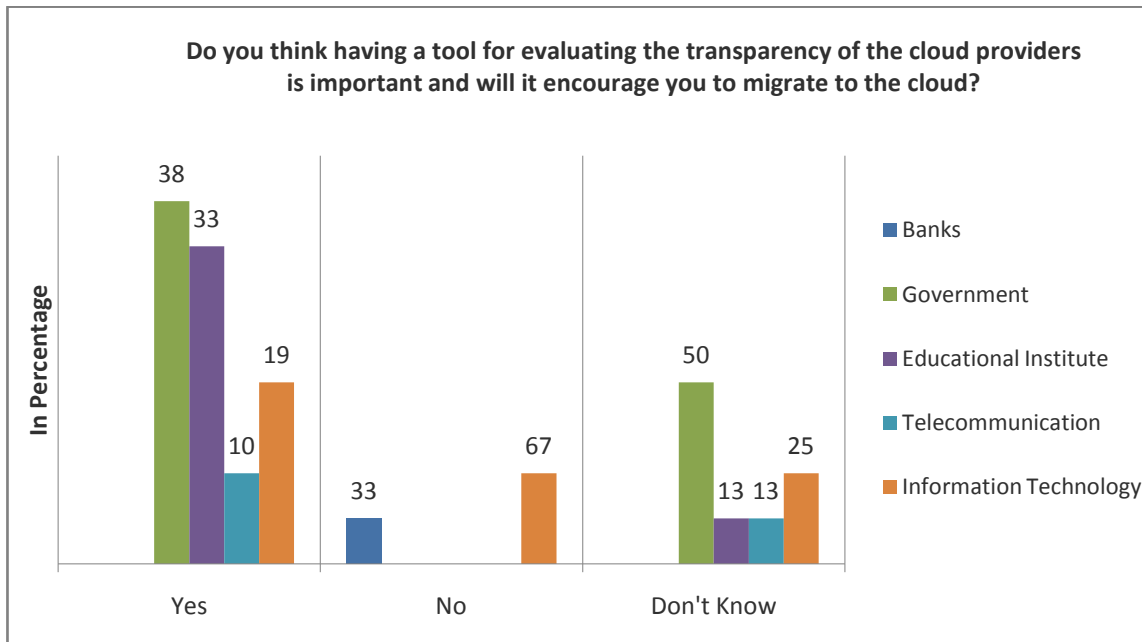


Fig.32. Sectors' opinion on using tools to evaluate providers' transparency.

The respondents' results for assessing the likelihood of using the tools for evaluating the cloud providers' transparency are presented in Figure 33. The education sector received the highest average rating of 4.13 representing 82.6%, closely followed by the government sector with an average of 4.0 receiving 80%, telecommunication companies scored 3.67 representing 73.4% and the information technology sector was 3.5 representing 70%. The overall average of the likelihood for using the tools across the different sectors is 3.90 representing a good percentage of approximately 78% who support the use of tools for the purpose of evaluating cloud providers' transparency.

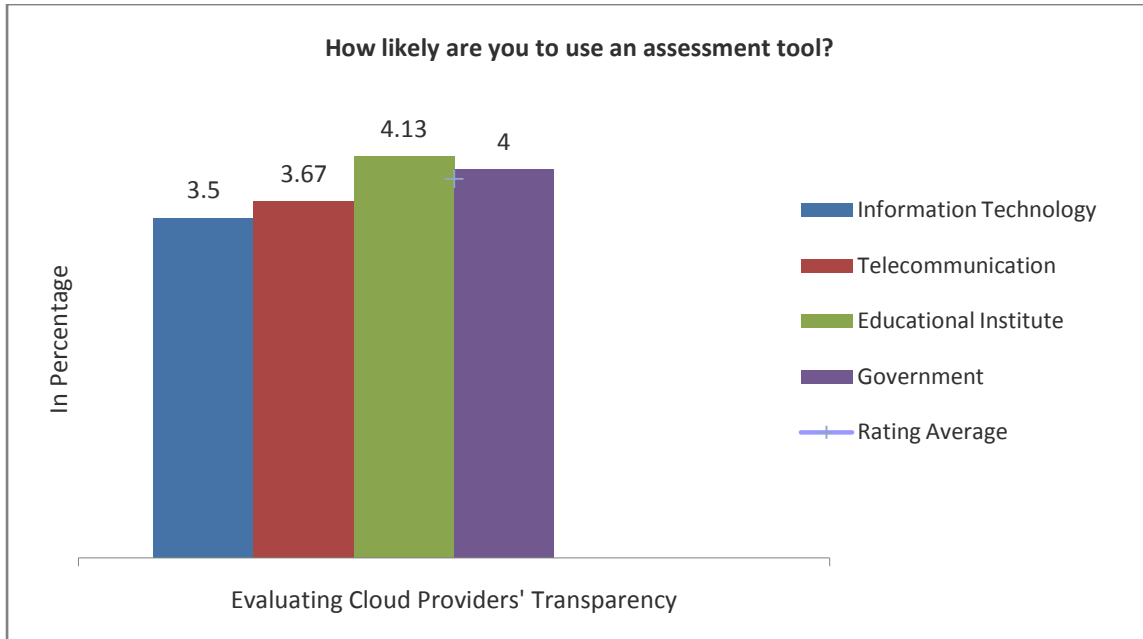


Fig.33. Sectors' likelihood of using the tools (non-adopters).

Previously in Section 6.4 we assessed the tools in general without mentioning further details about the sectors' opinions about them. Therefore, it is worth investigating whether the respondents from the different domain sectors (i.e., IT, governments, education, banks and healthcare) have, or have not, used these tools. Moreover, from the point of view of the non-adopters, we also need to know if such tools have or have not helped them to search for cloud providers and whether they will be using them in the near future.

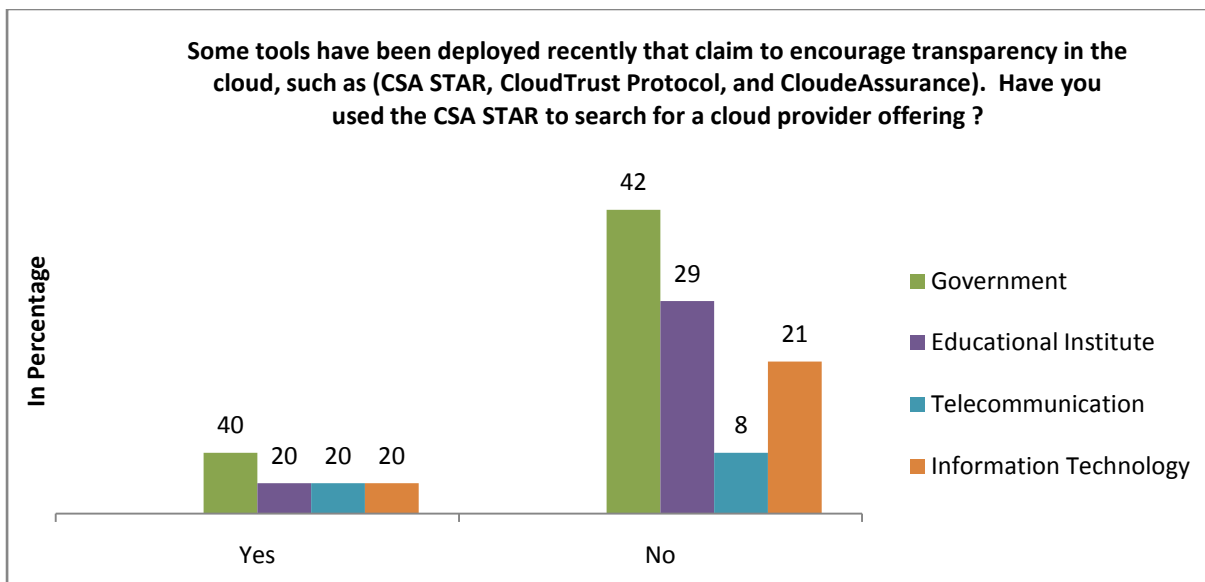


Fig.34. Sectors' usage percentage of CSA STAR.



From the non-adopters point of view, 17.2% of the respondents, from across the various sectors, have used the CSA STAR registry for the purpose of searching for a cloud provider offering. The remaining 82.8% of the responses from all sectors have shown no interest in using the tool. Out of those sectors that have used the CSA STAR registry, the leading sector in terms of the tool's usage is the government domain (40%) followed by the education sector, telecommunications and information technology, all of which received an equivalent percentage of 20%. The majority of the sectors that have not used CSA STAR are ranked as follows: Governments (42%) claiming that they are using the G-Cloud framework, and other reasons described previously in Figure 32, education (29%), information technology (21%) and telecommunications (8%).

Figure 35 presents the rating average for the usefulness of the CSA STAR registry among the sectors that have used it. One of the objectives of this survey is to investigate whether the tools of transparency have helped respondents in various sectors to make decision about using cloud computing solutions. The respondents' results, in terms of the usefulness of the CSA STAR, are as follows: The perceived usefulness was highest in the telecommunication sector, receiving an average rate of 4.0 out of 5.0 respondents (80%) saying that it was helpful. This was followed by the governmental sector, of which 70% stated that the CSA STAR was useful for them. In third place, the education sector rated the usefulness of the CSA STAR at 60% and respondents from the information technology sector stated that the CSA STAR has not been useful for them.

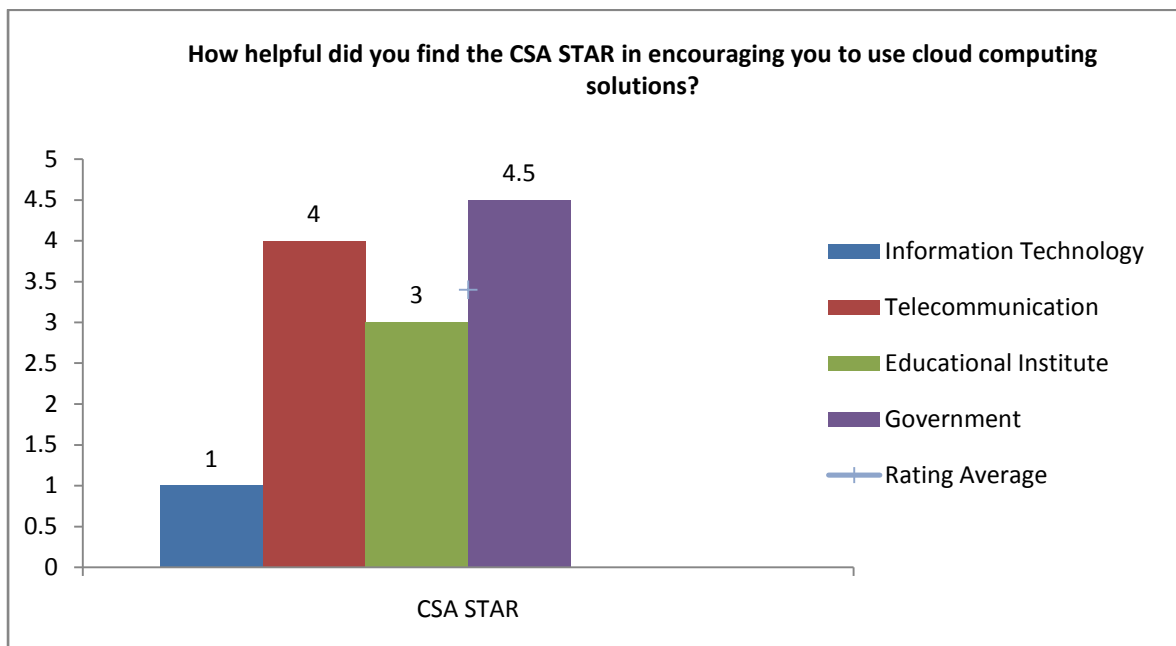


Fig.35. CSA STAR helpfulness for sectors (non-adopters).

We asked the respondents to state whether they would use the CSA STAR again in the future. Figure 36 presents their responses. 65.5% of the respondents, from across the different sectors, agreed that they would use the tool again in the future for the purpose of finding the appropriate cloud service provider. The remaining 34.5% voted “No” for CSA STAR usage in the future, which was due to several reasons. From the IT and educational perspective receiving (30% and 10% of responses) respectively, it was because of the respondents’ unfamiliarity with the tool. The governmental sector has many concerns, one of which is the lack of trust towards these tools and another is its dependency on using frameworks developed by the government such as the gCloud. Another reason is that they do not have enough information about the CSA STAR registry. The governmental domain is the highest among the other sectors, receiving 60% of the responses. The telecommunication sectors’ respondents received 10%, compared to other domains.

For those sectors who have agreed to use the CSA STAR registry, the education sector comes first with 42%, followed by the governmental sector(32%), IT (16%) and the last sector is telecommunications (11%), despite the fact that they were the top amongst others in assessing the usefulness of the CSA STAR registry. However, they only represent 33% of the responses received totally from the sector itself.

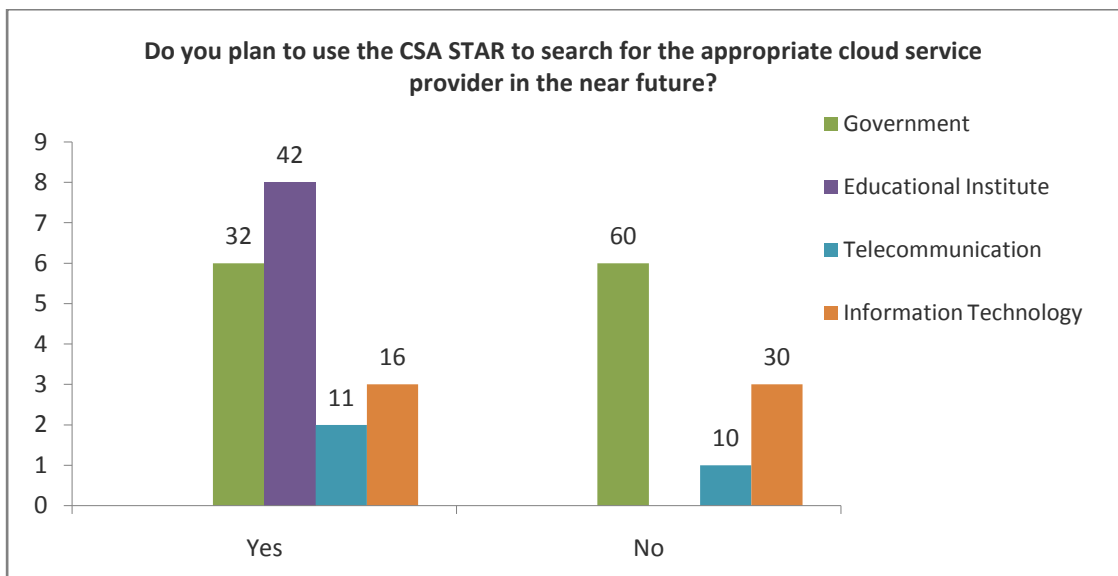


Fig.36. Sectors’ plan for using CSA STAR in the future (non-adopters).

The level of usage for the CTP between the sectors is presented in Figure 36. From the non-adopters' point of view, the percentage received for not using the CTP is 86.2% and 13.8% for those that have. The minority of those who have agreed to use the CTP all share the same percentages in terms of CTP's usage (25%). Both CTP and CSA STAR come in the exact order with minor differences in percentages. For example, the governmental sector has increased by 2% from the CSA STAR registry. Education and IT slightly decreased by 1%, so this indicated that both sectors prefer to use CTP rather than CSA STAR. The telecommunication sector has stable percentages in both CSA STAR and CTP.

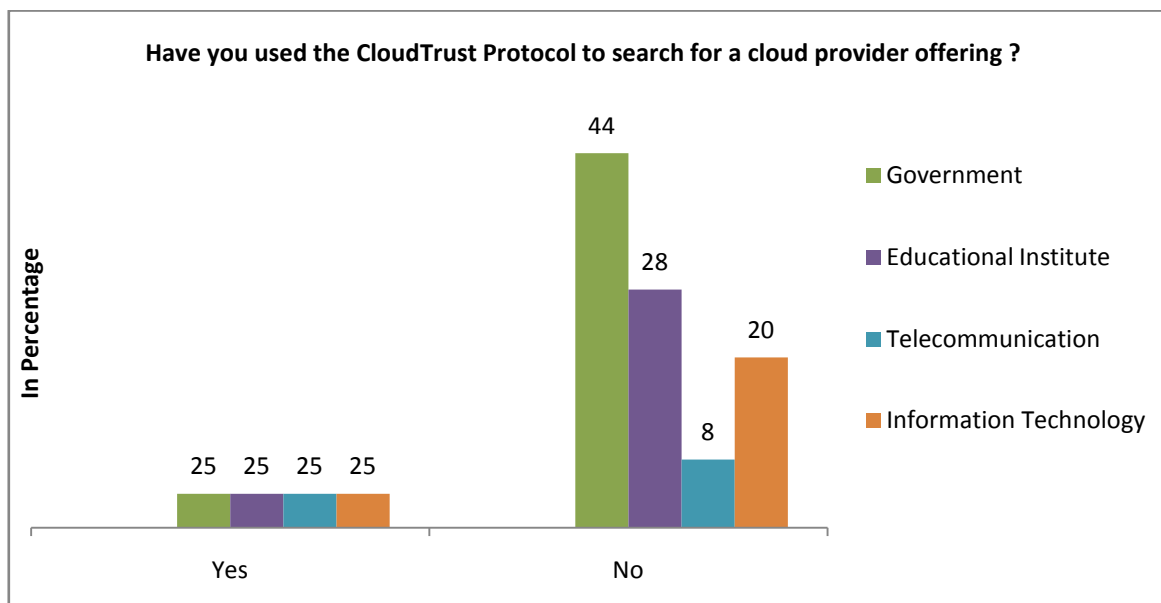


Fig.37. Sectors' usage percentage of CTP (non-adopters).

The CTP has been assessed by all sectors in terms of its usefulness towards making decisions about using cloud computing solutions. From the responses that have been received the CTP has scored 2.50 out of 5.0 (50% agree on its usefulness). Both the telecommunication and educational sectors share the same rating average regarding the helpfulness of the CTP compared to the CSA STAR. In terms of helpfulness, the governmental sector has decreased from the CSA STAR registry by 30% in terms of its helpfulness. The IT sector remains the least sector that expressed limitations on the helpfulness of both tools (CSA STAR and CTP).

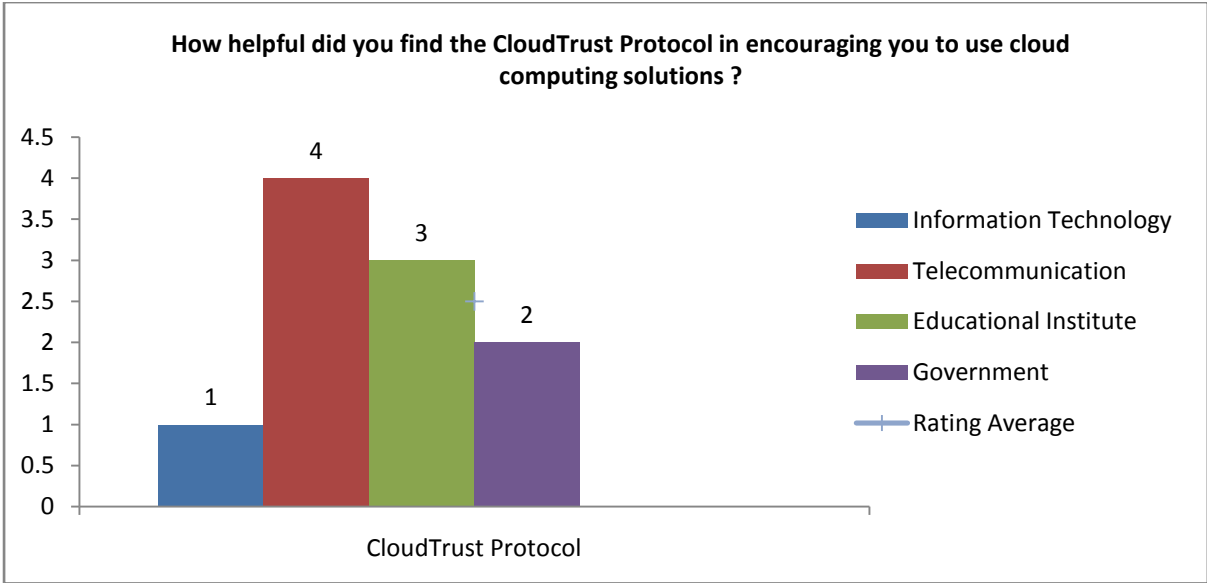


Fig.38. CTP helpfulness for sectors (non-adopters).

More than two thirds of the respondents selected to use the CTP in the near future and the remaining did not agree on using it again for several reasons.

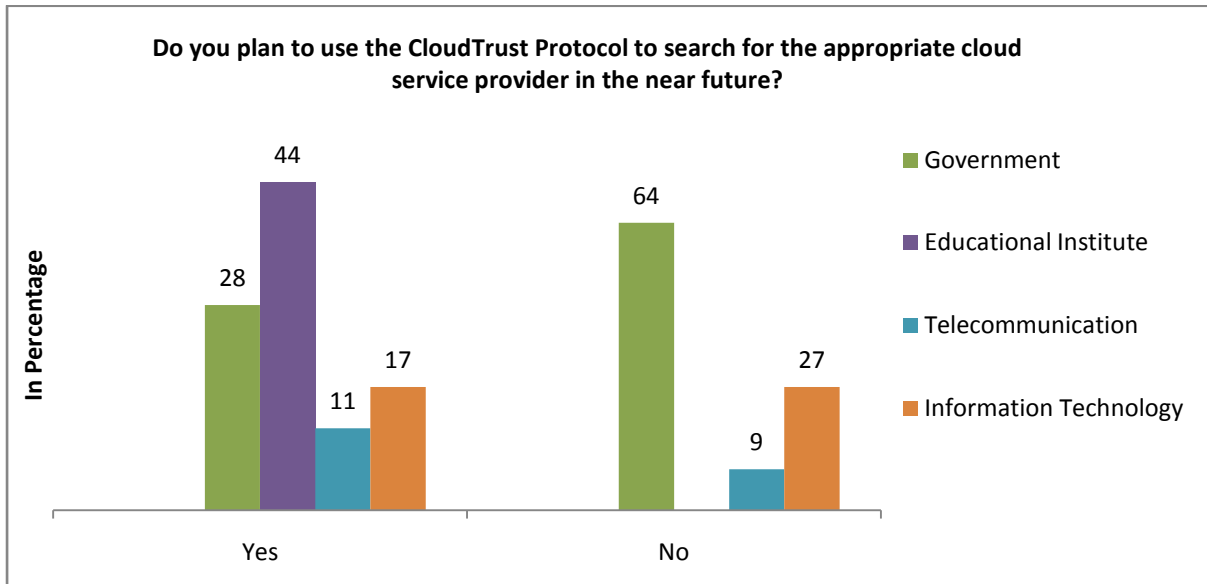


Fig.39. Sectors' plan for using CTP in the future (non-adopters).

From the IT, telecommunication and governmental perspective, the common reason for not using the CTP was because of unfamiliarity with the tool. The governmental sector has added several reasons that were previously illustrated in Figure 35, in relation to the future use of CSA STAR. Their reasoning is based on the way their accreditors will view the system and the fact that they have not started thinking about using cloud computing, therefore, they have not decided to look into the tools that encourage migration to the cloud, and the selection of a cloud service provider. The responses received from the sectors in the CTP have dropped slightly by 3% from the CSA STAR, in terms of using the tools in the near future.

The following Figure illustrates the respondents' results in terms of using the CloudeAssurance. Figure 40 shows that the CloudeAssurance is the least popular tool. Table 16 shows clearly the percentage of CloudeAssurance usage among different sectors. It has been used by only 10.3% of the respondents from the governmental and information technology sectors. 89.7% of the respondents, across the different domains, have not used the CloudeAssurance. In comparison to the sectors who have not used the CloudeAssurance, the top two sectors are government and education (38% and 31% respectively), followed by the IT domain (19%) and telecommunications (12%).

Table 16 CloudeAssurance Usage Percentage (Non-Adopters)

Have you used the CloudeAssurance to search for a cloud provider offering?								
Answer	What sector are you working in?						Response Percent	Response Count
	IT	Telecommunication	Education	Government	Healthcare	Banks		
Yes	1	0	0	2	0	0	10.3%	3
No	5	3	8	10	0	0	89.7%	26
<i>answered question</i>								<b>29</b>
<i>skipped question</i>								<b>3</b>

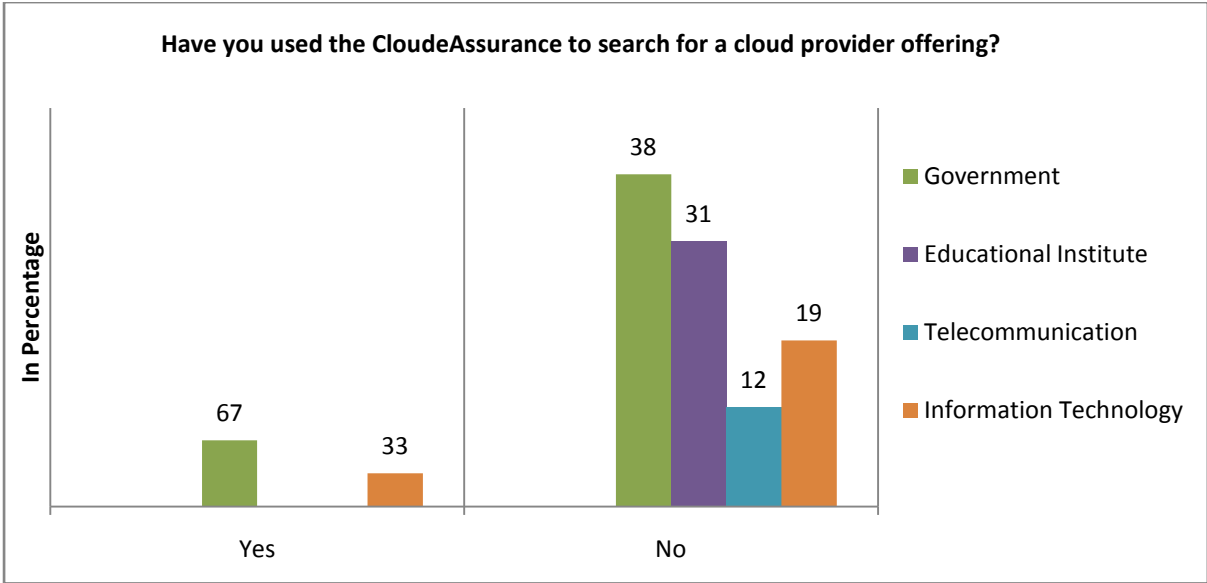


Fig.40. Sectors' usage percentage of CloudeAssurance (non-adopters).

With regards to the usefulness of the CloudeAssurance. For sectors that have not adopted the cloud but have used the tool, Figure 41 shows that the IT sector rated it most useful (with an average rate of 4.0/5.0), followed by the governmental sector (3.5/5.0). As one of the respondents from the government sector mentioned, their organisation is undecided whether it was helpful or not. The total average rate of its usefulness is 3.67/5.0, which is the best amongst the other tools. The CSA STAR is the second with 3.4/5.0 and the CTP is 2.5/5.0.

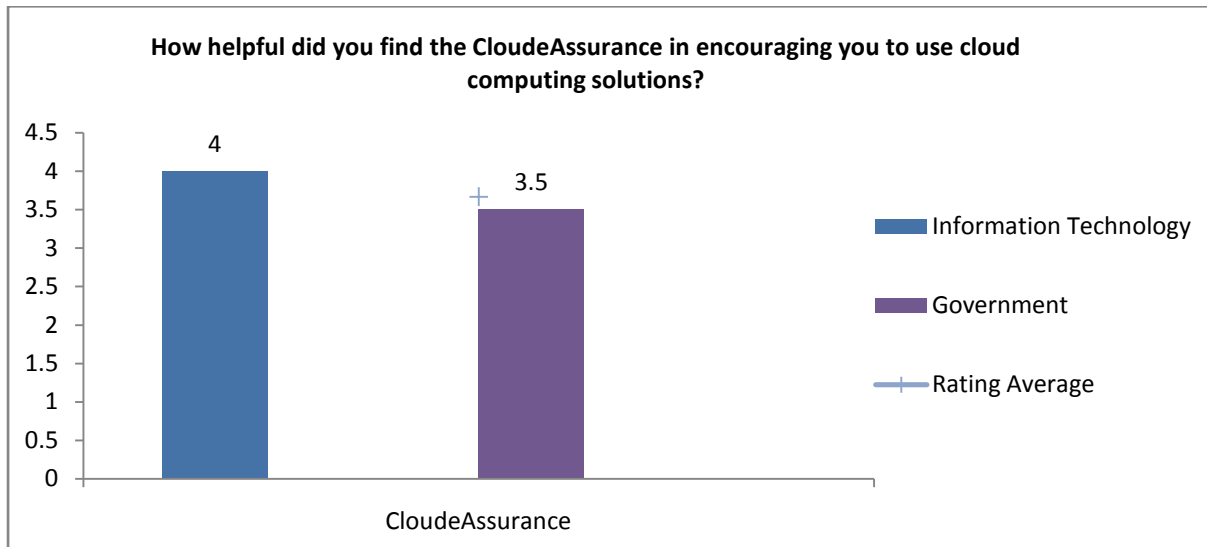


Fig. 41. CloudeAssurance helpfulness for sectors (non-adopters).

The following Figure assesses, to some extent, whether the respondents will use the CloudeAssurance in the near future.

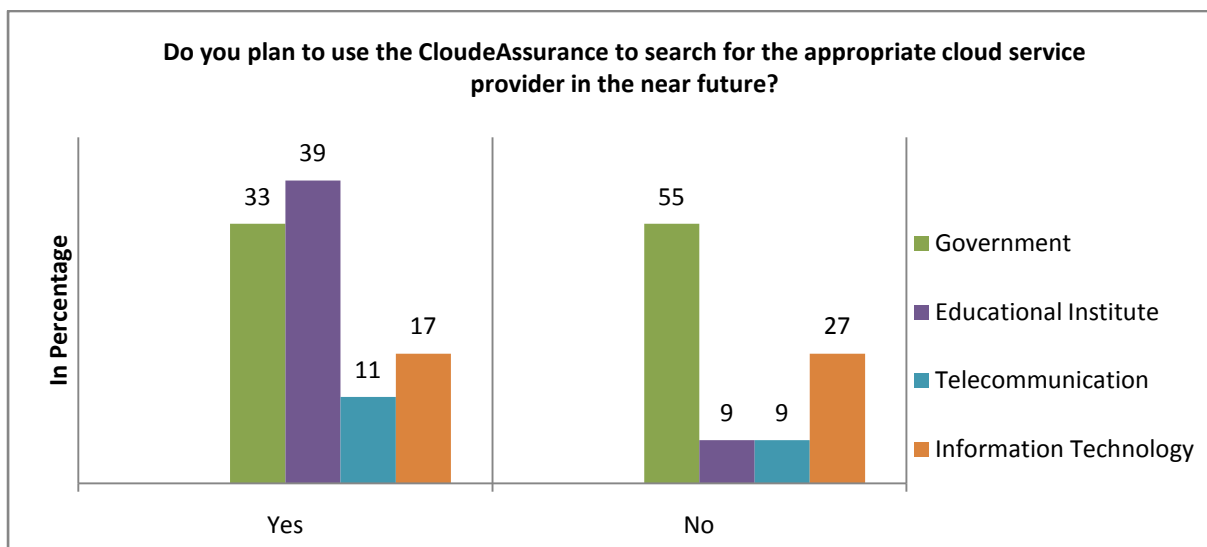


Fig.42. Sectors' plan for using CloudeAssurance in the future (non-adopters).

Despite the fact that only, a few of the respondents have used the CloudeAssurance, more than two-thirds (62.1%) as shown in Table 17 state that they are going to use the CloudeAssurance in the future. Although CloudeAssurance tool has been helpful only to the IT and government sector, the education sector have shown significant interest (87.5%) in using the tool in the near future.

50% of the governmental sector is closely interested in using the tool in the future, compared to the other responses received from the same sector; they are ranked second, after the education sector with more than one third (33%). About a third of both of the respondents from IT and telecommunications (17% and 11% respectively) are planning to use the CloudeAssurance in the future. Both the IT and telecommunication sectors have a common reason regarding their intentions to not use the tool in the future, in order to search for the right cloud service provider. They mentioned that they do not know the tool. From a governmental point of view, they are using the gCloud framework and they emphasised the lack of defined requirements that exist in the tool.

Table 17. Sectors' plan for using CloudeAssurance in the future (non-adopters).

Answer	What sector are you working in?						Response Percent	Response Count	
	IT	Telecommunication	Education	Government	Healthcare	Banks			
Yes	3	2	7	6	0	0	62.1%	18	
No	3	1	1	6	0	0	37.9%	11	
If "No", Please write your comment								4	
								<i>answered question</i>	29
								<i>skipped question</i>	3



## 6.4 Adopters Views on the Tools' Usefulness

This section will describe the results of the respondents who have already adopted cloud computing. We asked the respondents several questions in order to answer to the following questions: What is the opinion of the adopters of having a tool for the purpose of evaluating cloud providers' transparency? What is the likelihood of using tools such as CSA STAR registry, CTP and CloudeAssurance to evaluate the providers' transparency? What is the best tool in terms of its usage, helpfulness and their utilization in the near future?

The results suggest that more than two-thirds (76.6%) of the respondents have emphasised having a tool for evaluating cloud providers' transparency. This percentage is an increase of 11% on the non-adopters' results. There are a few of the respondents who have not used a tool; this percentage has increased slightly by 1.2%, compared with the non-adopters. The different sections have given several reasons for their choices. One response from a respondent in the IT sector mentioned the uncertainty about the accuracy of the results generated by the tool. The educational domain has a different opinion on the subject of transparency. They say that transparency will not help, especially if the type of data hosted in the cloud is sensitive. The governmental sector has a different opinion, stating that they are yet to see a comprehensive tool and as such, they have to use different tools to accomplish their own customised scripts depending on their needs and requirements. Some respondents (12.8%) are undecided whether to comment on the importance of the tools; looking at the respondents' profiles it can be suggested that their degree of influence might have an effect on their decision. 50% of the respondents emphasised that they have no influence in their organisation. Of the remaining, some said they do not have sufficient information about the tools in the market and some were concerned about the tools' trustworthiness.

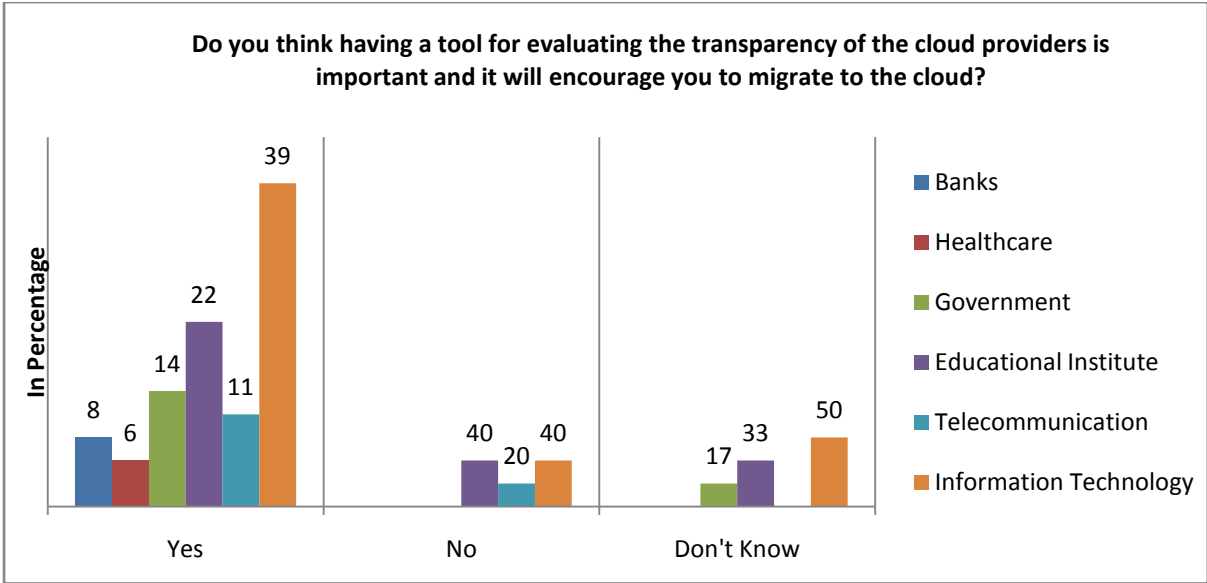


Fig.43. Sectors' opinion on using tools to evaluate providers' transparency (adopters).

Figure 44 highlights the sectors' opinions about having a tool for the evaluation of the cloud providers' transparency. The IT domain is the top sector, constituting about two thirds of all the other sectors combined. About a quarter of the responses were received from the education sector, which was in second place after the IT sector. The telecommunication domain has received 11% of the responses and the lowest two sectors are banking and healthcare. Despite receiving the least number of the responses received from these last two sectors, neither of them disagreed as to the importance of having the tools to evaluate cloud providers' transparency. The Figure also shows some of the sectors that were reluctant to answer this question, which are the IT, governmental and education sectors. The reasons for this were explained in the previous paragraph. Only a few respondents from the IT, education and telecommunication sectors disagreed as to having a tool for the evaluation of cloud providers' transparency.

The following Figure illustrates the results of the sectors that are likely to use the tools of transparency, in order to evaluate cloud providers' transparency. The overall rating average is 3.95 out of 5.0, representing 79% of the respondents who are likely to use tools to evaluate cloud providers' transparency. All of the respondents from the banking sector have strongly agreed to use the tools, followed closely by the telecommunication, IT and healthcare sectors. The least interested domains, with regards to using the tools are governments and education. The reasons for this have been described previously in Figure 33, as it is believed that there is no comprehensive tool that can match the customers' requirements. Moreover, it is suggested that transparency will not be a great help, especially if critical data is being hosted.

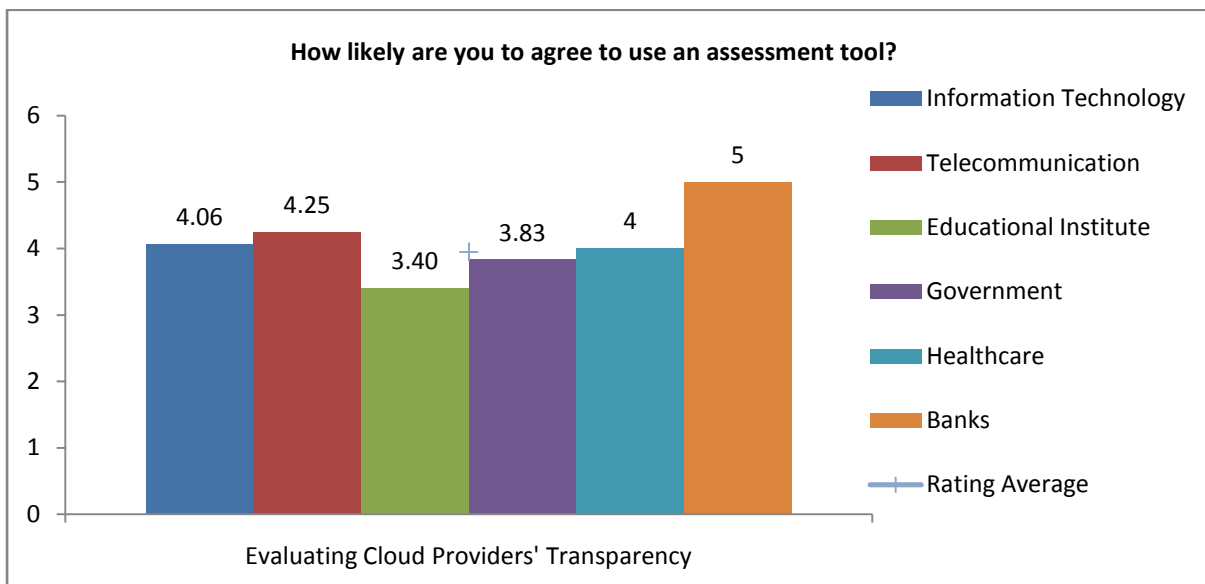


Fig.44. Sectors' likelihood of using the tools (adopters).

From the adopters' point of view, the level of usage for the CSA STAR has slightly decreased by 2.9%, compared with the non-adopters; their level of usage is 14.3%. For those who have not used CSA STAR it has increased by the same percentage (2.9%). We claim that the reason for not using the CSA STAR for searching for a cloud service provider might be because it provides more data, rather than offering a method for comparing between the services. This can create difficulties for potential customers when selecting the right cloud service provider. The next question, which is related to the usefulness of CSA STAR, might present a definite answer to our claim.

Figure 45 presents the percentages of the sectors' usage. In terms of using the CSA STAR, the top two joint sectors, collecting 33% of the responses, are IT and governments. Banks and telecommunications received 17%. For those sectors that have not used the CSA STAR, the IT sector has also been the top sector amongst others, gathering 42% of the responses. This is followed by education, with more than a quarter, governments (11%), telecommunications (8%) and jointly banks and healthcare (6%).

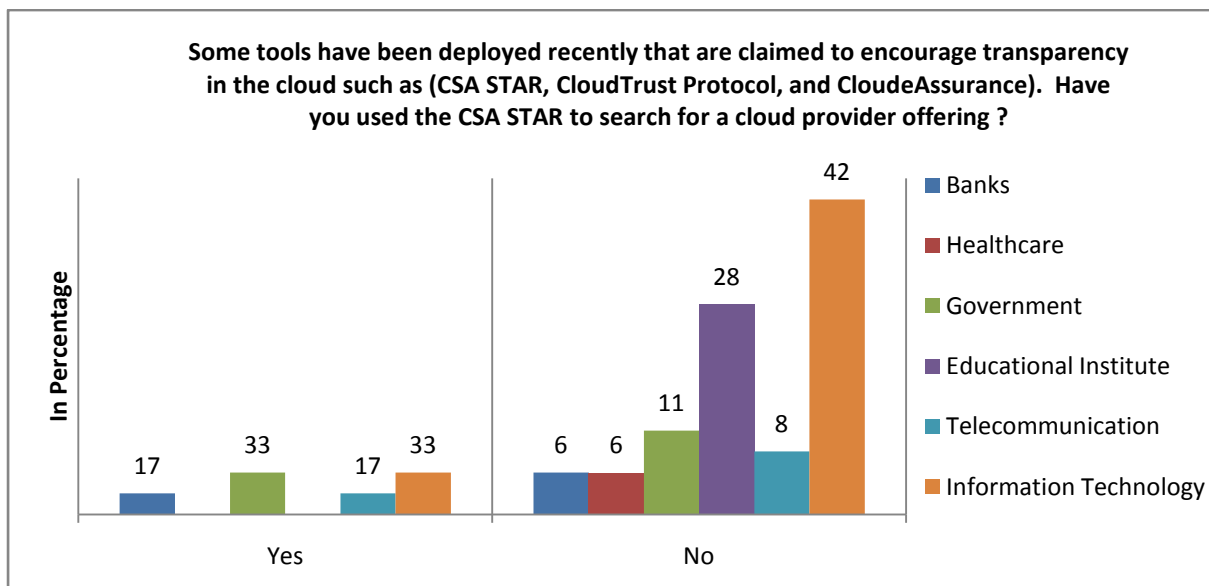


Fig.45. Sectors' usage percentage of CSA STAR (adopters).

Figure 46 shows the perceived level of usefulness of the sectors that have already adopted the cloud and used CSA STAR registry. 100% of the telecommunication sector respondents acknowledged the tool's helpfulness. Jointly, 80% of banks and governments have also agreed that CSA STAR was helpful to them. The lowest sector is that of IT, receiving 70%. The perceived level of usefulness of the CSA STAR from the point of view of IT has increased by 50%, compared with those IT respondents who have not adopted the cloud. The influential role of the respondents, as well as the adoption of the cloud, could have been the reason for the increased level of helpfulness for the IT sector. This is the same for the telecommunication sector, which has increased by 20%. With regards to the banking sector, the perceived level of helpfulness has reached 100%, when compared with those respondents who have not adopted the cloud. The governmental sector's perceived level of helpfulness has decreased slightly by 10%, compared with the respondents who have not adopted the cloud.

A respondent from the government sector mentioned, “The CSA STAR is a rich source of information that is held in its registry. However, we struggle to find the right provider, since there is no method of performing a comparison”. This statement might validate our claim, which is that the tool would be helpful if there is a mechanism that helps compare between the cloud providers’ offerings.

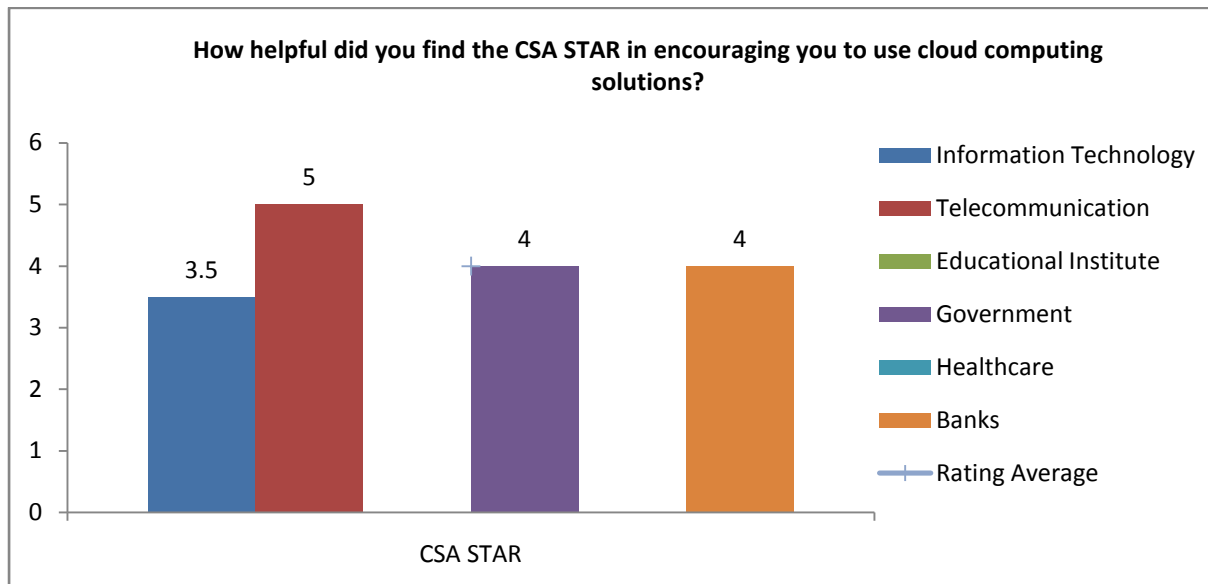


Fig.46. CSA STAR helpfulness for sectors (adopters).

With regards to the opinions of the sectors that will use the CSA STAR in the future, Figure 47 displays the percentages of each sector’s perceived level of future usage. This figure decreased by 20.3% between those who have and have not adopted the cloud. It dropped from 65.5% to 45.2%. More than half of the respondents have shown more interest in using the CSA STAR in the future, increasing from 34.5% to 54.8%. There are several reasons that have been captured in this survey to explain the different sectors’ responses for not using the CSA STAR in the future. Two responses were received from the IT sector, four responses from the education sector and one response from the governmental sector and two from healthcare.

Responses received from the IT sector have indicated that they use their own judgement in the selection of the cloud service provider, rather than using the tool, and they do not feel that they have enough information about the tool. The education sector has given several opinions about using the CSA STAR in the future. Their responses are explained in the following points:

- They are not familiar with the tool.
- They will use the use the tool for academic research purposes but not for real deployment.
- They are more likely to select the cloud service provider based on the services provided, and then look to see whether they meet appropriate security controls.
- They use service providers that tend to be limited for each service.

The government sector acknowledged the CSA STAR’s richness of information; however, the lack of a method for comparing between the cloud providers’ offering is their main issue. From the healthcare point of view, the unfamiliarity of the tool is one of the reasons that dissuaded potential customers from using it. Another reason was raised by the healthcare sector is that they need to do research on the tool itself.

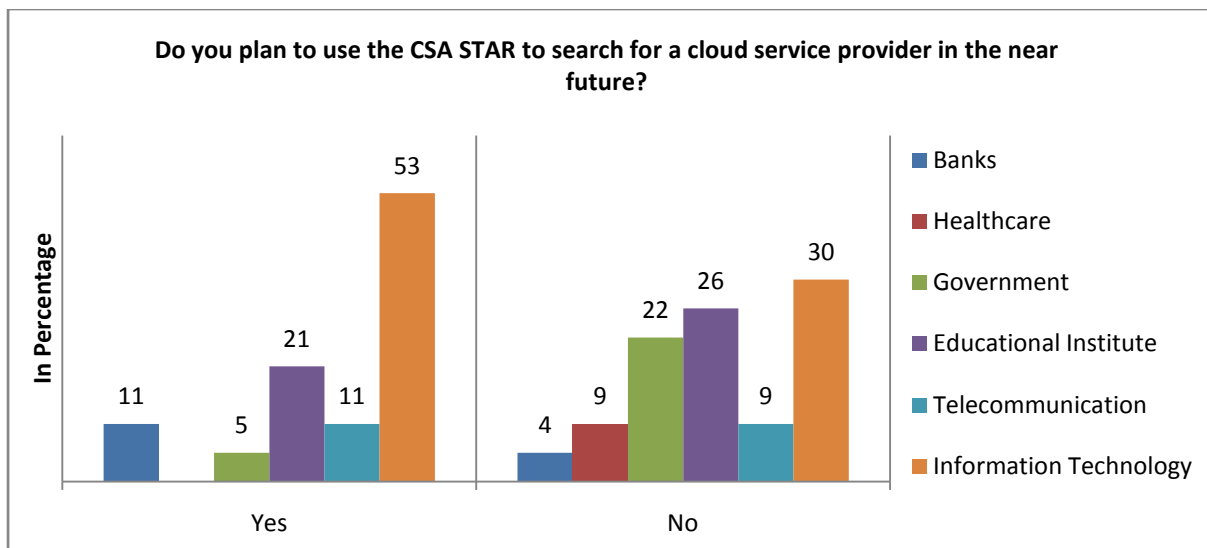


Fig.47. Sectors’ plan for using CSA STAR in the future (non-adopters).

Figure 48 shows the perceived level of usage for the CTP. It has increased by 2.9%, compared with the respondents who have not adopted the cloud, receiving 16.7%. The remaining 86.6% are not interested in using the CTP. From those, the top three joint sectors are telecommunications, education and healthcare. With regards to the IT sector, more than three quarters did not use the tool, followed by more than two third (67%) of the respondents from banks and governments. There are several factors that can be interpreted from the respondents’ answers. The respondents’ influential roles, the unfamiliarity of the tool and the sensitive nature of the data are the most common reasons for not using the CTP. This could also be the case for other tools, like CSA STAR and CloudeAssurance.

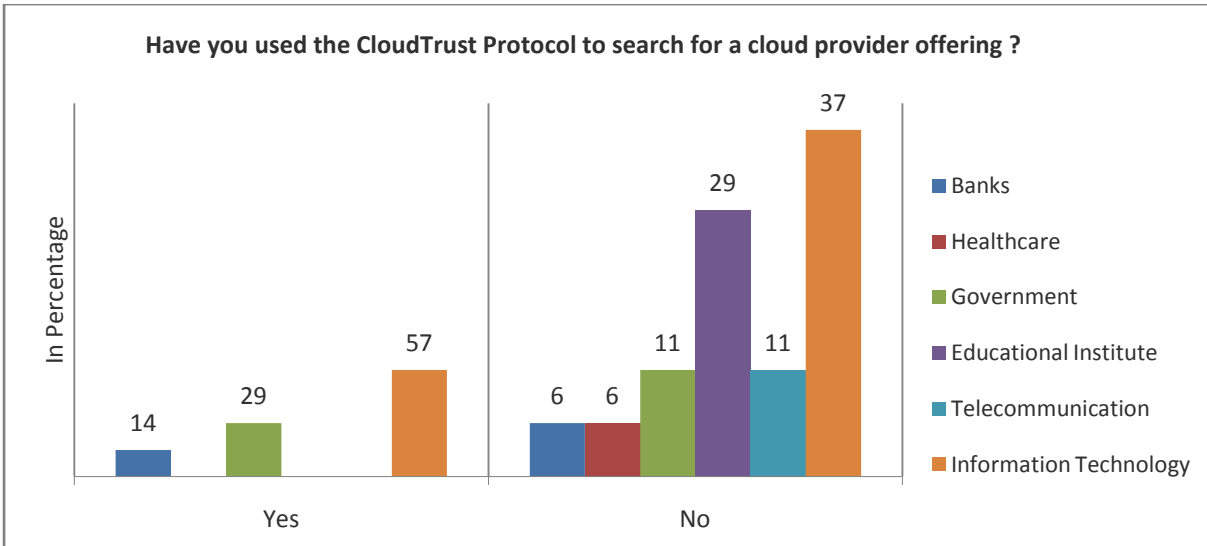


Fig.48. Sectors' usage percentage of CTP (adopters).

The responses that have been received from the sectors, in terms of assessing the usefulness of CTP, show that banking is the top sector that has benefited from the tool. CTP was more beneficial to banks than the CSA STAR. This might be because CTP has satisfied almost all of the respondents' assurance requirements, which were described earlier in Section 6.4. The governmental sector has received a score of 3.5/5.0 representing 70% of the respondents who have expressed its usefulness. CSA STAR registry has been more beneficial to governments than the CTP has. The last sector is IT, which indicates that CSA STAR is 25% better than CTP. So far we have compared the tools from the point of view of the adopters; however, the conclusion of this section will compare the usefulness of these tools between sectors from the point of view of both adopters and non-adopters.

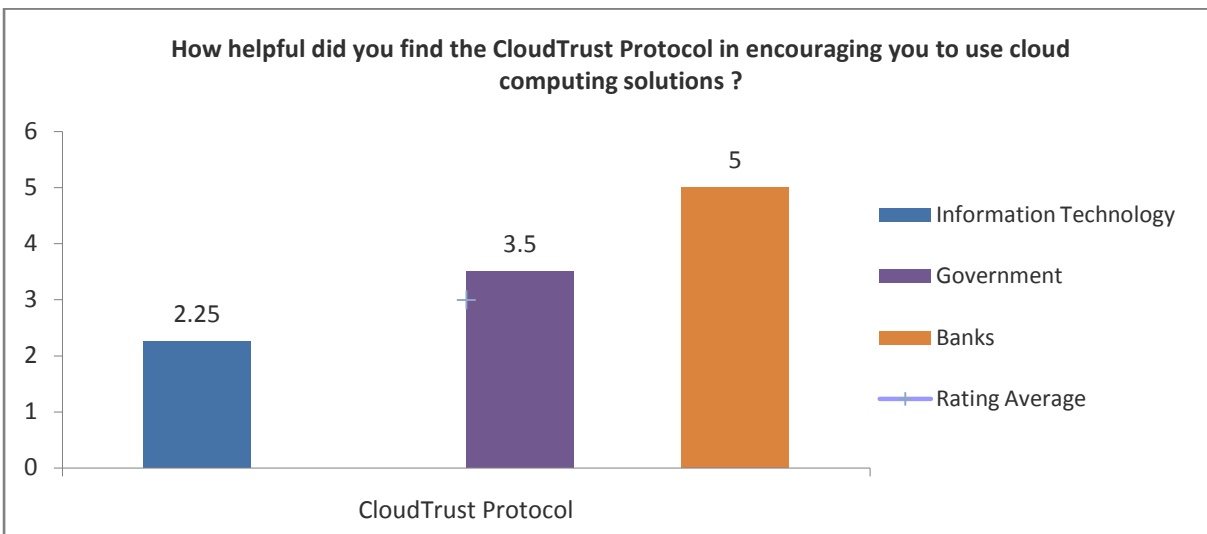


Fig.49. CTP helpfulness for sectors (adopters).

Figure 50 shows the respondents' opinions about using the CTP in the future. The perceived level of future usage for the CTP has received equal responses. 50% agreed to using the CTP in the future with the remaining showing no interest in using the tool in the near future for several reasons. Those reasons are captured from two sectors, namely, IT and education. From the IT perspective, they will use their own judgement to search for the right cloud service provider, rather than use the CTP. IT respondents also state that they do not have enough information about it, which has been the case for some tools. Responses received from the education sector have indicated several issues that include:

- Not decided to use the tool, looking into the respondent's nature of the organisation and the private cloud selected this might be the reason behind its hesitation.
- Not widely enough used yet.
- It could be used for academic research purposes but not for real deployment.
- The tool should focus on the functionality of the cloud service provide rather than on security.
- They use service providers that tend to be limited for each service.

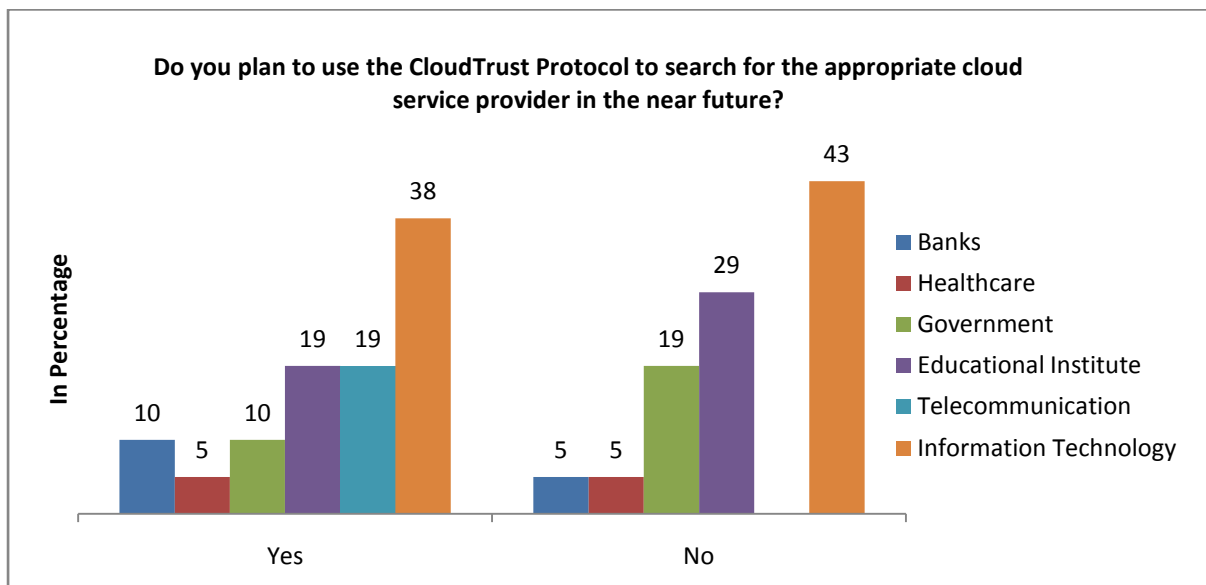


Fig.50. Sectors' plan for using CTP in future (adopters).

100% of the respondents from the telecommunication sector have acknowledged the tool's usage in the future. The other sectors, to some extent, share similar percentages towards using the tool in the future. The perceived level of usage of the tool, from the point of view of the adopters, is better than for those who have not adopted the cloud.



Figure 51 presents the respondents' opinions about using the CloudeAssurance tool. The level of usage has increased by 6.4% receiving 16.7% of the responses from the adopters' point of view. The remaining 83.3% have not used CloudeAssurance and have shown no interest in using it in the future. The top three sectors that have not used it are education, healthcare and banking. There are several reasons for this that have been derived from these sectors' responses. Table 18 illustrates each sector's reasons for not using CloudeAssurance.

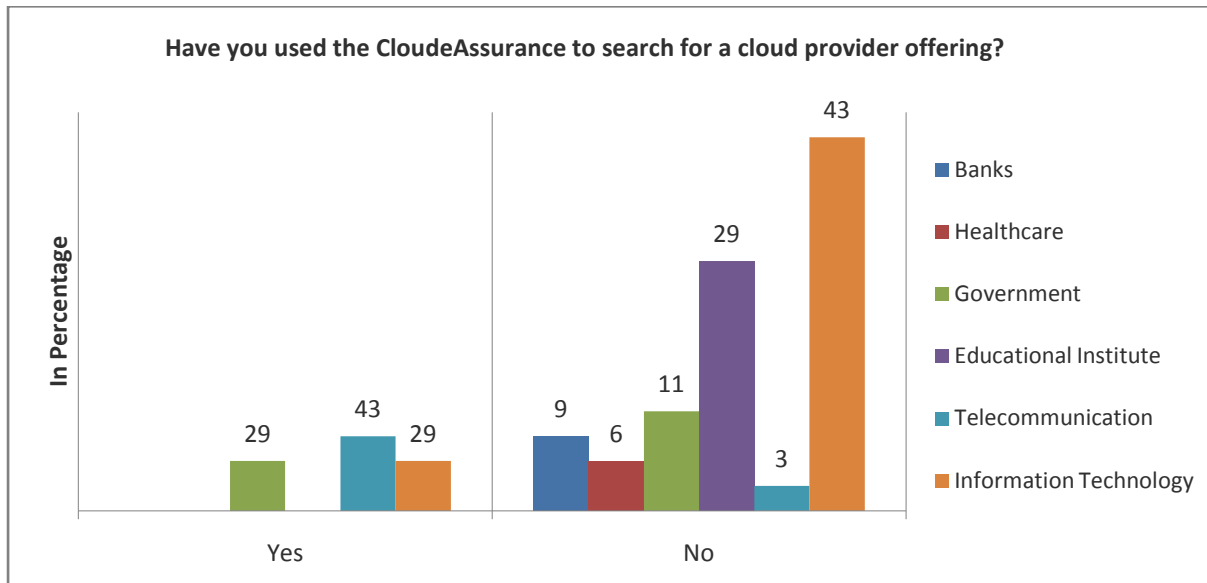


Fig.51. Sectors' usage percentage of CloudeAssurance (adopters).

Table 18. Sectors' Concerns Toward the Use of CloudeAssurance

Sector	Reasons
IT	<ul style="list-style-type: none"> <li>Using own tools and research</li> <li>Not enough knowledge about the CloudeAssurance tool</li> <li>Unsure of using the tool due to the nature of the organisation's data.</li> </ul>
Education	<ul style="list-style-type: none"> <li>Similar to CTP usage concerns highlighted in Figure 48.</li> </ul>
Government	<ul style="list-style-type: none"> <li>CloudeAssurance is not a free product, they provide a trial version but it is not sufficient to explore the functionality of the tool</li> <li>Waiting for the CSA OCF to finalize as so many have adopted it.</li> </ul>

Figure 52 shows the perceived level of helpfulness for the CloudeAssurance, which has dropped by 13.4% compared with non-adopters' point of view. The overall rating of the helpfulness from the sectors has recorded 3.0/5.0, which represents 60%. The telecommunication sector is the top amongst the others with 80%, followed by governments (50%) and IT (40%). The conclusion of this section presents a comparison between the tools (CSA STAR, CTP and CloudeAssurance) in term of its usage, usefulness and usage in the future.

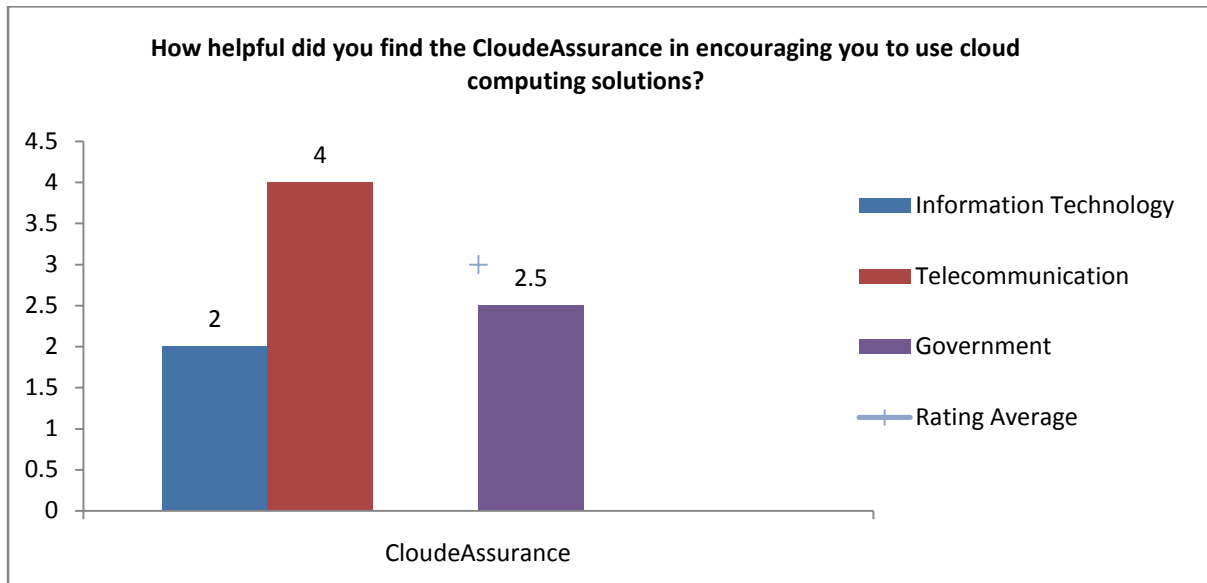


Fig.52. CloudeAssurance helpfulness for sectors (adopters).

About 50% of the respondents' agreed to use the CloudeAssurance in the future to search for cloud service providers. The level of usage of the tool, from the adopters' point of view, has decreased by 14.5%, compared with those who have not adopted the cloud. Almost all sectors share similar usage percentages to some extent, with the exception of the telecommunication sector, where all respondents acknowledged that they will use it in the future, as they have already expressed its usefulness amongst the other tools.

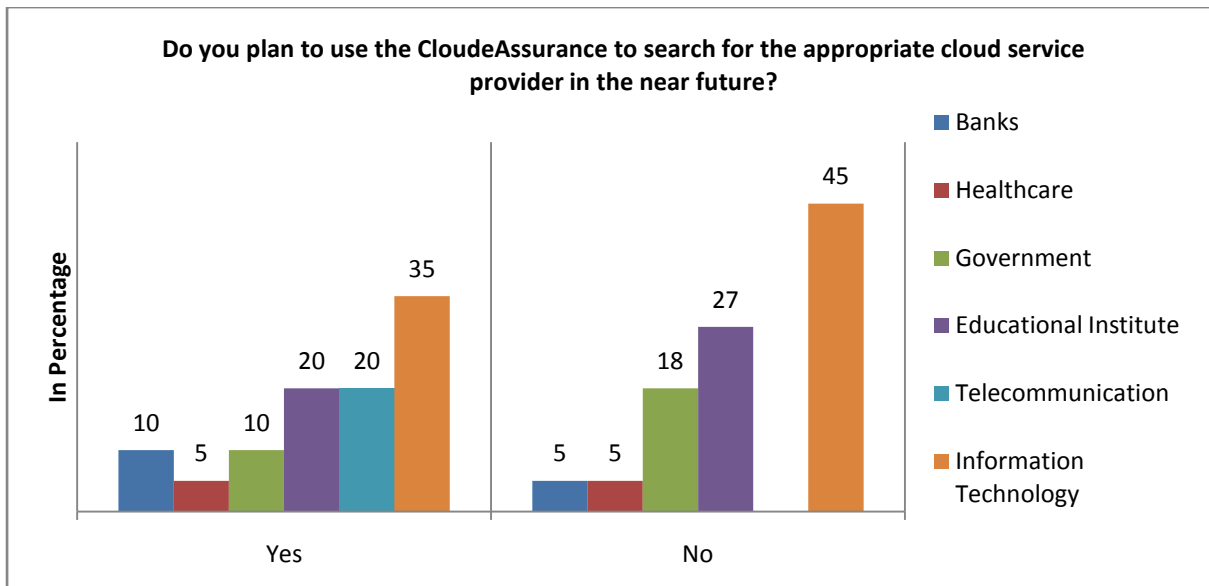


Fig.53. Sectors' usage percentage of CloudeAssurance (adopters).

## 6.5 Conclusion

The second part of the survey, which assesses the tools of transparency, highlights important findings from the respondents' general point of view. Looking in more depth, the results from both the adopters and non-adopters are highlighted and compared. Our aim is to discover whether existing tools, such as CSA STAR registry, CTP and CloudeAssurance have helped respondents from several sectors to answer the following points:

1. Respondents' opinion of the importance of having a tool for the purpose of evaluating cloud service providers, and that would play a role in encouraging sectors to migrate to the cloud.
2. Respondents' likelihood of using tools for evaluating cloud providers' transparency.
3. Respondents' usage of the tools.
4. Respondents' opinion of the tools' helpfulness.
5. Respondents' intentions to use the tools in the future.

The vast majority of respondents have agreed to the importance of using tools for the purpose of evaluating cloud providers' transparency, despite the fact that more than half of them did not use any of the three tools that have been mentioned. This might be understood to suggest a lack of trust in the results obtained from the tools. Moreover, the results suggest that the most popular tool (that respondents have actually used) is the CTP. This might be because it has fulfilled most of the customers' assurance requirements, as stated in Table 2 (Section 2.8). This could reinforce the assumption of the linkages between the popularity of the tool (percentage of usage) and fulfilment of the customers' assurance requirements. Although the CloudeAssurance was the least tool among the respondents, it still seems to be the most useful tool amongst the others, with 100% agreement on its usefulness. This could be due to its unique feature as a cloud rating system that helps customers in assessing and ranking cloud providers. Whereas the other tools, such as CSA STAR are only used as a repository that holds information about the provider's compliance to customers' requirements, without the ability to assess the providers' transparency. It is important to mention that the survey does not cover a specific sample size, so the general applicability of any conclusions is limited. However, the information that has been obtained can be used as a base for future work.

From the non-adopters' point of view, the majority of the respondents agreed on the importance of the tools for the purpose of evaluating cloud service providers, and they considered it as an important and encouraging step towards moving to the cloud. The number of the agreeing respondents could have increased by about quarter, provided that the remaining respondents have had a relevant and influential role within their organisation. Most of them also agreed to use the tools in order to evaluate cloud providers. However, some are reluctant to use the tools due to several factors that have been captured by the survey. The results suggest that the influential role of the respondents, among other factors, such as the trustworthiness of tools and having clear defined requirements are important in the survey. The leading two sectors in terms of their agreement to having and using a tool for the evaluation of the cloud provider are governments and the education sector.

CSA STAR registry is the most used tool, followed by the CTP. The least accepted tool is the CloudeAssurance and it has been utilized only by governments and the information technology sector though it is perceived as the most helpful tool across all sectors. It has been more helpful for governments and IT than any other tool. This indicates that the CloudeAssurance's helpfulness remains consistent, as mentioned previously in Section 6.4. The results have also shown that CSA STAR is still the second most useful tool. The one that has been the least useful for all the sectors is the CTP. From the sectors' perspective, it can be summarized that the telecommunication sector has achieved a great degree of usefulness with both CSA STAR and CTP, whereas the IT sector sees CloudeAssurance as the most helpful tool. Governments also selected CloudeAssurance and CSA STAR while the education sector mostly preferred the CTP.

Another important finding from the point of view of non-adopters is that most of them, more than two thirds, are willing to use these tools in the future. CSA STAR is the top amongst the others, with both CloudeAssurance and CTP sharing the exact same percentage in terms of future usage. Looking in depth from the sectors' perspectives, both education and governments are the most willing to use these tools in the future. Having said that, the government sector has also had a large number of responses that are not willing to use these tools in the future. Their reasons for not using the tools are justified by the following concerns:

- Sectors' unfamiliarity with the tools.
- Sectors' dependence on other frameworks, such as the gCloud especially made for governments.
- Lack of defined requirements.
- Sectors' accreditors' involvement.
- Tools' lack of trust.
- Not enough information provided by the tool.
- No consideration of using the tools because they have not thought about moving to the cloud.

The findings suggest that the perceived level of usage and helpfulness has been affected by the customers' assurance requirements, defined in Chapter 2, which was the case with the findings presented in Section 6.2. The only difference is that the CSA STAR was mostly used by non-adopters, rather than the CTP as it was suggested in Section 6.2.

Finally the assessment of tools from the non-adopters perspective is compared in Table 19. It shows the most used and useful tool. Tables 20, 21 and 22 highlight sectors' (IT, government, education, banks, healthcare and telecommunications) opinions about the tools' usage, helpfulness and usage in the future.

Table 19. The Most Used, Useful and Used Tool in the Future (Non-Adopters)

Criteria of tools' evaluation		
Most used	Most useful	Most used in future
CSA.	CloudeAssurance	CSA
CloudTrust	CloudTrust	CloudeAssurance and CloudTrust
CloudeAssurance	CSA	-

Table 20. Ranking Sectors Based on their Usage of the Tools (Non-Adopters)

Sectors	Usage				
	1	2	3	4	5
CSA	Gov.	Edu. IT & Tele.	-	-	-
CloudTrust	Gov. Edu. IT & Tele.	-	-	-	-
CloudeAssurance	Gov.	IT	-	-	-

Table 21. Ranking Sectors Based on the Tools' Helpfulness (Non-adopters)

Sectors	Helpfulness				
	1	2	3	4	5
CSA	Gov.	Tele.	Edu.	IT	-
CloudTrust	Tele.	Edu.	Gov.	IT	-
CloudeAssurance	IT	Gov.	-	-	-

Table 22. Ranking Sectors Based on their Future Planned use of the Tools (Non-adopters)

Sectors	Usage in Future				
	1	2	3	4	5
CSA	Edu.	Gov.	IT.	Tele.	-
CloudTrust	Edu.	Gov.	IT	Tele.	-
CloudeAssurance	Edu.	Gov.	IT	Tele.	-

We now highlight the adopters' most important opinions about their usage of the tools and the benefits and disadvantages they have faced. We asked respondents several questions to understand what tools they have used, which was the most useful tool for them when searching for cloud service providers, and the tool that they will use in the future.

Adopting cloud computing has been a good influence on the respondents' answers about having a tool that will evaluate the cloud providers' transparency. Respondents who have adopted the cloud, and who also have an influential role in their organisation, have shown an increase of 11%, compared with those who have not adopted the cloud and have a less influential role. In almost all of the sectors, respondents have emphasised the importance of having a tool for the purpose of evaluating providers' transparency. The top two sectors are IT and education. Respondents from governments, educational institutes and IT raised only a few concerns. Table 23 shows respondents' concerns about having tools for evaluating cloud providers' transparency. These concerns have affected the sectors' likelihood of using the tools. The most affected sectors are education and government.

Table 23. Sectors' Concerns Towards Having a Tool for Evaluating Provider's Transparency

<b>Respondent</b>	<b>Concern</b>
Information Technology	Not trusting the results that are generated by the tool
Education	Transparency will not help as long as critical data is hosted in the cloud
Government	No comprehensive tool is available to accomplish customised scripts



The predicted future use of the tools is about 15% less among the respondents who have not adopted the cloud. The respondents' concerns are summarised in Tables 24,25 and 26.

Table 24. Sectors' Concerns Towards Using CSA STAR (Adopters)

<b>Respondent</b>	<b>Tool</b>	<b>Concerns</b>
Education	CSA STAR	<ul style="list-style-type: none"> <li>- They are not familiar with the tool.</li> <li>- They will use the tool for academic research purposes but not for real deployment.</li> <li>- They are more likely to select the cloud service provider based on the services provided and then look to see whether they meet appropriate security controls.</li> <li>- They use service providers that tend to be limited for each service.</li> </ul>
IT		<ul style="list-style-type: none"> <li>- They use their own judgement in the selection of the cloud service provider, without using the tool.</li> <li>- They do not have enough information about the tool.</li> </ul>
Government		<ul style="list-style-type: none"> <li>- They lack a method for comparing between the cloud providers' offerings.</li> </ul>
Healthcare		<ul style="list-style-type: none"> <li>- Unfamiliarity with the tool is one of the reasons that did not let potential customers using it.</li> <li>- They need to do research on the tool itself.</li> </ul>

Table 25. Sectors' Concerns Towards Using CTP (Adopters)

<b>Respondent</b>	<b>Tool</b>	<b>Concerns</b>
IT	CloudTrust	<ul style="list-style-type: none"> <li>- They will use their own judgment to search for a provider.</li> <li>- They do not have sufficient information about the tool.</li> </ul>
Education		<ul style="list-style-type: none"> <li>- Not decided to use the tool.</li> <li>- Not widely enough used yet.</li> <li>- Use it only for academic research purposes but not for real deployment.</li> <li>- The tool should also focus on the functionality of the provider, not just security.</li> </ul>

Table 26. Sectors' Concerns Towards Using CloudeAssurance (Adopters)

<b>Respondent</b>	<b>Tool</b>	<b>Concerns</b>
IT	CloudeAssurance	<ul style="list-style-type: none"> <li>- Using own tools and research.</li> <li>- Not enough knowledge about the CloudeAssurance tool.</li> <li>- Unsure of using the tool due to the nature of their organisation's data.</li> </ul>
Education		<ul style="list-style-type: none"> <li>- Similar to CTP usage concerns highlighted in Figure 48.</li> </ul>
Government		<ul style="list-style-type: none"> <li>- CloudeAssurance is not a free product, they provide a trial version but it is not sufficient to explore the functionality of the tool</li> <li>- Waiting for the CSA OCF to finalize as so many have adopted it.</li> </ul>

Tables 27 – 30 compare each sector with regards to the tools' usage, the perceived level of helpfulness and future usage.

Table 27. The Most Used, Useful and Used Tool in the Future(Adopters)

<b>Criteria of tools' evaluation</b>		
<b>Most used</b>	<b>Most useful</b>	<b>Most used in future</b>
CloudTrust & CloudeAssurance	CSA	CloudTrust
CSA	CloudeAssurance & CloudTrust	CloudeAssurance
-	-	CSA STAR

Table 28. Ranking Sectors Based on their Usage of the Tools (Adopters)

Sectors	Usage				
	1	2	3	4	5
CSA	IT & Gov.	Tele. & Banks	-	-	-
CloudTrust	IT	Gov.	Banks	-	-
CloudeAssurance	Tele.	IT & Gov.	-	-	-

Table 29. Ranking Sectors Based on the Tools' Helpfulness (Adopters)

Sectors	Helpfulness				
	1	2	3	4	5
CSA	Tele.	Banks & Gov.	IT	-	-
CloudTrust	Banks	Gov.	IT	-	-
CloudeAssurance	Tele.	Gov.	IT	-	-

Table 30. Ranking Sectors Based on their Planned Future Use of the Tools

Sectors	Usage in Future				
	1	2	3	4	5
CSA	IT	Edu.	Tele. & Banks	Gov.	-
CloudTrust	IT	Tele. & Edu.	Gov. & Banks	Health	-
CloudeAssurance	IT	Tele. & Edu.	Gov. & Banks	Health	-

The results suggest that tools of transparency (CloudeAssurance and CTP) have turned out to be more useful to the non-adopters than respondents who have adopted cloud computing. This result would tend to reject our hypothesis, stated in Section 1.2.3. The only tool that conforms to our hypothesis is CSA STAR, which has shown itself to be more useful for adopters than the non-adopters.

## **Part III**

### **Chapter 7: CloudAdvisor**

#### **7.1 Introduction**

The CloudAdvisor framework has been developed to provide cloud customers with a mechanism to select the most trustworthy and transparent cloud providers. In order to do that, customer assurance requirements have been identified in Section 2.5. Requirements such as trustworthiness measurement, transparency measurement, support of evidence, keeping evidence up-to-date, adoption of best industry standards, and comparing between cloud providers' offering. Those requirements are believed to bring assurance to cloud customers provided that they have been considered in the development of tools. Some of the tools and frameworks that were described in Section 2.6 and compared in Table 2 (Section 2.8) have satisfied some of the requirements but not all of them. Therefore, the CloudAdvisor aims to satisfy all of the requirements.

In this chapter, the CloudAdvisor requirements are introduced in Section 7.2. The rationale for developing the CloudAdvisor framework is discussed in Section 7.3. In Section 7.4, the CloudAdvisor's motivation is presented. In Section 7.5, a detailed specification and workflow of CloudAdvisor will be designed showing how both the cloud customer and provider will benefit from it. In addition, various scenarios will be presented in order to provide cloud customers with the vision of how CloudAdvisor will work. For example, showing how the trustworthiness score is calculated for the cloud provider. Section 7.5 shows how the cloud provider's transparency is measured based on the CAIQ questionnaire and the Generic Scorecard Template (GST).

## 7.2 CloudAdvisor Requirements

The CloudAdvisor framework aims to satisfy the following requirements.

- Measuring cloud provider's trustworthiness score based on the business factors defined by [33].
- Measuring cloud provider's level of transparency based on CAIQ questionnaire template [31] and GST
- Allow cloud customers to monitor cloud provider's claims through evidence validation (i.e. is the evidence up-to-date?)
- It's worth mentioning that CloudAdvisor framework has been built on the basis of adopting Cloud Controls Matrix (CCM) framework and the Consensus Assessment Initiative Questionnaire (CAIQ). Therefore, it was important to evaluate CloudAdvisor's effectiveness which has been considered in Chapter 4 by conducting a survey questionnaire aims to assess the usefulness of CCM. The results from the survey questionnaire have shown positive opinions from respondents towards the usefulness of CCM.
- CloudAdvisor will assure there is a trade-off between security and transparency when asking for information from the provider in order to avoid compromising the security and privacy of both customers and providers
- CloudAdvisor intends to provide a risk assessment profile of the cloud provider before the consumer commits to any contractual agreement with them. Cloud consumers will be able to decide whether the cloud providers' infrastructure and service history are satisfactory before committing to any contractual agreement with cloud providers.
- CloudAdvisor framework can also be implemented as a web-based application accessible by both cloud providers and customers. where customers will be able to

obtain a real score for the providers based on their trustworthiness and transparency; and cloud provider will be able to submit the self-assessment questionnaire.

### **7.3 Rationale for developing CloudAdvisor**

IT managers and executives need a mechanism by which to select between the competing offers provided by different cloud providers. Service selection has been seen as a challenging issue since there may be numerous services that offer similar functionality but are provided by several different cloud providers [23]. More importantly, a trustworthy selection of a cloud provider in the cloud markets [32]. Therefore, selecting cloud providers will be mainly based on pre-assessing the cloud providers as business entities, according to multiple business factors [22], and the assessment of the security requirements compliance of the cloud providers [33] according to the CSA Security Controls defined in the CCM.

Pre-assessing cloud providers based on the history of breaches is an important step that could help cloud customers to choose between different competitive offers provided by cloud providers. [15]. Pauley has developed a score card that aims to evaluate the cloud providers' transparency according to four different domains, namely, security, privacy, auditability, and security level agreements. A set of questions has been formulated for each domain that a cloud customer might wish to ask. The evaluation is based on two steps. The first is a pre-assessment, where the cloud provider is evaluated as business entity according to some business factors, such as history of breaches and membership of cloud computing groups. The second step is called Postassessment, where the cloud provider's transparency is evaluated based on answering questions related to the abovementioned domains. The questions are formed by the CSA and ENISA.

Pauley's approach will be adopted here as it provides a means by which cloud customers can select a trustworthy cloud service from a cloud provider. However, there are some drawbacks to adopting this approach, which could be overcome by adding some important aspects. Pauley's approach fails to provide the evidence that support cloud providers' claims, in accordance to their answers, on these business factors. For instance, a cloud provider may answer that it is a member of a cloud computing group; however, this answer should be verified by evidence that shows it is indeed a member of a cloud computing group, such as CSA or others. Certification and compliance has been an important organisational consideration when it comes to service selection [33]. Therefore, evidence

should be in the form of certification from the organisation that the cloud provider claims it is a member of.

The need for evidence also applies to the questions that are related to the cloud providers' history of breaches. For example, if a cloud provider answers that it has encountered an outage, and it claims that it has informed the public (i.e. to the cloud customers), evidence is needed to verify this. Assurance of such evidence could help cloud customers to bring more sensitive and valuable business functions to the cloud and gain even larger payoffs. Therefore, "generating evidence-based confidence that assures that everything is claimed to be happening in the cloud is indeed happening as described, and nothing else" is seen to be the root of digital trust [21].

Another issue with this approach that could be considered a disadvantage is that cloud providers will be disqualified from further evaluation if they fail in the pre-assessment phase. To overcome this problem, the CloudAdvisor will not disqualify either the cloud provider or the cloud consumer because promoting transparency in the cloud will create digital trust. It is believed that creating digital trust, by restoring the visibility (transparency) in the cloud, will bring elastic benefits to both cloud providers and customers [21]

The CSA CCM has been chosen as the basis for our work as it promotes the use of best practices for providing security assurance within cloud computing. What is more, the CCM was designed to provide fundamental security principles to guide cloud providers and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. Moreover, the framework enables cloud customers to select a cloud service based on the capabilities and controls published by the providers. However, a shared concern that has been raised by several authors is how we verify that everything the provider claims happens in the cloud does indeed happen [21]. In other words, how can customers trust that the security controls are satisfied, as claimed by the providers, and are compliant with customers' requirements? [32, 33]

There are several works that have been conducted in order to address the abovementioned concerns. However, it is important to evaluate briefly the existing frameworks that have been the basis for this and other research. To the best of our knowledge, the CSA was the first framework that aimed to promote the best security practices, in order to provide security assurance within cloud computing [19].

However, the CSA could be criticised for not providing the cloud provider with the means to support its claims evidentially. Consequently, several works have recently emerged using the CSA CCM as their basis in order to address this gap and to answer questions such as, how are the claims of the providers verified and how are their claims maintained over time?

For example, a CTP was developed to be under the control of the cloud customers, as it is a mechanism that provides cloud customers with the capability to ask cloud providers questions based on important pieces of information called the “elements of transparency”. They deliver testimony about essential security configurations and operational characteristics for systems deployed in the cloud. The elements of transparency empower the cloud consumer with the right information to make the right choices about what processing and data to put in the cloud or leave out of the cloud, and to decide which cloud is best suited to satisfy their processing needs. However, the protocol builds trust for existing consumers rather than prospective customers, who are willing to choose between different cloud providers [33].

The GQM has been adopted by [33] as a mechanism that assesses the cloud providers’ security compliance based on the CCM and CAIQ. They have addressed cloud customers’ concerns by providing evidence that supports cloud providers’ claim. Adding also to some extent a quality to the evidence that is supported by the Cloud Provider. Quality of evidence such as compliance and completeness level of evidence. They have classified the completeness evidence into six classifications starting from no evidence, initial, planning, executing, monitoring and control, and closing. Each classification has a score value, which will be described later in the transparency measurement section. With regards to the compliance level of evidence, their scoring is based on three classifications. This includes: full compliance, partial compliance and non-compliance, each of which has its own score.

By providing this evidence, it will help cloud customers to resolve their concerns, as to how they can trust that providers’ security controls are satisfied and are compliant with customers’ requirements? [32]. Meanwhile, the second question, which is how to monitor the honesty of the cloud providers’ claims, is still not answered. In addition to this remaining gap, their approach lacks from the pre-assessment phase where the cloud provider’s trustworthiness should be measured. Therefore, the CloudAdvisor will try to address these important gaps, allowing cloud customers to be able to monitor the honesty of the cloud



providers' claims and, most importantly, to measure the cloud provider's trustworthiness, as has been done by Pauley.

#### **7.4 Motivation**

The idea of combining two features, trustworthiness and the competence to estimate the risk of interaction with the cloud provider has been introduced by [101]. This has encouraged us to develop the CloudAdvisor framework, which is based on coupling two salient features that are necessary when it comes to selecting the cloud provider that meets cloud customers' business requirements. The first is adopting the current CSA CCM and the CAIQ, by applying Pauley's method, and attaching a generic scorecard template (GST) to each control group placed in the CAIQ questionnaire. The aim is to measure cloud providers' transparency. The second feature is adopting the same method for providing cloud customers with a pre-assessment of cloud providers based on questions formed and developed by the CSA, ENISA and NIST. The aim is to measure cloud providers' trustworthiness. This trustworthiness level is calculated by providing a score for the business factors that have been defined by Pauley. His method is revised slightly to include evidence that supports cloud providers' claims.

#### **7.5 Workflow of the CloudAdvisor**

- (1) Cloud providers are entitled to register in order to create a fine-grained history profile based on answering questions. These questions are related to attributes, such as the number of security or privacy breaches that the cloud provider has suffered from, the number of outages and whether the cloud provider has publicized them. It also notes whether the provider is a member of an official cloud computing group. Pauley formulates these questions, however, we add the capability for providers to submit evidence that supports these claims and increases the confidence of customers. The evidence can be in a form or document, such as certification, or a link that shows published evidence. It is worth mentioning that even though CloudAdvisor will allow the submission of evidence of published information, this does not prevent cloud providers from omitting the reporting to CloudAdvisor of failures that did occur and they did not publicise. However, we considered two possible solutions. The first is by providing potential cloud customers with the ability to submit incidents using a web

form such as the DataLoss DB Open Security Foundation. The second solution is to include RSS feed from the Privacy Rights Clearinghouse database into the CloudAdvisor. This method will automatically fetch any existing breaches since 2005 or the latest.

At the same time, providers can start answering the CAIQ questionnaire. The GST is attached to the CAIQ questionnaire. The CAIQ template will contain the control area and questions that need to be answered by the providers. Each question in the CAIQ is attached to the GST, which holds answers and evidence submitted by providers.

- (2) The evidence is then validated by a trusted third party organisation that validates the entry of the provider, based on the evidence provided. Once the registration is confirmed and the validation process is complete, cloud providers trustworthiness and transparency will be calculated in Step 3.
- (3) Computing the trustworthiness score for the cloud providers' profile. A threshold value will determine the trustworthiness level (low, moderate or high) based on the computed profile score. Cloud providers' transparency is calculated based on the cloud provider's answers to the cloud control areas questions presented in the CAIQ questionnaire.
- (4) Producing a report of cloud providers' trustworthiness and transparency
- (5) The report will be available to the cloud customers to view, evaluate and compare different cloud providers' transparency.

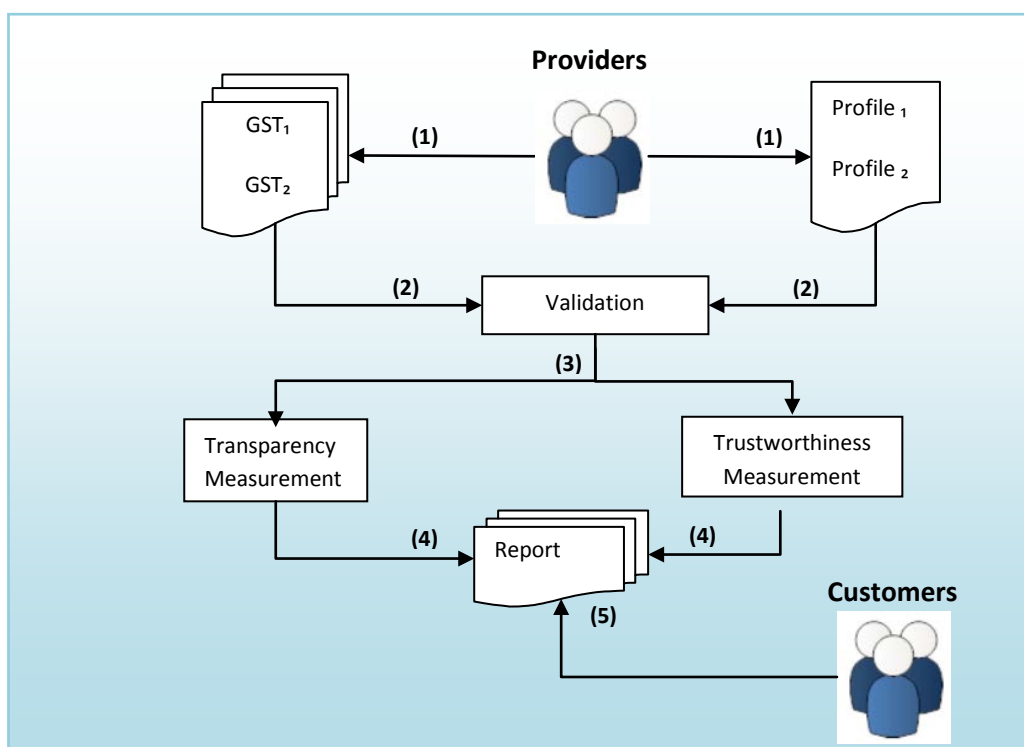


Fig.54. CloudAdvisor Workflow.

In the following section, the elements of this workflow are described in more detail.

### 7.5.1 Computing Trustworthiness Score – Adoption of Pauley’s Methodology

- **Pre-assessment Phase – Business Factors**

As Chapter 2 outlined, the pre-assessment phase is crucial to evaluate the cloud providers’ trustworthiness based on several attributes, such as the history of breaches, and other related business attributes that could increase cloud customers’ confidence. In this phase, Pauley’s original plan is to evaluate the cloud providers’ business entity based on the history of breaches and other factors, before any detailed assessment can take place. Pauley defines a threshold value where by the cloud provider should be included in the detailed assessment phase. However, in this thesis, the cloud provider will not be excluded from the second phase (the detailed assessment).

A threshold value will be defined, in order to evaluate the level of trustworthiness of the cloud provider, based on their score from answering the questions in the pre-assessment phase. For example, if the cloud provider has scored a value below 50, it means its trustworthiness level is **LOW**. On the other hand, a score of between 50 and 70 indicates a **MODERATE** trustworthiness level, and if a cloud provider scores over 70 its trustworthiness level is **HIGH**. The pre-assessment score is computed based on the business factors that are defined by Pauley. The following points will describe in more detail the attributes that are considered in the pre-assessment phase (Trustworthiness Attributes), as well as how this measurement is performed using the business factors. The business factors have been slightly revised, as shown in Table 31, by adding a question for each of the following factors: Security breaches, privacy breaches, outages and data loss, in order to properly evaluate the cloud provider’s history and encourage transparency.

In Pauley’s method the cloud provider is provided with a negative score equal to “0” if it discloses information about, for example, a security breach, privacy breach, outages or data loss. However, in this thesis the cloud provider is rewarded with a positive score equal to “1”, rather than given a negative score, provided that it discloses any information regarding security, privacy breaches, outages and data loss. However, it is still important to provide the cloud provider with a negative score equals to “0” or less than "1" if it has suffered from any type of breaches, outages or data loss.

Table 31.Improved Trustworthiness Attributes

	Business Factors	Score
1	Number of years in business	$\begin{aligned} & \text{if } y \leq 5 \text{ then} \\ & \text{if } y = 5 \text{ then } x = 0.8 \\ & \text{if } y = 4 \text{ then } x = 0.6 \\ & \text{if } y = 3 \text{ then } x = 0.4 \\ & \text{if } y = 2 \text{ then } x = 0.2 \\ & \text{if } y = 1 \text{ then } x = 0.0 \\ & \text{if } y > 5 \text{ then } x = 1 \end{aligned}$
2	Suffered from security breaches?  Published security breach?	$\text{Security Breach}_{Score} = \begin{cases} 1 & \text{if } sb = 0 \\ 1 - 0.sb & \text{if } sb \geq 1 \text{ and } sb \leq 9 \\ 0 & \text{if } sb \geq 10 \end{cases}$ $\text{if } sb \geq 1 \text{ then } T_{Security} = \left\{ \frac{\sum_{i=1}^e \text{Published Evidence}}{\sum_{i=1}^{sb} \text{Security Breach}} \right\}$
3	Suffered from privacy breaches?  Published privacy breach?	$\text{Privacy Breach}_{Score} = \begin{cases} 1 & \text{if } pb = 0 \\ 1 - 0.pb & \text{if } pb \geq 1 \text{ and } pb \leq 9 \\ 0 & \text{if } pb \geq 10 \end{cases}$ $\text{if } pb \geq 1 \text{ then } T_{Privacy} = \left\{ \frac{\sum_{i=1}^e \text{Published Evidence}}{\sum_{i=1}^{pb} \text{Privacy Breach}} \right\}$
4	Suffered from outages?  Published outages?	$\text{Outages}_{Score} = \begin{cases} 1 & \text{if } O = 0 \\ 1 - 0.O & \text{if } o \geq 1 \text{ and } o \leq 9 \\ 0 & \text{if } O \geq 10 \end{cases}$ $\text{if } O \geq 1 \text{ then } T_{Outage} = \left\{ \frac{\sum_{i=1}^e \text{Published Evidence}}{\sum_{i=1}^O \text{Outages}} \right\}$

5	<p>Suffered from data loss?</p> <p>Published data loss?</p>	$DataLoss_{Score} = \begin{cases} 1 & \text{if } l = 0 \\ 1 - 0.l & \text{if } l \geq 1 \text{ and } l \leq 9 \\ 0 & \text{if } l \geq 10 \end{cases}$ $\text{if } l \geq 1 \text{ then } T_{DataLoss} = \left\{ \frac{\sum_{i=1}^e \text{Published Evidence}}{\sum_{i=1}^l \text{DataLoss}} \right\}$
6	<p>Membership of Cloud Standard Groups?</p> <p>Published Membership Evidence?</p>	$Membership_{Score} = \begin{cases} 0 & \text{if } m = 0 \\ 1.m & \text{if } m \geq 1 \text{ and } m \leq 9 \end{cases}$ $\text{if } m \geq 1 \text{ then } T_{members hip} = \left\{ \frac{\sum_{i=1}^e \text{Published Evidence}}{\sum_{i=1}^m \text{Membership}} \right\}$
	Trustworthiness Total Score (TTS)	Total Trustworthiness Score of the 6 Business Factors
	Trustworthiness Percentile Score (TPS)	(Trustworthiness Total Score / 6) * 100
	Trustworthiness Level (TL)	<b>(Low</b> < 50), (70 ≥ <b>Moderate</b> ≥ 50), ( <b>High</b> > 70)

Therefore, adding to the CloudAdvisor framework, the background check assessment property aims to help us to assess the trustworthiness of the cloud provider, before the cloud customer makes any selection, or the CloudAdvisor conducts further assessment. This will include the assessment of the cloud providers' history of breaches and number of years in business.

Pauley's method will be adopted in order to assess cloud providers' trustworthiness. This is the first phase of the CloudAdvisor framework. The reason for this is to provide cloud customers with enough background information, related to cloud providers' history, prior to making any further assessment (for example, transparency assessment based on the CSA CCM framework). Pauley's method, as mentioned in Chapter 2, focuses on making a pre-assessment of the cloud provider before making further assessment. Pauley's method does

not provide the cloud customer with actual evidence and we try to overcome this problem by letting the cloud providers submit their evidence in order to validate their claims.

Pauley's method is based on asking questions and getting "Yes" or "No" answers. The same approach will be adopted, with the following differences:

- We will urge the cloud provider to provide evidence that can validate its claims.
- We will not exclude the cloud provider from the secondary assessment, which is known the transparency assessment. This is because the trustworthiness level of the cloud provider can change over time.
- We will encourage the cloud provider to score more points when it discloses more information about any type of breach.

The following points describe the scoring mechanism for the cloud provider's business.

- **Business Factors Computations**

Factor: **Years of Business**

Pauley indicated that, according to the US Small Business Administration, 50% of start-up companies fail in the first five years they do business. Therefore, a 0 score will be assigned to a company that has less than five years in business because of high probability of failure.

**Years of Business Computation**

- Question: How long has the cloud provider been in business?
- Factor Scoring value: **YoB\_Value**

**YoB\_Value = Years of Business Value.** The cloud provider will be assigned a zero value if their business has been running for less than one year, or a value of once if they have been running their business for more than five years, or different values ranging between (0.8 to 0.2) if the number of years is between five and four years.

**YoB\_Score = Years of Business Score in Percentage.**

$$Years\ in\ Business_{value} = \left\{ \begin{array}{l} 1\ if\ y > 5 \\ 0.8\ if\ y = 5 \\ 0.6\ if\ y = 4 \\ 0.4\ if\ y = 2 \\ 0.2\ if\ y = 1 \\ 0\ if\ y < 1 \end{array} \right\} (1)$$

$$Years\ in\ Business_{score} = \left\{ \begin{array}{l} 100 \\ 80 \\ 60 \\ 40 \\ 20 \\ 0 \end{array} \right\} (2)$$

#### Factor: **Membership of Cloud Standard Groups**

If the cloud provider is a member of any of the cloud computing groups such as ENISA, CSA, or any official certified cloud computing groups, it will increase the confidence of cloud customers. The cloud provider will score a value equal to one if it is part of any cloud computing groups; however, it is also entitled to submit evidence that backs up his claims. If it provides this evidence it will gain an additional score equal to one, otherwise a zero value will be given. This will affect the total score of the **Membership Factor**.

##### 1. Membership Factor

First of all, the CloudAdvisor prompts the cloud provider with a question, asking if it is a member of any of the cloud computing groups. If it answers, “Yes” then a list of official cloud computing groups is presented to the cloud provider for selection. Once the selection is confirmed, by answering, either “Yes” or “No”, the CloudAdvisor scoring engine will perform some computations based on the answers selected. The computation will be described after explaining how the cloud provider deals with the Membership Factor.

##### 2. Evidence Submission

When the cloud provider confirms that it is a member of the CSA cloud computing group, it is entitled to submit evidence that backs up this claim. If it does not have any evidence to submit it will be given a score of zero evidence. The evidence score will remain a zero value until it is provided. The CloudAdvisor offers flexibility to cloud provider, whenever the

evidence is submitted the score will eventually change. Various scenarios can be applied using the CloudAdvisor and computations can vary, based on the application on those scenarios. However, as an example, the Table below should explain clearly how the Membership Factor is computed with different scenarios for multiple cloud providers.

Table 32.Computing Provider's Trustworthiness – Scenario 1

Scenario 1						
Cloud Provider	Member of CCG?	NG	Evidence?	Score %	Value	Rank
<b>CP1</b>	Yes = 1	1	Yes = 1	100%	1	1
<b>CP2</b>	Yes = 1	1	No = 0	0%	0	2
<b>CP3</b>	No = 0	N/A	N/A	0%	0	3

**NG:** Number of groups that the cloud provider is a member of.

**CCG:** Cloud Computing Groups (i.e. CSA, ENISA, etc.)

**Evidence:** Evidence provided by the cloud providers that they are members.

The first scenario shows that both CP1 and CP2 are members of cloud computing groups. CP1 however has provided evidence that backs up its claim whereas CP2 has not. Therefore, when ranking cloud providers, based on the score of this factor, CP1 is in first place scoring 100%, while CP2 is ranked second with a score of 0%. In order to change the score of CP2 to 100%, it is entitled to submit evidence and, when it does, the score is automatically changed. CP3 has been given the lowest score of 0%, as it is not a member of any cloud computing group. However, this does not mean that CP3 is the worst provider, as other factors are also important and can play a significant role in changing the total score.

Table 33.Computing Provider's Trustworthiness - Scenario 2

Scenario 2						
Cloud Provider	Member of CCG?	NG	Evidence	Score %	Value	Rank
<b>CP1</b>	Yes = 1	3	Yes = 1	33.33%	0.33	3
<b><u>CP2</u></b>	Yes = 1	1	Yes = 1	100%	1	2
<b>CP3</b>	Yes = 1	2	No = 0	0%	0	4
<b><u>CP4</u></b>	Yes = 1	2	Yes = 2	100%	1	1

The second scenario can show that CP4 is ranked first, despite the fact that both CP2 and CP4 scored 100%. However, due to the large number of memberships that CP4 holds, it is more preferable than CP2. Both CP2 and CP4 provided evidence for their claims and they are



awarded with 100% score. Meanwhile, CP1 is in third place with a score of 33.33%. It claimed that it is a member of three cloud computing groups; however, it submitted only one piece of evidence. Therefore, we measure the transparency of membership factor for the cloud provider by dividing the total number of published evidence by the total number of memberships that it claims. The last one is CP3 with a score of 0%. It claims that it is a member of two groups; however, no such evidence was provided warranting a score of 0%. The score could change whenever the cloud provider submits evidence that supports its claims.

The cloud provider is evaluated based on its transparency with regards to the published evidence of published security/privacy breaches, outages, data loss incidents the claiming of and memberships. Therefore, the scoring mechanism is different for those five factors where evidence is a very important parameter that needs to be satisfied by the cloud provider. For instance, in the case of claiming is a member of any cloud computing groups.

Pauley's original method does not suggest that cloud providers should produce evidence to support their claims. In our case, we find that providing evidence is crucial in measuring the trustworthiness of cloud provider's membership factor. We are not just aiming to increase the confidence of the cloud customer through this factor only; we are also encouraging cloud providers to publish their evidence of each of Pauley's defined factors wherever possible. Thus, we are also measuring the transparency of cloud providers by publishing their evidence. Otherwise, the lack of evidence means the lack of trustworthiness and transparency.

## Factor: Membership

The Membership<sup>t</sup> score can have two possible scores depending on the cloud provider's answer as to whether they are a member of any cloud computing groups, such as ENISA or CSA. Membership<sup>t</sup> will have a score of "0" if the cloud provider answers "No"; otherwise the score is calculated by  $1.m$  where  $m$  is number of memberships that cloud provider holds. For example, if the number of memberships is three then the score of the cloud provider regarding the membership factor is 1.3. Equation (3) is responsible for measuring cloud provider's transparency with regard to his claims of being a member of any cloud computing groups. Therefore, the transparency is calculated by dividing the total number of published evidence of the Membership factor by the total number of memberships that the cloud provider hold. Equation (1) describes how the calculation is performed. The purpose of equation (2) is to convert the original score obtained from equation (1) into a percentile score.

$$\text{Membership}^t = \begin{cases} 0, & \text{if } m = 0, \\ (1.m), & \text{if } m \geq 1 \text{ and } m \leq 9 \end{cases} \quad (1)$$

$$\text{Membership}^t (\%) = \begin{cases} 0 \\ (1.m) * 100 \end{cases} \quad (2)$$

$$\text{Transparency Score} = \begin{cases} \frac{\sum_{i=1}^e \text{PublishedEvidence}}{\sum_{i=1}^m \text{TotalMemberships}}, & \text{if } m \geq 1 \end{cases} \quad (3)$$

Where **Membership<sup>t</sup>** = the trustworthiness score of the membership factor.

**e** = the total number of published evidence by the cloud provider with regards the membership factor.

**m** = the total number of memberships that the cloud provider holds.

**PublishedEvidence** = the total score of the published evidence provided by the cloud provider.

**TotalMemberships** = the total score of the memberships that the cloud provider holds.

Equation (2) will display the result in percentage %

The other factors, including security, privacy, data loss and outages, will follow the same scoring mechanism that has been applied to the Membership factor since evidence is highly important.

## Factor: Security Breach

The SecurityBreach<sup>t</sup> value can have three possible values depending on the cloud provider's answers as to whether it has suffered from security breaches, and, whether it has submitted evidence of published security breaches. SecurityBreach<sup>t</sup> will have a score equal to "1" if the cloud provider answers "No". If the answer is "Yes", then this means the cloud provider has suffered from a security breach. Thus, a score of "0" is assigned to the cloud provider if the number of breaches is more than 10 in a year. Alternatively, a score of  $(1 - 0.b)$  is assigned the provider if the number of breaches is between one and nine in a year. There is also a need to calculate the cloud provider's transparency with regards to publishing evidence of the existence of the security breach. This is calculated by dividing the total number of published evidence of the Security Breach factor by the total number of security breach incidents that the cloud provider has encountered. Equation (1) describes how the calculation is performed. The purpose of equation (2) is to convert the original score obtained from equation (1) into a percentile score.

$$\text{SecurityBreach}^t = \begin{cases} 1, & \text{if } b = 0 \\ 1 - 0.b, & \text{if } b \geq 1 \text{ and } b \leq 9 \\ 0 & \text{if } b \geq 10 \end{cases} \quad (1)$$

$$\text{SecurityBreach}^{t\%} = \begin{cases} 100 \\ (1 - 0.b) * 100 \\ 0 \end{cases} \quad (2)$$

The transparency score of the Security Breach factor needs to be calculated in case the cloud provider has encountered a security breach. Equation (3) shows how transparency is calculated based on the security breach factor.

$$\text{Transparency Score} = \begin{cases} \frac{\sum_{i=1}^e \text{PublishedEvidence}}{\sum_{i=1}^b \text{TotalSecBreaches}}, & \text{if } b \geq 1 \end{cases} \quad (3)$$

Where **SecurityBreach<sup>t</sup>** = the trustworthiness value of the Security Breach factor.

**e** = the total number of published evidence by the cloud provider with regards to the Security Breaches factor.

**b** = the total number of security breaches that the cloud provider has encountered.

**PublishedEvidence** = the total score of the published security breaches evidence provided by the cloud provider.

**TotalSecBreaches** = the total score of the security breaches that a cloud provider has encountered.

Equation (2) will display the result in percentage %

## Factor: Privacy Breach

The PrivacyBreach<sup>t</sup> value can have three possible values depending on the cloud provider's answers as to whether it has suffered from privacy breaches, and, whether it has submitted evidence of published privacy breaches. PrivacyBreach<sup>t</sup> will have a score equal to "1" if the cloud provider answers "No". If the answer is "Yes", then this means the cloud provider has suffered from a privacy breach. Thus, a score of "0" is assigned to the cloud provider if the number of breaches is more than 10 in a year. Alternatively, a score of  $(1 - 0.p)$  is assigned the provider if the number of breaches is between one and nine in a year. There is also a need to calculate the cloud provider's transparency with regards to publishing evidence of the existence of the privacy breach. This is calculated by dividing the total number of published evidence of the Privacy Breach factor by the total number of privacy breach incidents that the cloud provider has encountered. Equation (1) describes how the calculation is performed. The purpose of equation (2) is to convert the original score obtained from equation (1) into a percentile score.

$$\text{PrivacyBreach}^t = \begin{cases} 1, & \text{if } p = 0 \\ 1 - 0.p, & \text{if } p \geq 1 \text{ and } p \leq 9 \\ 0 & \text{if } p \geq 10 \end{cases} \quad (1)$$

$$\text{PrivacyBreach}^{t\%} = \begin{cases} 100 \\ (1 - 0.p) * 100 \\ 0 \end{cases} \quad (2)$$

The transparency score of Privacy Breach factor needs to be calculated in case the cloud provider has encountered a privacy breach. Equation (3) shows how transparency is calculated based on the privacy breach factor.

$$\text{Transparency Score} = \left\{ \frac{\sum_{i=1}^e \text{PublishedEvidence}}{\sum_{i=1}^p \text{TotalPrivBreaches}}, \text{if } p \geq 1 \right\} (3)$$

Where **PrivacyBreach<sup>t</sup>** = the trustworthiness value of the Privacy Breach factor.

**e** = the total number of published evidence by the cloud provider with regards to Privacy Breach factor.

**p** = the total number of privacy breaches that the cloud provider has encountered.

**PublishedEvidence** = the total score of the published privacy breaches evidence provided by the cloud provider.

**TotalSecBreaches** = the total score of the privacy breaches that a cloud provider has encountered.

Equation (2) will display the result in percentage %

## Factor: Outages

The Outages<sup>t</sup> value can have three possible values depending on the cloud provider's answers as to whether it has suffered from outages, and, whether it has submitted evidence of published outages. Outages<sup>t</sup> will have a score equal to "1" if the cloud provider answers "No". If the answer is "Yes", then this means the cloud provider has suffered from an outage. Thus, a score of "0" is assigned to the cloud provider if the number of outages is more than 10 in a year. Alternatively, a score of  $(1 - 0.p)$  is assigned the provider if the number of outages is between one and nine in a year. There is also a need to calculate the cloud provider's transparency with regards to publishing evidence of the existence of the outage. This is calculated by dividing the total number of published evidence of the Outage factor by the total number of outages incidents that the cloud provider has encountered. Equation (1) describes how the calculation is performed. The purpose of equation (2) is to convert the original score obtained from equation (1) into a percentile score.

$$\text{Outages}^t = \left\{ \begin{array}{l} 1, \text{if } o = 0 \\ (1 - 0.o), \text{if } o \geq 1 \text{ and } o \leq 9 \\ 0, \text{if } o \geq 10 \end{array} \right\} (1)$$

$$\text{Outages}^{t\%} = \left\{ \begin{array}{l} 100 \\ (1 - 0.o) * 100 \\ 0 \end{array} \right\} (2)$$

The transparency score of the Outages factor needs to be calculated in case the cloud provider has encountered an outage. Equation (3) shows how transparency is calculated based on the Outages factor.

$$\text{Transparency Score} = \left\{ \frac{\sum_{i=1}^e \text{PublishedEvidence}}{\sum_{i=1}^o \text{TotalOutages}}, \text{if } o \geq 1 \right\} (3)$$

Where **Outages**<sup>t</sup> = the trustworthiness value of the Outages factor.

**e** = the total number of published evidence by the cloud provider with regards to the Outages factor.

**o** = the total number of outages that the cloud provider has encountered.

**PublishedEvidence** = the total score of the published outages evidence provided by the cloud provider.

**TotalOutages** = the total score of the outages that the cloud provider has encountered.

Equation (2) will display the result in percentage %

The  $\text{DataLoss}^t$  value can have three possible values depending on the cloud provider's answers as to whether it has suffered from data loss, and, whether it has submitted evidence of published data loss.  $\text{DataLoss}^t$  will have a score equal to "1" if the cloud provider answers "No". If the answer is "Yes", then this means the cloud provider has suffered from a data loss. Thus, a score of "0" is assigned to the cloud provider if the number of incidents is more than 10 in a year. Alternatively, a score of  $(1 - 0.p)$  is assigned the provider if the number of incidents is between one and nine in a year. There is also a need to calculate the cloud provider's transparency with regards to publishing evidence of the existence of the data loss. This is calculated by dividing the total number of published evidence of the  $\text{DataLoss}$  factor by the total number of data loss incidents that the cloud provider has encountered. Equation (1) describes how the calculation is performed. The purpose of equation (2) is to convert the original score obtained from equation (1) into a percentile score.

$$\text{DataLoss}^t = \begin{cases} 1, & \text{if } d = 0 \\ (1 - 0.d), & \text{if } d \geq 1 \text{ and } d \leq 9 \\ 0, & \text{if } d \geq 10 \end{cases} \quad (1)$$

$$\text{DataLoss}^{t\%} = \begin{cases} 100 \\ (1 - 0.d) * 100 \\ 0 \end{cases} \quad (2)$$

The transparency score of  $\text{DataLoss}$  factor needs to be calculated in case the cloud provider has suffered from data loss. Equation (3) shows how transparency is calculated based on the  $\text{DataLoss}$  factor.

$$\text{Transparency Score} = \begin{cases} \frac{\sum_{i=1}^e \text{PublishedEvidence}}{\sum_{i=1}^d \text{TotalDataLoss}}, & \text{if } d \geq 1 \end{cases} \quad (3)$$

Where  $\text{DataLoss}^t$  = the trustworthiness value of the  $\text{DataLoss}$  factor.

**e** = the total number of published evidence by the cloud provider with regards to DataLoss factor.  
**d** = the total number of data losses that the cloud provider has encountered.  
**PublishedEvidence** = the total score of the published data loss evidence provided by the cloud provider.  
**TotalDataLoss** = the total score of the data loss that cloud provider has encountered.  
Equation (2) will display the result in percentage %.

A script for calculating cloud provider's trustworthiness and transparency has been developed using Java. It is presented in the Appendix (B.2). It shows how CloudAdvisor would measure cloud providers' trustworthiness based on the business factors identified by Pauley, and adding to this the importance of submitting evidence that support their claims. It will present different scenarios, for example, showing that providers who have more transparency (i.e. submitting more evidence despite the fact they have suffered from various breaches or outages) are, in some cases better than providers that have not submitted any evidence when they have suffered from breaches or outages.



## 7.5.2 Transparency Measurement – Adoption of CSA CCM Framework

With regards to the CSA CCM framework, it consists of 11 control areas that are specifically designed by the CSA. These 11 control areas provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of the cloud provider. Table 34 shows the control groups defined by the CSA, and within each control group there are several control areas.

Table 34. Cloud Controls Matrix - Control Areas

<b>1</b>	<b>Compliance</b>
<b>2</b>	Data Governance
<b>3</b>	Facility Security
<b>4</b>	Human Resources
<b>5</b>	Information Security
<b>6</b>	Legal
<b>7</b>	Operations Management
<b>8</b>	Risk Management
<b>9</b>	Release Management
<b>10</b>	Resiliency
<b>11</b>	Security Architecture

The CAIQ questionnaire consists of 202 questions that are related to the 11 control groups shown in the above Table. In this thesis, some of the questions related to the compliance group are presented in Table 35, in order to provide an example of how transparency measurement is conducted. More information about the control areas that exist within the compliance group, can be found in the Appendix (B.1).

The CSA has inspired other authors [22, 33, 67] to base their work on the solid foundation provided by the CSA. Therefore, the CSA's CCM framework and the CAIQ will be adopted as the foundation here in an attempt to assess and compare different cloud providers' offerings.

Table 35. Control Group (Compliance) – Questions

Control Group	CGID	CID	Consensus Assessment Questions	Comments and Notes
<b>Compliance</b>				
Audit Planning	CO-01	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	
Independent Audits	CO-02	CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?	
		CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly, as prescribed by industry best practices and guidance?	
		CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure, as prescribed by industry best practices and guidance?	
		CO-02.4	Do you conduct internal audits regularly, as prescribed by industry best practices and guidance?	
		CO-02.5	Do you conduct external audits regularly, as prescribed by industry best practices and guidance?	
		CO-02.6	Are the results of the network penetration tests available to tenants at their request?	
		CO-02.7	Are the results of internal and external audits available to tenants at their request?	
Third Party Audits	CO-03	CO-03.1	Do you permit tenants to perform independent vulnerability assessments?	
		CO-03.2	Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?	
Contract/Authority Maintenance	CO-04	CO-04.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	
Information System Regulatory Mapping	CO-05	CO-05.1	Do you have the ability to logically segment or encrypt customer data,so that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	
		CO-05.2	Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?	

## 7.6 Generic Scorecard Template (GST)

A GST has been developed and can be attached to the CAIQ questionnaire. The justification behind the GST is to allow us to measure the transparency of the provider based on the questions presented in the CAIQ. Five attributes have been selected to define the GST. Two of these were selected from the CAIQ questionnaire (response and comments), and the remaining three attributes (support of evidence, publication of evidence and auditing evidence) were defined based on the customers' assurance requirements that were proposed in Chapter 2. The method of measurement is simple, as it is adapted from Pauley's methodology [22].

### 7.6.1 Measurement Attributes of GST

Table 36. Generic Scorecard Template (GST) Attributes

Attributes	Possible Values	Score
Response	1 or 0	<i>[if (Response = Yes) then score = 1, else score = 0]</i>
Comments	1 or 0	<i>[if (explained) then score = 1, else score = 0]</i>
Evidence	1 or 0	<i>[if (provided) then score = 1, else score = 0]</i>
Published	1 or 0	<i>[if (published) then score = 1, else score = 0]</i>
Auditing	1 or 0	<i>[if evidence is up to date then score = 1, else score = 0]</i>

$$\left[ CP_{Transparency} = \frac{Transparency_{CG}}{Number\ of\ CG} * 100 \right] (1)$$

$$\left[ Transparency_{CG} = \frac{Transparency_{CID}}{Number\ of\ CID} * 100 \right] (2)$$

$$\left[ Transparency_{CID} = \frac{CP_{response} + CP_{comment} + CP_{Evidence} + CP_{publis\ hed} + CP_{Auditing}}{Number\ of\ attribute} * 100 \right] (3)$$

***CP<sub>response</sub>*** is the cloud provider's answer to the question, the score assigned to this attribute is either 1 or 0, as explained in Table 34.

***CP<sub>comment</sub>*** is the cloud provider's comment and notes on the answer; the score assigned to this attribute is either 1 or 0. It will be assigned a 0 if the provider does not provide information regarding their answer.

***CP<sub>evidence</sub>*** is the cloud provider's evidence that is presented; this evidence is in the form of document that might be a certification, standard, policy, procedure or service level agreement. The more evidence provided by the provider the better it will compare with other providers.

***CP<sub>Auditing</sub>*** The cloud provider should always maintain valid evidence by keeping it up-to-date as documents such as certifications have expiration dates, therefore, it is important to maintain its validity.

A trusted third party, professional security personnel, or a trusted auditor can evaluate the quality and existence of evidence. For example, when a provider answer a question and write his comment. The comment field will be checked and validated by a trusted third party organization or professional security personnel. The CSA organization used this approach of validation to check each provider's entry.

The evidence can be submitted by the provider in a form of WebLink that refers the customer to it or it could be a certificate that is obtained from authorised certifications bodies such as SAS70, ISO, CCSK, etc.

## 7.6.2 Example of Measurement

This section conducts an example showing how cloud providers' transparency is measured. There are currently 96 entries in the CSA STAR registry [115]. In order to show consistency in the comparison of the results, cloud providers offering a similar delivery of service will be selected. For example, cloud providers who provide IaaS will only be compared against others who do so. The cloud providers will be selected from the CSA STAR registry as it has realistic data. The selected providers are described in Table 37.

Table 37. Example of IaaS Providers

	<b>Provider</b>	<b>Reference</b>	<b>Delivery Model</b>
1	CloudSigma AG	[102]	IaaS
2	Terremark	[103]	IaaS
3	Windows Azure	[104]	IaaS

Table 38. Example of Transparency Measurement - Cloud Provider 1

<b>Cloud Provider 1</b>	<b>Compliance</b>			<b>Score</b>	<b>17.5%</b>
CO-01.1: Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	Response	Yes	1	CO-01.1 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.1: Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?	Response	Yes	1	CO-02.1 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.2: Do you conduct network penetration tests of your cloud service infrastructure regularly, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.2 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.03: Do you conduct regular application penetration tests of your cloud infrastructure, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.3 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.04: Do you conduct internal audits regularly, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.4 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.05: Do you conduct external audits regularly, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.5 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.06: Are the results of the network penetration tests available to tenants at their request?	Response	Yes	1	CO-02.6 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.07: Are the results of internal and external audits available to tenants at their request?	Response	Yes	1	CO-02.7 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-03.01: Do you permit tenants to perform independent vulnerability assessments?	Response	Yes	1	CO-03.1 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-03.02: Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?	Response	Yes	1	CO-03.2 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-04.01: Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Response	Yes	1	CO-04.1 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		

CO-05.01: Do you have the ability to logically segment or encrypt customer data sothat data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Response Comments Evidence Published Auditing	Yes No No No No	1 0 0 0 0	CO-05.1 Score	0.20
CO-05.02: Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?	Response Comments Evidence Published Auditing	Yes No No No No	1 0 0 0 0	CO-05.2 Score	0.20
CO-06.01: Do you have policies and procedures in place describing what controls you have in place to protect tenants' intellectual property?	Response Comments Evidence Published Auditing	Yes No No No No	1 0 0 0 0	CO-06.1 Score	0.20
CO-06.02: If utilization of tenants' services housed in the cloud is mined for cloud provider benefit, are the tenants' IP rights preserved?	Response Comments Evidence Published Auditing	No No No No No	0 0 0 0 0	CO-06.2 Score	0
CO-06.03: If utilization of tenants' services housed in the cloud is mined for cloud provider benefit, do you provide tenants with the ability to opt-out?	Response Comments Evidence Published Auditing	No No No No No	0 0 0 0 0	CO-06.3 Score	0

The compliance results for cloud provider 2 are shown below.

Table 39. Example of Transparency Measurement - Cloud Provider 2

<b>Cloud Provider 2</b>	<b>Compliance</b>			<b>Score</b>	<b>26.25%</b>
CO-01.1: Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	Response	Yes	1	CO-01.1 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.1: Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?	Response	Yes	1	CO-02.1 Score	0.40
	Comments	Yes	1		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.2: Do you conduct network penetration tests of your cloud service infrastructure regularly, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.2 Score	0.40
	Comments	Yes	1		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.03: Do you conduct regular application penetration tests of your cloud infrastructure, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.3 Score	0.40
	Comments	Yes	1		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.04: Do you conduct internal audits regularly, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.4 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.05: Do you conduct external audits regularly, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.5 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.06: Are the results of the network penetration tests available to tenants at their request?	Response	No	0	CO-02.6 Score	0.20
	Comments	Yes	1		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-02.07: Are the results of internal and external audits available to tenants at their request?	Response	Yes	1	CO-02.7 Score	0.40
	Comments	Yes	1		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-03.01: Do you permit tenants to perform independent vulnerability assessments?	Response	Yes	1	CO-03.1 Score	0.40
	Comments	Yes	1		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-03.02: Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?	Response	Yes	1	CO-03.2 Score	0.20
	Comments	No	0		
	Evidence	No	0		
	Published	No	0		
	Auditing	No	0		
CO-04.01: Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate	Response	Yes	1	CO-04.1 Score	0.20
	Comments	No	0		
	Evidence	No	0		



regulations?	Published Auditing	No No	0 0		
CO-05.01: Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Response Comments Evidence Published Auditing	Yes No No No No	1 0 0 0 0	CO-05.1 Score	0.20
CO-05.02: Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?	Response Comments Evidence Published Auditing	Yes No No No No	1 0 0 0 0	CO-05.2 Score	0.20
CO-06.01: Do you have policies and procedures in place describing what controls you have in place to protect tenants' intellectual property?	Response Comments Evidence Published Auditing	Yes No No No No	1 0 0 0 0	CO-06.1 Score	0.20
CO-06.02: If utilization of tenants' services housed in the cloud is mined for cloud provider benefit, are the tenants' IP rights preserved?	Response Comments Evidence Published Auditing	Yes No No No No	1 0 0 0 0	CO-06.2 Score	0.20
CO-06.03: If utilization of tenants' services housed in the cloud is mined for cloud provider benefit, do you provide tenants with the ability to opt-out?	Response Comments Evidence Published Auditing	Yes No No No No	1 0 0 0 0	CO-06.3 Score	0.20

Table 38 shows cloud provider 3's transparency measurement score.

Table 40. Example of Transparency Measurement - Cloud Provider 3

<b>Cloud Provider 3</b>	<b>Compliance</b>			<b>Score</b>	<b>78.75%</b>
CO-01.1: Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	Response	Yes	1	CO-01.1 Score	1
	Comments	Yes	1		
	Evidence	Yes	1		
	Published	Yes	1		
	Auditing	Yes	1		
CO-02.1: Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?	Response	Yes	1	CO-02.1 Score	0.80
	Comments	Yes	1		
	Evidence	Yes	1		
	Published	No	1		
	Auditing	Yes	1		
CO-02.2: Do you conduct network penetration tests of your cloud service infrastructure regularly, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.2 Score	0.80
	Comments	Yes	1		
	Evidence	Yes	1		
	Published	No	0		
	Auditing	Yes	1		
CO-02.03: Do you conduct regular application penetration tests of your cloud infrastructure, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.3 Score	0.80
	Comments	Yes	1		
	Evidence	Yes	1		
	Published	No	0		
	Auditing	Yes	1		
CO-02.04: Do you conduct internal audits regularly, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.4 Score	0.80
	Comments	Yes	1		
	Evidence	Yes	1		
	Published	No	0		
	Auditing	Yes	1		
CO-02.05: Do you conduct external audits regularly, as prescribed by industry best practices and guidance?	Response	Yes	1	CO-02.5 Score	0.80
	Comments	Yes	1		
	Evidence	Yes	1		
	Published	No	0		
	Auditing	Yes	1		
CO-02.06: Are the results of the network penetration tests available to tenants at their request?	Response	Yes	1	CO-02.6 Score	0.80
	Comments	Yes	1		
	Evidence	Yes	1		
	Published	No	0		
	Auditing	Yes	1		
CO-02.07: Are the results of internal and external audits available to tenants at their request?	Response	Yes	1	CO-02.7 Score	0.80
	Comments	Yes	1		
	Evidence	Yes	1		
	Published	No	0		
	Auditing	Yes	1		
CO-03.01: Do you permit tenants to perform independent vulnerability assessments?	Response	Yes	1	CO-03.1 Score	0.60
	Comments	Yes	1		
	Evidence	Yes	1		
	Published	No	0		
	Auditing	No	0		
CO-03.02: Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?	Response	Yes	1	CO-03.2 Score	0.60
	Comments	Yes	1		
	Evidence	Yes	1		
	Published	No	0		
	Auditing	No	0		
CO-04.01: Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate	Response	Yes	1	CO-04.1 Score	0.80
	Comments	Yes	1		
	Evidence	Yes	1		

regulations?	Published Auditing	No Yes	0 1		
CO-05.01: Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Response Comments Evidence Published Auditing	Yes Yes Yes No Yes	1 1 1 0 1	CO-05.1 Score	0.80
CO-05.02: Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?	Response Comments Evidence Published Auditing	Yes Yes Yes No Yes	1 1 1 0 1	CO-05.2 Score	0.80
CO-06.01: Do you have policies and procedures in place describing what controls you have in place to protect tenants' intellectual property?	Response Comments Evidence Published Auditing	Yes Yes Yes No Yes	1 1 1 0 1	CO-06.1 Score	0.80
CO-06.02: If utilization of tenants' services housed in the cloud is mined for cloud provider benefit, are the tenants' IP rights preserved?	Response Comments Evidence Published Auditing	Yes Yes Yes No Yes	1 1 1 0 1	CO-06.2 Score	0.80
CO-06.03: If utilization of tenants' services housed in the cloud is mined for cloud provider benefit, do you provide tenants with the ability to opt-out?	Response Comments Evidence Published Auditing	Yes Yes Yes No Yes	1 1 1 0 1	CO-06.3 Score	0.80

## Chapter 8: Towards the Evaluation of CloudAdvisor

### 8.1 Introduction

The CloudAdvisor framework described in Chapter 7 is proposed as a possible solution that aims to encourage and promote transparency in the cloud computing offerings of different providers, and providing a tool to support decision-making that balances security with transparency (something that providers and customers are keen to achieve). This chapter concerns the evaluation of the CloudAdvisor framework. The assessment of the extent to which the framework meets the goals set out in Chapter 7 is a challenge because we need to address the following important questions:

- How can customers trust that the security controls are satisfied, as claimed by the providers, and are compliant with consumers' requirements?
- If the customer chooses the best cloud provider based on the risk assessment profile that is gained from the CloudAdvisor, how can the claims of the cloud provider's transparency continue to be monitored after the customer has committed to the provider?

We therefore begin by evaluating CloudAdvisor's parameters in Section 8.2. Section 8.3, sets out the evaluation criteria and requirements for the CloudAdvisor framework, explaining the importance of each requirement. After that, possible evaluation techniques – specifically questionnaire-based and simulation-based approaches are discussed in Section 8.4. A comparison between the evaluation techniques is conducted in Section 8.5 using an “evaluation criteria matrix” where it will show how each evaluation technique is compliant to the evaluation requirements, considering the advantages and risks of each evaluation approach. In Section 8.6, the selection of the evaluation technique is made and justified. Finally, Section 8.7 will present and discuss Simulation results.

## 8.2 Evaluation of CloudAdvisor Parameters

In this section, we will evaluate the importance of trustworthiness parameters that are previously presented in Table 31 in Section 7.5.1 and that the CloudAdvisor will use them.

Trust and reputation systems have been regarded as an important role in decision making in the internet world [128]. Thus, considering trustworthiness as one of the criteria's of evaluation is important. Transparency has been also taken into consideration as important criteria in evaluating providers because it acts as a reflection mechanism by assisting potential cloud customers in revealing the strengths and weakness of the provider before they commit to any contractual agreement [133].

Several parameters such as security, privacy, outages and data loss have been identified from the literature that are considered important to include when evaluating cloud provider's trustworthiness. Those parameters have been selected because few articles have focused on the security aspect of cloud providers [47]. In addition, security and availability were selected as one of the parameters in assessing trust in cloud computing [25, 129].

Other parameters such as the years in business that the cloud provider has been in and if he is a member of well established cloud computing groups such as CSA, ENISA and CloudAudit. Asking cloud provider how long has it been in business is very important as it has been one of most important criteria when evaluating cloud providers [22, 130]. Gartner has also emphasized that business continuity is one of the top 7 security risks in cloud computing [44]. The idea of these groups is to promote the use of best practices for providing security assurance within cloud computing. For example, CSA organization has now 188 members of cloud providers [131].

The parameters have been also used to measure the overall trustworthiness of cloud providers. For example, the provider is entitled to report to the cloud customer about any security incident that might put the customers in risk. As collaboration between the cloud customer and provider in order to identify and respond to incidents related to security and privacy in cloud computing is important [132]. The transparency is also measured in order to know whether cloud providers are being

honest in providing legitimate information about the incidents they have encountered. This is mainly done by dividing the number of reported incidents (i.e. evidence of publication) by the total number of incidents as presented in Table 29.

### **8.3 Evaluation Criteria and Requirements**

Although the several frameworks that exist in the market are created mainly to help customers select a provider that best meets their business requirements, to the best of our knowledge there is no work that has considered evaluating them. Most of the transparency frameworks such as Cloud Provider Transparency Scorecard (CPTS) and Security Compliance Assessment (SCA) were developed based on the best security industry standards that exist in the Cloud Controls Matrix (CCM) framework. The selection of a provider is made even more difficult by the fact that there are thousands of providers competing in the market. This implies that participation in an evaluation mechanism should be at reasonable cost in terms of effort, both to the service provider and to the potential customer.

In order to construct an evaluation mechanism for CloudAdvisor, supporting comparison against existing frameworks, we propose both criteria against which frameworks should be evaluated, and requirements on the evaluation mechanism itself. The latter are required because any mechanism for assessing a transparency framework should be capable of being deployed in practice, and so should be affordable both to providers and customers in terms of the resource required to perform an evaluation.

We first identify criteria that should be included in the evaluation of a transparency and trustworthiness framework. We present each of these as questions:

#### **1. Does the framework permit the assessment (e.g., by giving a score) of the trustworthiness of providers?**

In each framework, we will examine its capability to measure the provider's trustworthiness based on a set of attributes defined by Pauley and augmented in this thesis that could be bring assurance to the customer. It includes questions that are articulated around the following attributes: years in business, history of breaches, outages, data loss and membership of relevant professional organisations. A "years in business" factor provides a rough assessment of the provider's success as mentioned in Chapter 7 [22]. The history of

breaches has been regarded as one of the important factors when it comes to the selection of the provider. The customer could be able to know when was the last time the provider has experienced a security or privacy breach [15]. Being a member of an official body in cloud computing could bring more assurance to the customer. This could be achieved by obtaining for example, a certificate of membership from an official organization; the certificate can be regarded as a trust metric, which in return could foster customer's confidence [11].

## **2. Does the framework permit the assessment (e.g., by giving a score) to the transparency of providers?**

For each provider providing evidence that support claims about trustworthiness or transparency will provide assurance to the customer. Bhensook [22] emphasized the need for evidence which confirms to the customer that providers are performing customer's requirements as expected. Therefore, which framework of transparency will be able to fulfil this requirement is important. An evidence score for trustworthiness and transparency should be calculated and assigned for each provider.

## **3. Does the framework allow evidence about providers' trustworthiness and transparency to be taken into account?**

If each cloud provider presents evidence that support its claims then it will result in assuring the customer. Bhensook [22] emphasised the need for evidence, which confirms to the customer that providers are performing their requirements as expected. Therefore, it is important to determine which transparency framework fulfils this requirement. An evidence score for trustworthiness and transparency is calculated and assigned for each provider.

## **4. Does the framework support monitoring the honesty of providers?**

Honesty has been regarded as one of the three trusting belief attributes [23]. Therefore, it is not sufficient to know that the provider has submitted evidence that support his claims of transparency and trustworthiness: evidence for the transparency requirement should be up-to-date. For example, if the evidence provided is a certification, then the certificate should not have expired.

## **5. Does the framework perform a comparison between providers' offerings?**

Selecting the right provider is an important requirement for the customer. Therefore, examining which transparency framework will help the customer in performing a comparison among several providers is an evaluation requirement.

## **6. Does the framework allow the assessment of the extent of adoption of the Cloud Controls Matrix industry standard?**

The CCM framework has been considered the base for the proposed CloudAdvisor, and most other transparency frameworks, such as SCA, and to some extent the CPTS. This is due to the global acceptance of best industry standards. Therefore, examining which model of transparency has, or has not, adopted the CCM framework will be considered as evaluation criteria.

## **7. Does the framework support customers in making a sound selection of provider?**

Customers need assurance from providers that they follow sound security practices to mitigate the risks that face both customers and providers. Obtaining this assurance will help customers to make informed decisions when or before selecting the provider. Therefore, examining which of the transparency frameworks has, or has not, fulfilled this requirement is considered in the evaluation process.

We also identify requirements that the evaluation approach itself should satisfy in order to be usable to both providers and customers:

## **8. Does participation in the evaluation impose a tolerable burden on providers?**

One of the recommendations that ENISA have put forward emphasizes the need to reduce the assurance burden on the provider. This can be achieved by providing customers or auditors with a number of relevant and common questions that would not compromise providers' infrastructures security and not overwhelm them with unnecessary questions. In order to fulfil this requirement a CAIQ questionnaire developed by the CSA defines a set of questions that any customer or auditor might like to ask the provider. The concept behind CAIQ is that it documents a cloud provider's security controls in each layer of the cloud



delivery models (i.e., SaaS, PaaS and IaaS). Moreover, it also assesses the cloud computing offerings provided by the providers and assures security control transparency [31].

**9. Does the evaluation mechanism support comparison between different transparency frameworks?**

Being able to compare between different frameworks of transparency is an advantage for the customer as they will be able to evaluate each model and know each one's weakness and strengths. In addition, it will help us to improve the proposed model (i.e., CloudAdvisor) if there are other properties that need to be added or omitted. Therefore, knowing which evaluation technique will fulfil this requirement is a must. The three transparency frameworks considered in the evaluation process are CloudAdvisor, CPTS and SCA.

**10. Does the evaluation mechanism allow the comparative assessment of frameworks by means of user-relevant scenarios?**

Customers would like to select a trustworthy and transparent cloud provider that is verified by means of evidence. In addition, they want to be able to monitor the cloud provider's honesty by ensuring that cloud providers' evidence is up-to-date. In this requirement we need the customer to have the option of testing the various scenarios of the cloud provider. For more details, cloud providers' scenarios are described in Section 8.3.2. Therefore, choosing the evaluation technique that will help us achieving the above requirement is very important.

**11. Does the mechanism allow evaluations to be conducted at reasonable cost?**

We proposed two evaluation mechanisms (i.e., questionnaire-based and simulation-based) in Section 8.4 for evaluating CloudAdvisor. It is important to decide which evaluation method is better than the other in terms of satisfying the abovementioned criteria numbered (1 to 7), the requirements numbered (8 to 11), and more importantly the time and resources needed to conduct the evaluation. Therefore, this requirement has taken into consideration discussing the advantages and disadvantages of the evaluation methods (see Section 8.4.1 and 8.4.2) and selecting the evaluation method that has less cost in time and resources.

## **8.4 Possible Evaluation Techniques**

This section explains two possible evaluation techniques that can be used to evaluate the CloudAdvisor. First, the questionnaire-based approach is discussed in Section 8.4.1. Then, we explain the simulation-based analysis approach in Section 8.4.2.

### **8.4.1 Questionnaire-based Survey**

First of all, in order to make the evaluation process feasible, a web application should be developed that provides customers and service providers with away to experiment with the CloudAdvisor. The concept behind the CloudAdvisor is to help customers to find the most convenient service provider, in terms of a set of attributes such as trustworthiness and transparency, and in addition to be able to compare between different providers. Following this, a survey questionnaire is developed and distributed to customers across different sectors from academia, telecommunications, education, IT companies, banks and governments.

The advantages of this approach are that we obtain real data being provided from the provider and fed to the CloudAdvisor platform. In addition, the customers will have the opportunity to experiment with it. They will be able to search for the best trustworthy and transparent provider. Moreover, avoiding the provider who has the least score in either trustworthiness or transparency or both. Another benefit of building the CloudAdvisor is that it will always provide the customer with updated information about the providers. In other words, the customer will be able to receive notifications of change from the provider from time to time. For instance, if a provider was able to provide evidence that support claims of either transparency or trustworthiness, then the evidence will increase the provider's score and it will be reflected on the overall score. This will certainly be important for the customer.

In order to evaluate the CloudAdvisor effectively, it is recommended to have a good number of participants for both provider and customers to evaluate it against other the methods. From the customers' evaluation point of view, they will have to evaluate the CloudAdvisor against the CPTS and the SCA. The criteria of evaluation stipulate that the method will support trustworthiness measurement, transparency measurement, evidence, an up-to-date evidence and systematic comparison between provider's offerings. However due to the limitation of time and the substantial number of potential providers taking part, this approach does not satisfy requirement 11.

### 8.4.2 Simulation-Based Analysis

Simulation is defined as “the imitation of the operation of a real-world process or system over time” [105]. In this alternative evaluation approach, a simulation-based analysis is proposed in order to permit comparison between CloudAdvisor, the CPTS, and the SCA. The aim of the comparison would be to evaluate each model’s capability in answering the questions presented in Section 8.3. Table 41 shows the evaluation matrix that can be used to conduct a comparison between the CloudAdvisor, CPTS, and SCA in terms of satisfying the criteria

Table 41. CloudAdvisor Evaluation Matrix

Model	Comparison Criteria				
	Trustworthiness	Transparency	Evidence	Evidence up-to-date	Providers’ comparison
CloudAdvisor					
CPTS					
SCA					

The workflow, presented in Figure 55, describes how the evaluation would be conducted when running the simulation. The simulator consists of six components, which are:

1. Generation of cloud service providers
2. Data Generation
3. Scoring Engine
4. Reporting Results
5. Evaluating Results

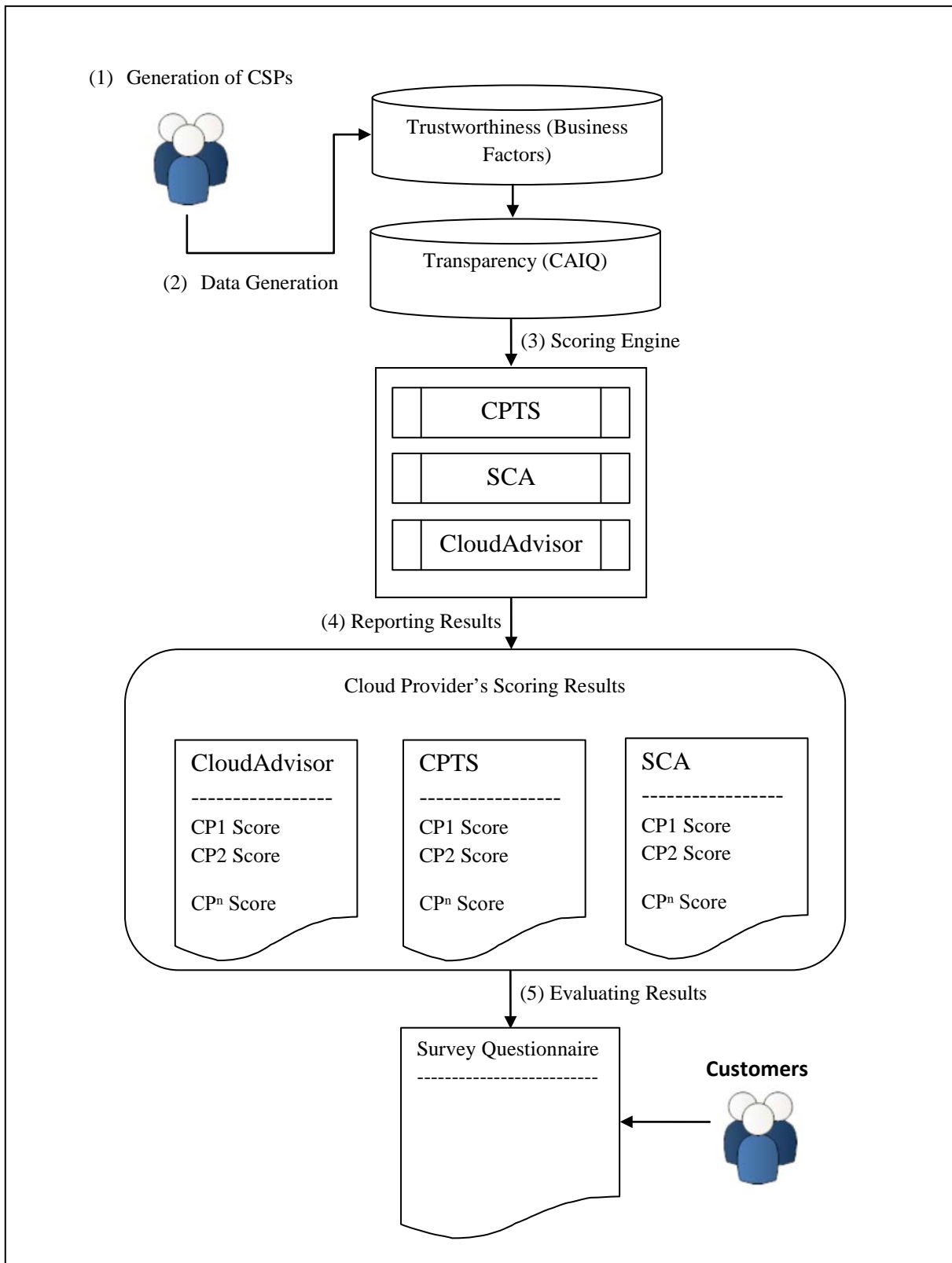


Fig.55. CloudAdvisor evaluation - simulation-based analysis approach.

We explain each of these components in greater detail below.

#### 1. Generating Cloud Service Providers

When the participant (i.e. potential customer) who wishes to evaluate the CloudAdvisor against other frameworks runs the simulator, the participant will be able either to select the number of CSPs that will be included in the comparative analysis study or simply by generating the number of CSPs randomly using a random function. When the CSPs are generated they will be initialized with brief information related to the provider's cloud offering type such as the delivery models (i.e. IaaS, PaaS, and SaaS) and the deployment models for delivering the services, which include public, private or hybrid clouds.

#### 2. Generating Cloud Service Providers Data

This component is responsible of generating random data for each CSP. The CSP is entitled to data that represent the CSP's trustworthiness and transparency. The trustworthiness data are articulated around factors which will help the customer to know the business and security history of the CSP, including includes years in business, membership, security and privacy breaches, outages and data losses.

Data relating to transparency exists in the CAIQ questionnaire that has been developed by the CSA, where a CSP should answer over 140 questions that are related to 11 control areas that exist in the CCM framework and are displayed in the CAIQ template. The CSP has been given the choice to participate in submitting data to support claims of compliance in these control areas. The control areas have been considered and chosen as the basis for transparency's compliance because they have been regarded as best security practices. This is very important for the CSP in order to provide assurance to the customer.

After all data is generated for each CSP, it will be disseminated to the scoring engine where it will calculates the CSP's scores based on the three frameworks CloudAdvisor, CPTS and SCA. It will evaluate each framework's capability of measuring the CSP's trustworthiness and transparency, provision of evidence that supports CSP's claims of trustworthiness and transparency and monitoring the evidence is kept up-to-date.

When the simulator is run by the participant a random integer is generated to represent the number of CSPs that their trustworthiness and transparency will be calculated and compared using the three different frameworks (i.e., CloudAdvisor, CPTS and SCA). The first data that will be generated for the CSP concerns the trustworthiness which includes the years that a CSP has been in business, the histories of breaches affecting security and privacy, outages and data loss that occurred intentionally or accidentally, and the CSP's membership of any relevant cloud computing group. The data is based on questions that will be displayed on the simulation window were the participant will also be able to observe the CSP's answers that are generated randomly. This permits the exploration of the various scenario results that are described later in the scoring engine component. The types of generated data are as follows:

- **Years in Business**

We define  $n$  as a random integer number generated to represent the number of years that the cloud service provider has been in business. Where  $n$  should be in the following range:

$$(n \geq 5 \text{ or } n < 5)$$

- **Security Breach**

We define  $ns$  as the number of security breach incidents that the provider has suffered from.

$$\text{if } ns > 0, es \geq 0$$

Where  $es$  is a generated integer number that represents the amount of evidence provided by the cloud service provider that supports its claims.

- **Privacy Breach**

We define  $np$  as the number of privacy breaches that the cloud service provider has suffered from.

$$\text{if } np > 0, ep \geq 0$$

Where  $ep$  is a generated integer number that represents the amount of evidence provided by the cloud service provider to support its claims.

- **Outages**

We define  $o$  as the number of outages that the cloud service provider has suffered from.

$$\text{if } o > 0, eo \geq 0$$

Where  $eo$  is a generated integer number that represents the amount of evidence provided by the cloud service provider to support its claims.

- **DataLoss**

We defined  $dl$  as the number of data loss incidents that the cloud service provider has suffered from.

$$\text{if } dl > 0, edl \geq 0$$

Where  $edl$  is a generated integer number that represents the number of units of evidence provided by the cloud service provider to support its claims.

- **Membership**

We define  $m$  as the number of memberships that the cloud service provider has.

$$if\ m > 0, em \geq 0$$

Where  $em$  is a generated integer number that represents the number of evidence provided by the cloud service provider to support its claims.

After simulating the entry of the trustworthiness data, the second type of data that will be simulated is the transparency data of the cloud service provider. The transparency data are based on the CAIQ template developed by the CSA, where over 140 questions are presented to the cloud service provider to be answered. As part of the simulation, these questions will be displayed to the participant once the trustworthiness data are finalized and calculated to obtain the scores for the participating cloud service providers. The nature of the transparency data will be treated similarly to the trustworthiness data. First of all, the transparency should be measured in accordance to the CCM Control Area, starting with the compliance control and finishing with the security architecture control. For each control area, a set of questions based in a text format will be displayed to the participant. Then, a set of attributes (the first four attributes that were previously defined in Chapter 7) will be aligned to each control area that needs to be provided with answers. These attributes are:

- Providers' response to the question
- Providers' comments on the question
- Providers' provision of evidence
- Status of the evidence
- Weight of control area

The last attribute, the weight of the control area, could be either simulated or entered by the participant, in order to observe how the providers' scores can vary. Since we are considering the assessment of the cloud provider's trustworthiness, Alhamad [106] suggests that the customers could have a choice of entering the weights of each factor, or of leaving them the choice of not to do so, as they could be generated automatically and equally assigned by the simulation. For instance, a customer might be interested in the information security control area more than any other control areas whereas some might see the legal control area as being very important depending on their business requirements. The



participant in the simulation will have no control over these attributes. Their data are generated automatically, except for setting the weights of control areas, which can be either simulated or entered by the participant.

### 3. Scoring Engine

This component is vitally important to allow the customer to compare the cloud service providers' scores, as well as to the provider where the scores will be computed for each cloud service provider. Comparison between cloud service providers will create a competitive environment among them. The scoring engine will automatically receive the data from the previous component (i.e. data dissemination) in order to calculate the scores of trustworthiness, transparency, evidence and evidence up-to-date for the number of cloud service providers that has been generated by the simulator. Based on the characteristics of each model, various scores will be displayed to the customer and explained. The various results will depend on the data that has been generated. Therefore, the customer can see different scenarios within the simulation. The several scenarios of the cloud service provider that the customer could encounter are:

- Trusted cloud provider but not verified
- Trusted and verified cloud provider
- Transparent but not verified
- Transparent and verified cloud provider
- Not Trustworthy and not transparent
- Cloud provider honesty is Verified or Not Verified

The aim is to assess which of the three frameworks (CloudAdvisor, CPTS and SCA) satisfies the requirements that are articulated in Section 8.2. A workflow has been designed to explain the different scenarios that the customer will see based on the generated data. Therefore, various scenarios will be developed in order to test the workflow and to provide the customer with the results of each model. In this section, multiple scenarios for the assessment of the cloud service providers, based on the three frameworks, will be applied to the simulator. It will start by generating random data to test the three stages of the workflow, which are the trustworthiness assessment phase, transparency assessment and evidence assessment by insuring the evidence is up-to-date.

## **Scenario 1 – Trustworthiness Assessment Phase**

In the first scenario the customer needs to examine three cases: (1) if the cloud service provider is trustworthy, (2) if it has been verified or not and (3) checking the cloud service provider's honesty. The last case is important if, for instance, the cloud service provider is deemed to be trustworthy and verified by the evidence that it provided. The validation of the evidence should be examined in a timely manner because some forms of evidence can expire. There are three possible cases that will be drawn here from the simulator. The first concludes that a cloud service provider is trustworthy; however, it fails verification because of the lack of the evidence needed to increase the customer confidence. In the second case, the customer could be lucky finding a trustworthy and verified cloud service provider. When comparing between various cloud service providers, the customer would prefer the one that is trusted and has been verified by some evidence. The framework that could support this desired deliverable would prevail against the others. Therefore, a comparison between the CloudAdvisor, CPTS and the SCA is vitally important to know which model will deliver a trustworthy and verified cloud service provider to the customer. It is worth noting that checking the honesty of the cloud service provider is applied to each stage of the workflow because it is not sufficient to know that it is trustworthy and transparent but it is of equivalent importance to preserve those features, as long as evidence is updated within time.

## **Scenario 2 – Transparency Assessment Phase**

In this scenario, after completing the first phase, the customer is keen to know more about the cloud service provider with regards to its transparency (reporting to the customer). The cloud service provider will be compared with others in terms of their transparency. As it has been mentioned in the previous chapter, the cloud service providers' transparency is measured based on the CCM and the questions gained from the CAIQ. In this stage, there are also three possible cases that the customer will encounter. The first, (1) Transparent Cloud Service Provider, (2) Verified or not, and (3) the honesty of the Cloud Service Provider's Transparency.

For the first case, the cloud service provider's transparency is measured and compared against other cloud service providers. This means the cloud service provider is indeed being transparent to the customers' security requirements; however, without any proof this should

indicate that the cloud service provider is not verified as evidence is very important to support its claims of transparency. Therefore, the cloud service provider is instigated to provide evidence that supports its claims of transparency. Without evidence the customer will conclude that this cloud service provider is transparent but it has failed the verification process. Being flexible is also an important feature that should be included in any system, therefore, from the CloudAdvisor and the SCA point of view, they support providing evidence at any time, which will reflect on the cloud service providers' results. The last case, which will continue to be considered as a recursive function, is the need to check when evidence is about to expire. Checking the honesty of the cloud service providers' transparency is vitally important because of the customer's dependence on them to ensure that their security requirements are up-to-date. Having explained all the three cases, this will be a major benefit to the customer to know which delivery model of the CloudAdvisor, CPTS and the SCA best serves them. The customer will be able to see which one has best helped them in evaluating the transparency of cloud service providers.

### Scenario 3 – Evidence Assessment Phase

The last scenario will always check for the honesty of the cloud service provider. Two possible scenarios can be drawn from the simulation results. The first is that the cloud service provider has failed to maintain its honesty in terms of providing up-to-date evidence of either trustworthiness or transparency; in this case it shall be regarded as a Not Verified CSP. Whereas, the second scenario is having a trusted and transparent cloud service provider whose honesty has been verified.

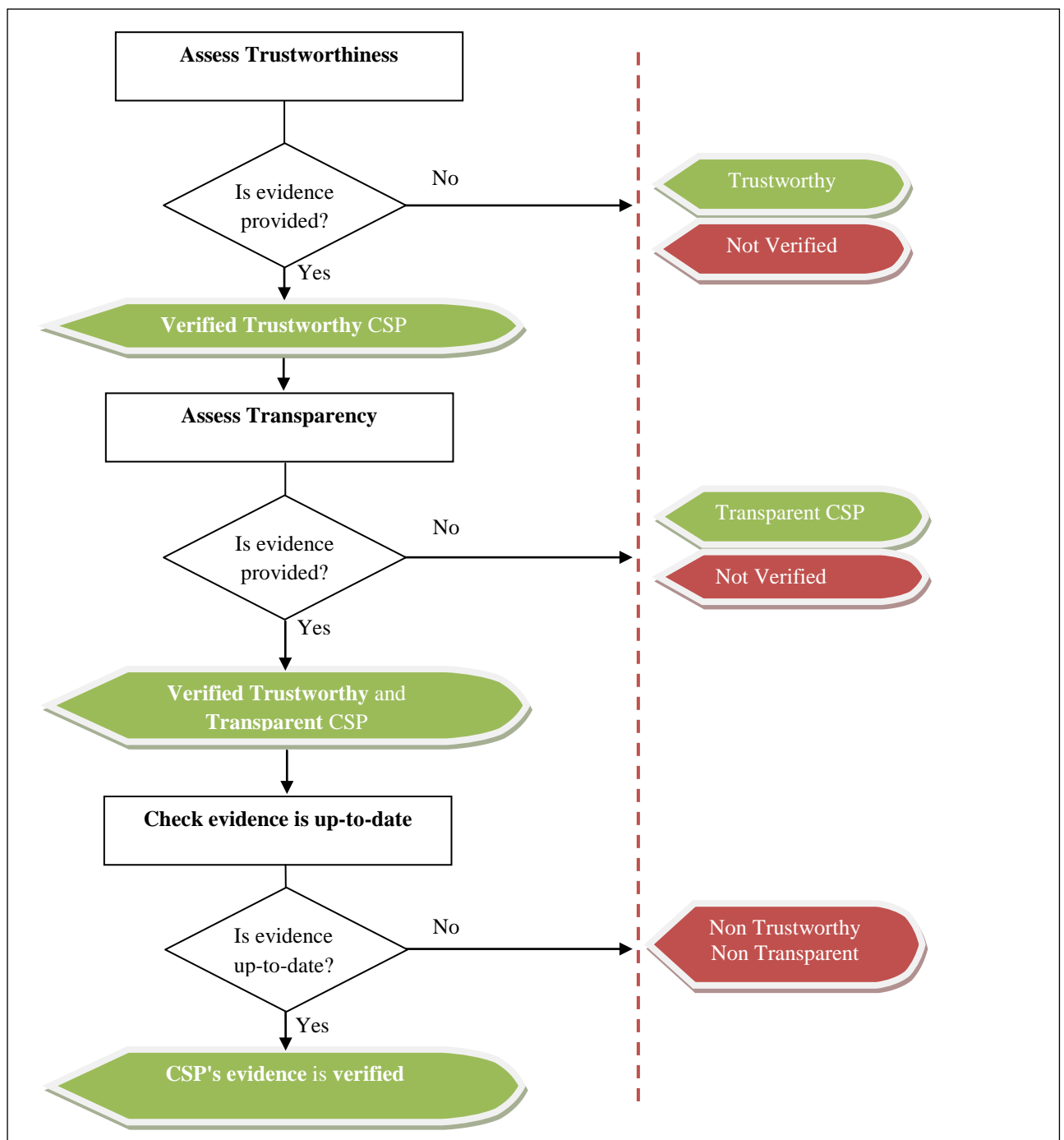


Fig.56. Scenarios for cloud provider assessment.

4. Reporting the Results: Displaying the results to the customer can be regarded as a transparent relationship. In other words, the cloud service provider should make a simple communication to the customer, displaying all the necessary information that has been gathered by the simulation. This will achieve the definition and objective of transparency. Since there are three different frameworks, the three different results will be presented to the customer from the scoring engine on the simulator screen. In addition, it will help to accomplish the main objective, which is the customers' evaluation of the results.

#### 5. Evaluating the Results

The type of evaluation that has been considered is to develop a short survey questionnaire that will ask the participant questions to evaluate the proposed solution (i.e. CloudAdvisor) against the other frameworks, namely CPTS and SCA. The survey questionnaire aims to answer the following questions and the design of the survey questionnaire is described in Appendix A.

## 8.5 Comparison of Evaluation Techniques

In the following Table, we present the possible evaluation techniques and the criteria of selection based on the defined evaluation requirements in Section 8.3. Then, we present the advantages and disadvantages of each technique according to the predefined evaluation requirements. Last but not least, it presents the selection of the evaluation technique, stating the risks associated with it, and the possible options to mitigate these risks.

Table 42. Comparison Between Evaluation Techniques

Evaluation Technique	Requirements										
	1	2	3	4	5	6	7	8	9	10	11
Questionnaire-based	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
Simulation-based	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓

1. Does the framework permit the assessment (e.g., by giving a score) of the trustworthiness of providers?
2. Does the framework permit the assessment (e.g., by giving a score) to the transparency of providers?
3. Does the framework allow evidence about providers' trustworthiness and transparency to be taken into account?
4. Does the framework support monitoring the honesty of providers?
5. Does the framework perform a comparison between providers' offerings?
6. Does the framework allow the assessment of the extent of adoption of the Cloud Controls Matrix industry standard?
7. Does the framework support customers in making a sound selection of provider?
8. Does participation in the evaluation impose a tolerable burden on providers?
9. Does the evaluation mechanism support comparison between different transparency frameworks?
10. Does the evaluation mechanism allow the comparative assessment of frameworks by means of user-relevant scenarios?
11. Does the mechanism allow evaluations to be conducted at reasonable cost?

Before any selection of the evaluation technique is made, we will explain each evaluation technique in terms of meeting the above requirements. Moreover, the advantages and the risks associated with each approach will be presented followed by discussion of how the risks will be mitigated.

### 8.5.1 Evaluation of Questionnaire-based approach

- **Advantages and Risks**

By using the questionnaire-based approach the customer will be able to use the CloudAdvisor platform, which will require the engagement of providers to offer information to the customers. From the customers' point of view, they will be able to obtain scores for both trustworthiness and transparency while also performing comparisons between different cloud computing offerings. The CloudAdvisor platform will support providers by allowing them to submit credible evidence. Customers will have the advantage of monitoring the honesty of the providers. In this approach cloud providers are entitled to submit their entry so their scores can be computed and displayed to the customers. However, this method is very expensive, in terms of time, where several cloud providers need to use the CloudAdvisor platform. When the customers finish using the CloudAdvisor they will be invited to participate in a survey questionnaire, in order to evaluate the CloudAdvisor platform. The benefit of this approach is that customers will be able to make better-informed decisions.

However, there are other risks associated with a questionnaire-based approach. Adopting this method is very expensive, in terms of time, because customers will not be able to participate in the survey questionnaire until all the invited providers have accepted the invitation and started to submit their data to the CloudAdvisor platform. Moreover, this approach will require considerable time from the provider to complete the data, especially as over 140 questions from the CAIQ need to be answered, and this is only from one provider. The questionnaire-based approach will not cover some requirements that we believe are important. These include the exploration of the various scenario results from the cloud provider. In addition, to be able to compare between the three frameworks of transparency, in terms of meeting the following requirements: measuring the trustworthiness, measuring the transparency, support of evidence and computing evidence score and monitoring the evidence is kept up-to-date.

## 8.5.2 Evaluation of Simulation-based approach

- **Advantages and Risks**

This approach is proposed in order to mitigate the risks associated with the questionnaire-based approach. There are several advantages shared between the simulation-based and questionnaire-based approaches. The common advantages are:

- The ability to measure the providers' trustworthiness and transparency
- The provision of supporting evidence that gives assurance to customers
- Monitoring the honesty of the providers by keeping the evidence up-to-date, which will also foster assurance
- The capability of performing a comparison between providers' offerings, which will facilitate the process of provider's selection.
- In addition, the adoption of CCM framework as best industry standards.

There are distinctive advantages that make the simulation-based approach win over the questionnaire-based approach. These advantages are the ability to compare between different frameworks of transparency, which are the proposed CloudAdvisor, CPTS, and SCA. The customer will observe how each model will respond to the generated data, in terms of transparency and trustworthiness calculations, and evidence scores. More importantly, they will be able to test the various scenarios results of providers, which are described in Figure 56. The time factor is not against us when compared to the questionnaire-based approach where time is essential.

Adopting this method could lead to some risks, however the benefits could overcome them. The risks associated with this method are:

- Since the data are generated randomly and not being fed by the providers, the customers will lack the ability to make informed decisions about the selection of a provider. In return, however, they will be able compare which model of transparency is close enough to satisfy their business requirements.
- In the real environment the customer will be able to communicate with the provider whereas the simulation-based will lack this advantage because agreements should be made based on real data.



In this thesis, the simulation-based approach will be chosen. The justification of this selection is discussed in the following section.

## **8.6 Selection of Evaluation Technique**

An ideal evaluation of the above frameworks is based on getting real data from both the provider and the customer. However, this realistic approach is limited in resources in terms of time. Therefore, the simulation-based analysis can be an alternative approach where several advantages can be observed. They are:

- The participant can be in the role of the customer or auditor. The former is responsible for assigning the weights for the control areas. The latter will be able to change the quality of evidence based on the cloud auditor's judgment.
- The simulation-based approach can be regarded as an ideal attempt towards improving the transparency of the cloud service provider. It can explore the potential frameworks that exist in the literature, it can test these frameworks showing their advantages and disadvantages and perform an independent evaluation in order to obtain feedback that could improve transparency, or the current existing frameworks, or both.

The only disadvantage that can be observed from adopting this approach is that real data not fed from the cloud service provider and no communication can be made between the three actors: the provider, customer and the auditor.

## **8.7 Simulation Results**

In this Section, we present two types of results generated and calculated by the simulation. The first concerns cloud providers' trustworthiness results based on CloudAdvisor and Security Compliance Assessment (SCA). The second concerns cloud providers' transparency results based on CloudAdvisor and CPTS.

For more information, regarding the generated data and calculated results they are all presented in Appendix C.

Table 43 and 44 shows the scores for each factor for the cloud providers and the trustworthiness score for them. The generated data for these factors are presented in the appendix. As it can be seen from the tables below, trustworthiness score in the CloudAdvisor is higher than the trustworthiness score presented in the Cloud Provider Transparency Scorecard. The reason for that is that we have modified the equations that calculates the factors in CloudAdvisor framework in order to bring fairness between the providers. For instance, if a provider suffers from a security breach, CPTS normally gives zero score without considering the number of incidents. However, we mitigate this problem in CloudAdvisor. For example, if a provider suffers from two incidents of security breach, the score that will be given to the provider is 0.8 but not zero. The equations have been defined earlier both in Section 3.3.2 and Section 7.5.1.

The last row (Transparency Score) in Table 43 shows zero scores for all of the providers. This is because they have not submitted evidence that support their answers for all of the factors. Whereas Table 44, shows that the transparency score is available since each one of the providers has submitted evidence that support their claims. The transparency score is different from one to another depending on the providers' effort in providing evidence.

Table 43. Cloud Provider Transparency Scorecard - Trustworthiness Results

<b>CPTS</b>				
	<b>Cloud Providers</b>			
<b>Factors</b>	<b>CP2</b>	<b>CP91</b>	<b>CP14</b>	<b>CP49</b>
Years of Business	0	1	1	1
Membership	1	1	1	1
Security Breach	0	1	0	0
Privacy Breach	0	0	0	0
Outages	0	0	0	0
DataLoss	0	0	0	1
Trustworthiness Score	17%	50%	34%	50%
Transparency Score	0%	0%	0%	0%

Table 44. CloudAdvisor's Trustworthiness Results

CloudAdvisor				
Factors	Cloud Providers			
	CP2	CP91	CP14	CP49
Years of Business	0.6	1	1	1
Membership	1.9	1.2	1.5	1.3
Security Breach	0.8	1	0.6	0.9
Privacy Breach	0.4	0.6	0.3	0.8
Outages	0.7	0.8	0.4	0.5
DataLoss	0.3	0.2	0.8	1
Trustworthiness Score	69%	70%	67%	80%
Transparency Score	59%	50%	40%	17%

Figure 57 is graphical representation of the above tables (i.e. Table 43 and 44) that compares between CloudAdvisor and CPTS in terms of trustworthiness calculation for cloud providers. Other frameworks such as CSA STAR and SCA has not been included in the comparison, as they do not have the capability of measuring trustworthiness.

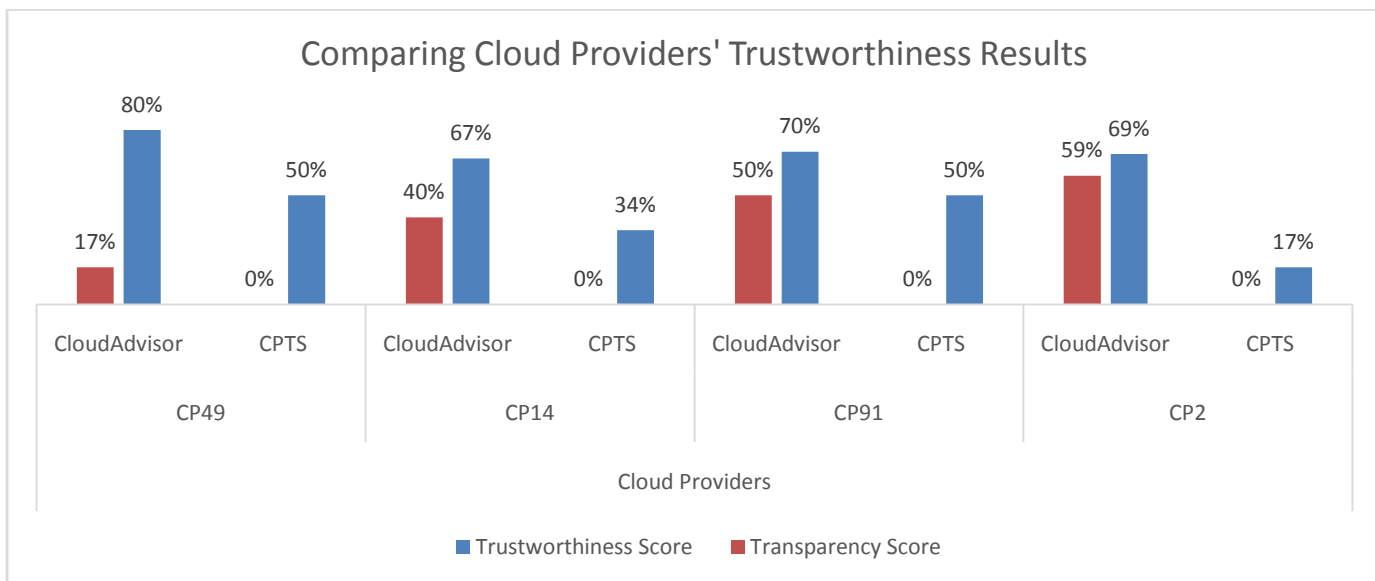


Figure 57. Comparing Cloud Providers' Trustworthiness Based on CloudAdvisor and CPTS

Table 45 shows the results of transparency measurement for both CloudAdvisor and SCA. We have only compared two providers instead of four because of the space limitation. In addition, we did not include the CSA STAR and CPTS frameworks, as they do not have the capability to measure transparency. Transparency measurement is based on providing scores for the eleven control areas that exist in the CCM framework. The only difference

between the SCA and CloudAdvisor is that it does not check if the evidence that is provided is kept up-to-date. This shows why SCA's results different from the CloudAdvisor.

Table 45. Transparency Results (CloudAdvisor Vs. SCA)

Transparency Results				
Factors	Cloud Providers			
	CP2		CP91	
	SCA	CloudAdvisor	SCA	CloudAdvisor
Compliance	24%	45%	33%	45%
Data Governance	33%	48%	25%	56%
Facility Security	9%	42%	25%	44%
HR Security	40%	30%	30%	30%
IS Security	28%	54%	32%	49%
Legal	30%	50%	45%	60%
Operations Management	31%	44%	42%	53%
Risk Management	31%	56%	32%	48%
Release Management	33%	43%	43%	53%
Resiliency	33%	53%	28%	47%
Security Architecture	33%	48%	38%	47%

Figure 58 is graphical representation of the above Table 45 that compares between CloudAdvisor and SCA in terms of transparency calculation. Other frameworks such as CSA STAR and CPTS has not been included in the comparison, as the CSA STAR does not have the capability of measuring transparency. The CPTS does not rely entirely on CCM framework, which makes it incomplete, compared to CloudAdvisor.

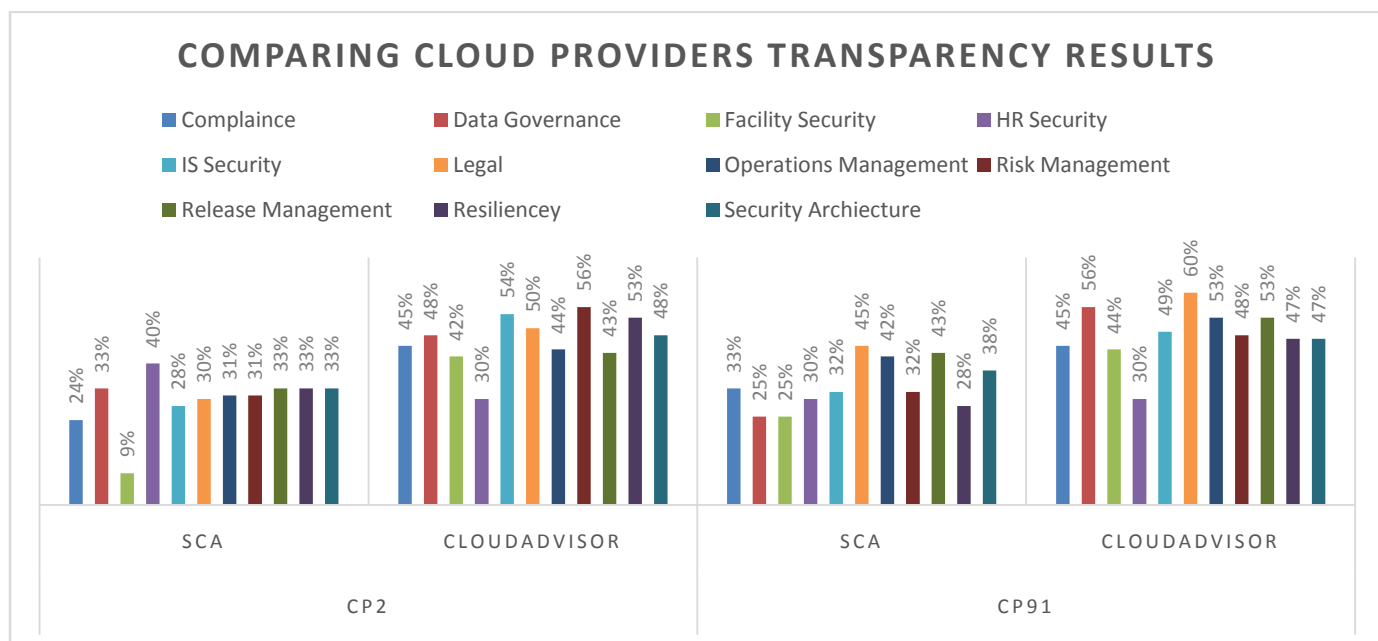


Figure 58. Transparency Results - A Comparison between Providers

In summary, the results have shown that CloudAdvisor is capable of measuring both cloud provider's trustworthiness and transparency and considering evidence support. Whereas other frameworks such as CPTS is capable only of measuring trustworthiness. The transparency aspect is considered by CPTS but it has not focused on using best industry standards such as the CCM Control Areas. In addition, the questions that have been formed are not enough for cloud customers to get their answers. With regards to the SCA, it is very close to CloudAdvisor in terms of measuring cloud providers' transparency however it lacks the quality of evidence such as keeping the evidence up-to-date. The CSA STAR has a rich repository but it does not measure trustworthiness and transparency. This is why CSA STAR was not included in the results.

## **Part IV**

### **Chapter 9: Conclusion and Future Work**

#### **9.1 Introduction**

This chapter summarises the work and limitations of the research presented in this thesis (Section 9.2). The goal and objectives outlined in Section 1.2 are evaluated with respect to their successful completion and the research recommendations are explored in Section 9.3.

#### **9.2 Summary and Limitations**

The need for an approach that could encourage cloud customers to adopt cloud computing, and help them to select the right cloud service provider without compromising security for both parties and encouraging transparency from the cloud provider, has been introduced in Chapter 1. Cloud customers need assurance from cloud providers that they are protecting their sensitive information and, similarly, cloud providers are reluctant to disclose sensitive information that could jeopardise the security of both cloud customers and providers. These concerns have risen due to the lack of control, lack of trust and lack of transparency. There is an argument that says that transparency is increasing while there is a lack of tools to measure the transparency of cloud providers. This argument has encouraged us to conduct a survey questionnaire, the design of which was presented in Chapter 4 and the results and discussion in Chapter 5 and 6. The questionnaire was entitled “Cloud Computing Adoption Issues and the Tools that Encourage Migration to the Cloud”. The first part of the survey aimed to learn respondents’ concerns about cloud computing adoption and the factors that encourage them to step forward to adopt it. In addition, the second part of the survey aimed to assess the tools of transparency, such as CSA STAR, CloudeAssurance and CTP in terms of their use to search for the cloud service provider and whether they were helpful and would be used in the future.

The survey questionnaire was launched in October 2012 and stopped collecting responses in October 2014, in order to have sufficient time to analyse the data. The survey has covered several sectors, including education, banks, governments, information technology and

healthcare. 177 responses were collected, 99 of which were completed (about 56%) and 78 respondents (44%) did not complete the survey. From those, who did not complete the survey questionnaire I think it was because the first questions that appeared to them were some demographic questions not the main questions of the survey, which might discourage them from completing that the survey [89]. The type of respondents were selected from technical and business side in an effort to encompass those who have an understanding of the technology and technological requirements for organisations, as well as those with experience in understanding the business goals of information technology projects.

The mailing list was created to include a variety of groups that specialise in cloud computing security and transparency, such as CSA, CSASTAR Support Group and Cloud Computing, SaaS, and Virtualization. In addition to that, another mailing list was created and collected from the websites of banks, education, healthcare, telecommunication, government and IT sectors.

The most important findings from the survey questionnaire, from both adopters and non-adopters points of view, are highlighted as follows. The results have shown that the main motivations for adopting the cloud were cost reduction, increased reliability and ubiquitous network access. With regards to their selection of the delivery and deployment model, SaaS model is dominant against the others and most of the respondents have chosen private cloud to be their best deployment model. This has been justified by the nature of the data and applications that they hold. In addition, respondents have preferred to choose multiple cloud providers to host their data or application, rather than relying on a single provider. A comparison has been conducted between the respondents from several sectors, including education, governments, IT, telecommunication, banks and healthcare. Banks prefer IaaS and the IT, education and governmental sectors prefer the SaaS model; the results indicate that the PaaS model is more convenient for telecommunication companies whereas healthcare prefers to use a combination of PaaS and SaaS models. With regards to the sectors' selection of type of cloud, the private cloud has been the most preferred type of deployment model for all sectors. We have identified which sectors prefer to use single or multiple cloud providers. The results have shown that IT and telecommunication select multiple providers, whereas responses from healthcare and education indicate that they rely on a single cloud provider. The other sectors (banks and governments) were interested in both single and multiple providers. Now we have highlighted the results from the adopters' point of view the following paragraph will highlight the main findings from non-adopters.

Despite the fact that 40% of the respondents have not adopted the cloud, around 72% of them are willing to adopt the cloud for several reasons that include cost reduction, flexibility of resource allocation and de-allocation, and broad network access. We assumed that the tools for selecting cloud service providers would be a major contribution for potential cloud customers to adopt the cloud. This assumption has been set out as one of the hypothesis in Section 1.2.3. The results, however, have shown that this factor is not significant. Governmental and education sectors have considered “tools that help customers to select cloud service providers” as an important factor in Section 5.3.4 (Figure 22). Meanwhile, respondents who have not adopted the cloud have done so for several reasons. The top concerns were the lack of security guarantees, followed by legal considerations, data confidentiality and auditability. Banks have placed more emphasis on the lack of transparency as a major inhibitor for cloud adoption.

The second part of the survey will highlight the main findings related to the assessment of tools. Assessing tools like CSA STAR, CloudeAssurance and CTP, we asked the respondents to give their opinions about using these tools for the purpose of evaluating cloud providers’ transparency. In addition, we asked them to state if they had used them to help search for best cloud provider that met their business requirements and if they had found them to be helpful.

The results suggest that most of the respondents who have used any of the three tools agree as to the importance of using them in order to evaluate cloud providers’ transparency. Having said that, some respondents from the IT, education and government sectors raised concerns regarding the importance of having a tool for evaluating cloud providers’ transparency. For instance, one IT respondent mentioned that they do not trust the results that are generated by the tool. From an educational point of view, it was claimed that transparency would not help as long as sensitive information is hosted in the cloud. Whereas respondents from the government sector stated that there is no comprehensive tool that can accomplish customised scripts. The most used tool was CTP and the least used was the CloudeAssurance. Section 2.5 identified a set of customer assurance requirements from the literature. A comparison between the tools was conducted in terms of the tools’ fulfilment of these requirements. The CTP fulfilled almost all of the requirements. The tool that fulfilled these requirements the least was the CSA STAR. This might suggest that customers’ assurance requirements are important to satisfy. Despite the omission of CloudeAssurance from the



comparison, it has been rated as the best in terms of its helpfulness to the respondents. This might be because of the application's ability to provide a ranking scheme for their customers.

Looking at the sectors' opinions that have not used the tools, we highlighted their concerns described in Section 6.3. To cite a few of them, respondents from the governmental sector (who have not adopted the cloud) stated that their concerns were:

- They are unfamiliar with the tools.
- They depend on other frameworks, such as gCloud.
- They do not trust that the tools in the market will produce correct results.
- There is not enough information provided about the tools.

Regarding the future use of CSA STAR, CloudeAssurance and CTP, we were able to receive feedback from education, government, IT and healthcare sectors. They are presented in the conclusion section (Section 6.5). To mention a few of them, they are presented in the following points:

- CSA STAR has raised some concerns among the IT, education, government and healthcare sector.
  - The IT respondents mentioned that they use their own judgment in the selection of cloud service providers. Moreover, they do not have sufficient information related to the CSA STAR registry.
  - The respondents from education showed that they are not familiar with the tool's existence. Some mentioned that they would use the tool for academic research purpose but not for real deployment.
  - Respondents from the government sector mentioned that CSA STAR does not provide customers with the capability to compare between cloud providers.
  - The healthcare and education sectors share the concern that they are not familiar with the tool. In addition to that, they need to do research on the tool itself before using it.

- CTP has raised concerns among the IT and education sectors.
  - The respondent from IT has expressed the same concerns that were mentioned in relation to CSA STAR, namely, the unfamiliarity of the tool and insufficient information related to it.
  - Respondents from education mentioned several concerns, to cite only a few. They mentioned that the tool should focus on the functionality of the provider not only security and that it is not yet widely used enough.
  
- CloudeAssurance has raised concerns among IT, education and governmental sectors.
  - The IT sector mentioned that they would use their own tools and conduct research. Moreover, some have said that depending on the nature of the data it will decide whether to use the tool or not.
  - Educational concerns are similar to those stated in relation to CTP.
  - Responses from the governmental sector have indicated that the CloudeAssurance is a commercial product that offers potential customers only a limited amount of time to explore how it works and to gauge whether it would satisfy their requirements or not.

Prior to the development of the survey questionnaire, some customer assurance requirements were identified and presented in the literature in Chapter 2. Those requirements might increase transparency and help cloud customers to search for the right cloud provider, if these requirements were adopted and considered during the development of a tool. Having said that, this has motivated us to develop a CloudAdvisor framework that aims to help cloud customers and cloud providers. The basis of the CloudAdvisor is to identify and cover the gaps that were not addressed from the literature. CloudAdvisor aims to satisfy two important components. The first is measuring the trustworthiness of cloud providers, based on business factors that are identified by Pauley. In addition to that, the measurement has to be validated by allowing cloud providers to submit evidence that supports their claims, which in turn could increase cloud customers' confidence in the provider. Moreover, it aims to monitor cloud providers' honesty through the provision of up-to-date evidence. The second component is related to transparency measurement. Transparency is measured based on the providers' compliance to the control areas developed by the CSA organisation. This was mainly achieved by attaching a Generic Scorecard Template (GST) to the Consensus

Assessment Initiative Questionnaire (CAIQ) template. The purpose of the GST is to allow cloud providers to submit their responses to the questions, comments, evidence and location of the evidence that are available in the CAIQ template. Then validating the answers by a trusted third party, auditor or a security professional in the field of cloud computing. The validation process might take long time because of the volume of the work that need to be checked manually by the auditor.

The method is described in Chapter 3 in more detail and an example of how trustworthiness and transparency is measured is presented in Chapter 7.

Another method that was been taken into consideration for measuring the transparency of cloud provider is the GQM approach. It is a top-down approach where the goals are first defined (e.g. compliance that represents the first control area of the CCM framework) and then questions that relate to the goal are stated. After this, the metrics are defined at the bottom. Defining the metrics was important as it helped us to provide a quantitative way of measuring cloud providers' transparency. However defining metrics is difficult and requires teamwork with expertise in the field. Moreover, there is on-going work on defining specific cloud metrics for the CCM control areas. The CSA Metrics Work Group (MWG) has developed security metrics that are needed to evaluate CCM's control areas. So far, the CSA MWG has created their first 10 metrics covering about 25 of CCM's control areas. Therefore, the GQM approach has not been adopted.

In Chapter 8, two possible evaluation techniques were proposed in order to evaluate the CloudAdvisor framework. The first was a survey-based questionnaire method where the CloudAdvisor should be implemented first and then a number of participants from both providers and customers invited to test and evaluate the platform. The providers were asked to register and start submitting their responses about various business factors (presented in Chapter 7), which is an important step towards building providers' trustworthiness profiles. The second step was asking providers' to answer the questions that are placed in the CAIQ questionnaire, in order to measure their transparency and to know how are they comply with customers' requirements. Then, the customers would be entitled to compare between the CloudAdvisor and other approaches, such as the CPTS and the SCA, based on the evaluation criteria defined in Section 8.3

The second method, which could be an alternative to the survey-based questionnaire, was a simulation-based analysis. This approach was proposed in order to compare between CloudAdvisor, CPTS and SCA in terms of their fulfilment of the customer assurance requirements presented in Section 8.4.2, without the need for providers' participation. The simulation was composed of five components, which are: (1) cloud providers' generation, (2) data generation, (3) scoring engine for calculating the trustworthiness and transparency scores of cloud providers, (4) reporting results and (5) evaluating results that will be conducted by the customers. These components were explained in more detail in Section 8.4.2. In order to select the best evaluation technique for the CloudAdvisor in this study, a comparison between survey-based questionnaire and simulation-based analysis was conducted in Section 8.5. Moreover, describing the advantages and disadvantages of each approach has been taken into consideration in Section 8.5.1 and 8.5.2. Simulation-based analysis was selected as the best evaluation technique for the CloudAdvisor and the reasons for this are outlined in Section 8.6. Section 8.7 discussed the simulation results. The results has shown a comparison between CloudAdvisor, CPTS, and SCA in terms of measuring trustworthiness and transparency.

Some of the limitations that Simulation-based approach might bring is that it will not be able to fetch real data from cloud providers. Instead, it will use some random data that is generated by a Java script. This will not assist customers to make better informed decisions towards the selection of cloud provider. In an effort to solve this problem, CSA has a repository that contains cloud providers answers but they are not helpful when we included the GST template. Additional information is needed and it is hard to contact cloud providers to complete the information needed in the GST template. Simulation-based approach, however, allow us to perform a comparison between different frameworks of transparency, which are CloudAdvisor, CPTS, and SCA. Customers will be able to observe how each framework will act towards trustworthiness and transparency measurement. In addition, they will be able to test the various scenarios results of providers, which are described in Figure 56.

### 9.3 Future Work

Based on the summary discussed in Section 9.2, there are some observations that need to be worked out, both in the survey questionnaire and the CloudAdvisor framework. For instance, there was a lack of response from different countries from various sectors, such as telecommunication, healthcare and banking. The majority of responses were received from Saudi Arabia (about 52% of the responses). This can be justified by the scientific trip that was conducted. The survey questionnaire was aimed only at the cloud customer not the provider. Therefore, we could perform another survey questionnaire that aims to receive feedback regarding providers' concerns towards disclosing information to their customers. For instance, are the questions in the CAIQ questionnaire formulated so that they will not compromise the security of either cloud providers customers?

With regards to CloudAdvisor framework, some suggestions have been taken into consideration in an attempt to improve the functionality of future work. For example, the following points highlight the recommended suggestions:

- CloudAdvisor is based on satisfying customer assurance requirements that have been identified in the literature (Chapter 2). We could conduct a survey questionnaire that aims to include other potential requirements from the experts that exist both in academia and industry.
- CloudAdvisor is based on two components; the first measures trustworthiness by focusing on factors that are related to the cloud providers' history as business entity and of its security. We could include other (QoS+) attributes [47]. To cite a few, they include (1) SLAs, (2) certification, (3) geographical location of the data centre (4) customer support facilities and, (5) performance test. The second component of the CloudAdvisor aims to measure cloud provider's transparency based on the CCM and CAIQ. Our work has been based on the CCM version 1.1. Future work regarding the improvement of transparency could use the latest version of the CCM and CAIQ (3.0.1). CCM version 3.0.1 has added five new controls. It addresses information security risks of the data in the cloud, both in transit and while accessing it. These controls are: mobile security, supply chain management, transparency and accountability, interoperability and portability and encryption and key management.

- Reputation can be regarded as an important factor for evaluating cloud provider's trustworthiness [77]. Therefore, leaving feedback by a cloud customer to a cloud provider could be a further area of investigation to be included in the CloudAdvisor as a future work. However, it has its own advantage and disadvantage. For example, leaving feedback by the customers will bring more confidence to other customers when they see some cloud providers are being ranked like on eBay and Amazon. Having said that, malicious or unprofessional users can add unreasonable feedback for cloud providers [134]. In an attempt to solve this problem, some mechanisms have been proposed such as filtering in order to eliminate unreasonable attacks. However, there is no clear evidence shows that it works, instead it has reduced them.
- Evaluating CloudAdvisor: there is an option of whether to implement the CloudAdvisor as a web application that will let both cloud providers and customers experiment with it giving customers a chance to: (1) evaluate cloud providers' transparency and trustworthiness and (2) be able to compare between different cloud providers. An alternative solution is a simulation built using random data. The simulation will test three frameworks (CloudAdvisor, CPTS and SCA) in terms of their fulfilment of the following requirements: (1) trustworthiness measurement (2) transparency measurement (3) evidence support and (4) up-to-date evidence.

## Appendix A

### Cloud Computing Adoption Issues and the Tools Encouraging Migration

#### A.1 Survey Questionnaire Template

Participant Information Sheet
<p>Title of Project: Towards Balanced Security and Transparency In Cloud Computing</p>
<p>Researcher: Mohammed Almanea (PhD Computing Sciences) Email: mohammed.almanea@ncl.ac.uk Phone: +447786829547</p>
<p>Purpose of the Study</p> <p>This questionnaire forms part of a study of the factors affecting customers' adoption of cloud computing, and of the extent to which existing tools and frameworks for transparency have or have not encouraged organizations from different sectors to migrate to the cloud. By "transparency" we mean "appropriate disclosure of the governance aspects of security design, policies, and practices"</p>
<p>The questionnaire has two parts.</p>
<p>Part 1: Includes general questions related to the drivers and constraints affecting the adoption of cloud technology.</p>
<p>Part 2: Relates to the tools/frameworks that could encourage transparency in the cloud.</p>
<hr/>
<p>The study will be distributed across different countries and among different sectors including Healthcare, Banks, Telecommunications, Education, and Information Technology companies</p>
<p>We have tested this survey. It should take not more than 10 minutes to complete</p>
<p>Your information will be kept anonymous and it will only be used for an academic purposes.</p>

## Part 1: Cloud Computing Adoption Drivers and Constraints for Enterprises

In this section, we would like to know the factors that affect enterprises' decision to adopt or not to adopt cloud computing.

**\* 1. Which of the following categories best describes your employment status?**

- Employed.
- Not employed.
- Other (please specify)

**\* 2. What is the highest level of education you have completed?**

- Bachelor's Degree
- Master's Degree
- Doctoral Degree
- Professional Degree (MD, JD)
- Other (please specify)

**\* 3. How many years of experience in Information Technology you have?**

- 1-5
- 6-15
- 16-30
- Over 30



**\* 1. How would you classify the scale of your enterprise?**

- Large - > 250 employees
- Medium - < 250 employees
- Small - < 50 employees
- Micro - < 10 employees

**\* 2. What sector are you working in?**

- Information Technology
- Telecommunication
- Educational Institute
- Government
- Healthcare
- Banks
- Other (please specify)

**\* 3. Which of the following best describes your job title ?**

**\* 4. In which country is your enterprise based?**

**5. Does your role influence your enterprise's decision whether to adopt or not adopt cloud computing solution?**

- Yes
- No

**\* 6. Are you already using Cloud-based services?**

- Yes
- No

**\* 1. How likely are you to consider beginning to ...**

Never      Less Likely      Neutral      Likely      More Likely

Adopt Cloud Computing                   

If you choose "Never" or "Less Likely" Please provide a comment

**\* 1. If you are planning to adopt cloud computing technology, what is the deployment model (i.e. type of the cloud - Public, Private or Hybrid - ) that you will choose to best suit your business and security requirements?**

- Public
- Private
- Hybrid (Public and Private)
- Don't know yet

## Reasons that could encourage your adoption of Cloud Computing

### \* 1. What is/are the reason(s) that could encourage you to adopt the cloud computing paradigm?

- Ubiquitous network access (i.e. access from anywhere and at anytime)
- Rapid decrease in hardware cost and increase in computing power and storage
- Elimination of the operational burden to cloud service providers
- Increased reliability through redundancy
- Elimination of an up-front investment
- Higher flexibility of resource allocation and de-allocation
- The ability to pay for the use of computing resources on a short-term basis
- Tools for selecting cloud service providers
- Other (please specify)

**\* 1. Thinking about potential barriers to the adoption of cloud technology, please check one or more of the options available that you feel are likely to inhibit your organization's adoption of cloud computing.**

- Unclear about liabilities on SLAs
- Isolation failure in a multi-tenant environment
- Data Lock-in
- Lack of security guarantees from Cloud Providers
- Legal considerations
- Lack of compliance with best industry standards (ISO, PCI DSS, HIPAA)
- Lack of transparency about cloud providers' security and privacy towards cloud customers' delivered services
- Malicious insiders
- Business continuity/Availability
- Data Confidentiality and auditability
- Lack of control over IT assets
- Other (please specify)

## Part 2 - Tools that encourage Transparency

In this part, we invite you to think about the possibility of having an assessment tool on the web that allows you to evaluate the transparency of cloud providers. By "transparency" we mean "appropriate disclosure of the governance aspects of security design, policies, and practices". We ask you consider whether such a tool would be helpful to you in deciding whether or not to adopt cloud technology.

**\* 1. Do you think having a tool for evaluating the transparency of the cloud providers is important and it will encourage you to migrate to the cloud?**

- Yes  
 No  
 Don't Know

Please Leave your Comment If answered "No"

**\* 1. How likely you agree on using an assessment tool for ..**

Strongly Disagree      Disagree      Undecided      Agree      Strongly Agree

Evaluating Cloud Providers' Transparency                             

Please write your comment if "Disagree" or "Strongly Disagree"

**\* 2. Some tools have been deployed recently that are claimed to encourage transparency in the cloud such as (CSA STAR, CloudTrust Protocol, and CloudeAssurance).**

**Have you used the CSA STAR to search for a cloud provider offering ?**

- Yes  
 No

**\* 1. How helpful did you find the CSA STAR in encouraging you to use cloud computing solutions?**

	Not helpful	Little helpful	Undecided	Helpful	Very helpful
CSA STAR	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please write your comment if "Not helpful" or "Little helpful"

**\* 2. Do you plan to use the CSA STAR to search for the appropriate Cloud Service Provider in the near future?**

- Yes  
 No

If "No", please write your comment

**\* 3. Have you used the CloudTrust Protocol to search for a cloud provider offering ?**

- Yes  
 No



**\* 1. How helpful did you find the CloudTrust Protocol in encouraging you to use cloud computing solutions ?**

	Not helpful	Little helpful	Undecided	Helpful	Very helpful
CloudTrust Protocol	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please write your comment if "Not helpful" or "Little helpful"

**\* 2. Do you plan to use the CloudTrust Protocol to search for the appropriate Cloud Service Provider in the near future?**

- Yes  
 No

If "No", please write your comment

**\* 3. Have you used the CloudeAssurance to search for a cloud provider offering?**

- Yes  
 No

**\* 1. How helpful did you find the CloudeAssurance in encouraging you to use cloud computing solutions?**

	Not helpful	Little helpful	Undecided	Helpful	Very helpful
CloudeAssurance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please write your comment if "Not helpful" or "Little helpful"

**\* 2. Do you plan to use the CloudeAssurance to search for the appropriate Cloud Service Provider in the near future?**

- Yes
- No

If "No", Please write your comment

**\* 1. Please specify the type(s) of service that you are using (check one or more of the boxes)**

- Infrastructure as a Service (e.g. Amazon EC2, S3, Rackspace, GoGrid)
- Platform as a Service (e.g. Google Apps, Salesforce, Microsoft Azure)
- Software as a Service (e.g. Google Docs)
- Other (please specify)

**\* 2. Based on the delivery services (IaaS, PaaS, and SaaS) that you have hired from the cloud provider, what is the type of cloud model that has been used to deliver your services?**

- Private
- Public
- Hybrid (Simultaneous use of Public and Private Clouds)
- Other (please specify)

**\* 3. What was/were the reason(s) for choosing the model that you think is best suited your enterprise?**

- Non-mission-critical applications and data
- Mission-critical applications and data
- Mission and Non-Mission Critical Applications and data
- Other (please specify)

**\* 4. Have you used a single cloud service provider in order to meet your business requirements, or multiple providers?**

- Single Cloud Service Provider
- Multiple Cloud Service Providers

**\*5. What is/are the reason(s) that encouraged you to adopt the cloud computing paradigm?**

- Ubiquitous network access (i.e. access from anywhere and at anytime)
- Rapid decrease in hardware cost and increase in computing power and storage
- Elimination of the operational burden to cloud service providers
- Increased reliability through redundancy
- Elimination of an up-front investment
- Higher flexibility of resource allocation and de-allocation
- The ability to pay for the use of computing resources on a short-term basis
- Tools for selecting cloud service providers
- Other (please specify)

Thank you for your time and your valuable input ....


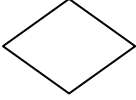
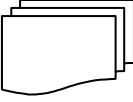

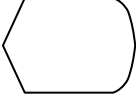
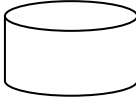


**\*1. Do you wish to be contacted if necessary ?**

No

Yes, please write your email

Thank you for your time and your valuable input .

## A.2 Workflow Annotations

	Shape	Name
1		Process
2		Decision
3		Multi Document
4		Document
5		Display
6		Database
7		Module
9		Person (i.e. customers or providers)

## Appendix B

### Cloud Controls Matrix Framework

#### B.1 Cloud Controls Groups

Table 46. Cloud Controls Matrix Groups

	<b>Control Group</b>	<b>Questions</b>	<b>Weight</b>
1	Compliance	16	8%
2	Data Governance	16	8%
3	Facility Security	9	4%
4	HR Security	4	2%
5	Information Security	75	37%
6	Legal	14	7%
7	Operation Management	6	3%
8	Risk Management	12	6%
9	Release Management	6	3%
10	Resiliency	12	6%
11	Security Architecture	32	16%
	<b>Total</b>	<b>202</b>	<b>100%</b>

Table 47. Compliance Control Areas

<b>Control Group</b>	<b>Number of Controls</b>	<b>CGID</b>	<b>Control</b>	<b>Number of Questions</b>
Compliance	6	CO-01	Audit Planning	1
		CO-02	Independent Audits	7
		CO-03	Third Party Audits	2
		CO-04	Authority Maintenance	1
		CO-05	Information System Regulatory Mapping	2
		CO-06	Intellectual Property	3

Table 48. Data Governance Control Areas

Data Governance	8	DG-01	Ownership	1
		DG-02	Classification	5
		DG-03	Handling/Labeling/Security Policy	2
		DG-04	Retention Policy	2
		DG-05	Secure Disposal	2
		DG-06	Nonproduction Data	1
		DG-07	Information Leakage	2
		DG-08	Risk Assessments	1



Table 49. Facility Security Control Areas

Facility Security	8	FS-01	Policy	1
		FS-02	User Access	1
		FS-03	Controlled Access Points	1
		FS-04	Secure Area Authorization	1
		FS-05	Unauthorised Persons Entry	1
		FS-06	Offsite Authorization	1
		FS-07	Offsite Equipment	1
		FS-08	Asset Management	2

Table 50. HR Control Areas

HR Security	3	HR-01	Background Screening	1
		HR-02	Employment Agreements	2
		HR-03	Employment Termination	1

Table 51. Information Security Control Areas

Control Group	Number of Controls	CGID	Control	Number of Questions
Information Security	34	IS-01	Management Program	1
		IS-02	Management Support / Involvement	1
		IS-03	Policy	3
		IS-04	Baseline Requirements	3
		IS-05	Policy Reviews	1
		IS-06	Policy Enforcement	2
		IS-07	User Access Policy	2
		IS-08	User Access Restriction / Authorization	2
		IS-09	User Access Revocation	2
		IS-10	User Access Reviews	3
		IS-11	Training / Awareness	2
		IS-12	Industry Knowledge / Benchmarking	2
		IS-13	Roles / Responsibilities	1
		IS-14	Management Oversight	1
		IS-15	Segregation of Duties	1
		IS-16	User Responsibility	3
		IS-17	Workspace	3
		IS-18	Encryption	2
		IS-19	Encryption Key Management	4
		IS-20	Vulnerability / Patch Management	6
		IS-21	Antivirus / Malicious Software	2
		IS-22	Incident Management	3
		IS-23	Incident Reporting	2
		IS-24	Incident Response Legal Preparation	4
		IS-25	Incident Response Metrics	2
		IS-26	Acceptable Use	3
		IS-27	Asset Returns	2
		IS-28	e-Commerce Transactions	2
		IS-29	Audit Tools Access	1
		IS-30	Diagnostic / Configuration Ports Access	1
		IS-31	Network / Infrastructure Services	2
		IS-32	Portable / Mobile Devices	1
		IS-33	Source Code Access Restriction	2
		IS-34	Utility Programs Access	3

Table 52. Legal Control Areas

Control Group	Number of Controls	CGID	Control	Number of Questions
Legal	2	LG-01	Nondisclosure agreements	1
		LG-02	Third Party Agreements	3

Table 53. Operation Management Control Areas

Control Group	Number of Controls	CGID	Control	Number of Questions
Operation Management	4	OP-01	Policy	1
		OP-02	Documentation	1
		OP-03	Capacity/ Resource Planning	2
		OP-04	Equipment Maintenance	5

Table 54. Risk Management Control Areas

Control Group	Number of Controls	CGID	Control	Number of Questions
Risk Management	5	RI-01	Program	2
		RI-02	Assessments	2
		RI-03	Mitigation / Acceptance	2
		RI-04	Business / Policy Change Impact	1
		RI-05	Third Party Access	7

Table 55. Release Management Control Areas

Control Group	Number of Controls	CGID	Control	Number of Questions
Release Management	5	RM-01	New Development / Acquisition	1
		RM-02	Production Changes	1
		RM-03	Quality Testing	1
		RM-04	Outsourced Development	2
		RM-05	Unauthorised Software Installations	1

Table 56. Industry Standards Mapped to CCM

Standard	Reference
COBIT	[116]
HIPAA	[55]
ISO27001	[117]
SP800-53	[118]
FedRamp	[54]
PCI-DSS	[53]
BITS	[119]
GAPP	[120]

## B.2 Simulation Script – Trustworthiness and Transparency Measurement

```
import java.math.BigDecimal;
import java.math.RoundingMode;
import java.util.Arrays;
import java.util.Random;

public class RunSimulation {
    private static void log(String aMessage) {
        System.out.println(aMessage);
    }

    public static void main(String[] args) {

        // Generating random number for the number of Cloud Providers

        Random randomGenerator = new Random();
        int NCP = randomGenerator.nextInt((4 - 1) + 1) + 1;
        log("Number of Cloud Providers : " + NCP);
        log("\n");

        // Defining Cloud Provider IDs

        int[] CPID;
        CPID = new int[NCP];

        // Years of Business Factor Variables

        double[] YoB;
        double[] YoB_Score;
        double[] YoB_Value;
        double[] YoB_Score_CloudAdvisor;
        double[] YoB_Value_CloudAdvisor;

        YoB = new double[NCP];
        YoB_Score = new double[NCP];
        YoB_Value = new double[NCP];
        YoB_Score_CloudAdvisor = new double[NCP];
        YoB_Value_CloudAdvisor = new double[NCP];

        // Membership Factor Variables

        double[] NM;
        double[] NE;
        double[] Membership_Trustworthiness_Score;
        double[] Membership_Trustworthiness_Score_CloudAdvisor;

        double[] Membership_Trustworthiness_Value;
        double[] Membership_Trustworthiness_Value_CloudAdvisor;

        double[] Membership_Transparency_Score;
        double[] Membership_Transparency_Value;

        NM = new double[NCP];
        NE = new double[NCP];

        Membership_Trustworthiness_Score = new double[NCP];
        Membership_Trustworthiness_Score_CloudAdvisor = new double[NCP];

        Membership_Trustworthiness_Value = new double[NCP];
```

```

Membership_Trustworthiness_Value_CloudAdvisor = newdouble[NCP];

Membership_Transparency_Score = newdouble[NCP];
Membership_Transparency_Value = newdouble[NCP];

// Security Breach Factor Variables

double[] SecBreaches;
double[] PublishedEvidence;
doubleSecBreach_Trustworthiness_Score[];
doubleSecBreach_Trustworthiness_Score_CloudAdvisor[];
doubleSecBreach_Trustworthiness_Value[];
doubleSecBreach_Trustworthiness_Value_CloudAdvisor[];
doubleSecBreach_Transparency_Score[];
doubleSecBreach_Transparency_Value[];

SecBreaches = newdouble[NCP];
PublishedEvidence = newdouble[NCP];
SecBreach_Trustworthiness_Score = newdouble[NCP];
SecBreach_Trustworthiness_Score_CloudAdvisor = newdouble[NCP];
SecBreach_Trustworthiness_Value = newdouble[NCP];
SecBreach_Trustworthiness_Value_CloudAdvisor = newdouble[NCP];
SecBreach_Transparency_Score = newdouble[NCP];
SecBreach_Transparency_Value = newdouble[NCP];

// Privacy Breach Factor Variables

double[] PrivBreaches;
double[] P_PublishedEvidence;
doublePrivBreach_Trustworthiness_Score[];
doublePrivBreach_Trustworthiness_Score_CloudAdvisor[];
doublePrivBreach_Trustworthiness_Value[];
doublePrivBreach_Trustworthiness_Value_CloudAdvisor[];
doublePrivBreach_Transparency_Score[];
doublePrivBreach_Transparency_Value[];

PrivBreaches = newdouble[NCP];
P_PublishedEvidence = newdouble[NCP];
PrivBreach_Trustworthiness_Score = newdouble[NCP];
PrivBreach_Trustworthiness_Score_CloudAdvisor = newdouble[NCP];
PrivBreach_Trustworthiness_Value = newdouble[NCP];
PrivBreach_Trustworthiness_Value_CloudAdvisor = newdouble[NCP];
PrivBreach_Transparency_Score = newdouble[NCP];
PrivBreach_Transparency_Value = newdouble[NCP];

// Outages Factor Variables

double[] Outages;
double[] Outages_PublishedEvidence;
doubleOutages_Trustworthiness_Score[];
doubleOutages_Trustworthiness_Score_CloudAdvisor[];
doubleOutages_Trustworthiness_Value[];
doubleOutages_Trustworthiness_Value_CloudAdvisor[];
doubleOutages_Transparency_Score[];
doubleOutages_Transparency_Value[];

Outages = newdouble[NCP];
Outages_PublishedEvidence = newdouble[NCP];
Outages_Trustworthiness_Score = newdouble[NCP];
Outages_Trustworthiness_Score_CloudAdvisor = newdouble[NCP];
Outages_Trustworthiness_Value = newdouble[NCP];

```

```

Outages_Trustworthiness_Value_CloudAdvisor = newdouble[NCP];
Outages_Transparency_Score = newdouble[NCP];
Outages_Transparency_Value = newdouble[NCP];

// DataLoss Factor Variables

double[] DataLoss;
double[] DataLoss_PublishedEvidence;
doubleDataLoss_Trustworthiness_Score[];
doubleDataLoss_Trustworthiness_Score_CloudAdvisor[];
doubleDataLoss_Trustworthiness_Value[];
doubleDataLoss_Trustworthiness_Value_CloudAdvisor[];
doubleDataLoss_Transparency_Score[];
doubleDataLoss_Transparency_Value[];

DataLoss = newdouble[NCP];
DataLoss_PublishedEvidence = newdouble[NCP];
DataLoss_Trustworthiness_Score = newdouble[NCP];
DataLoss_Trustworthiness_Score_CloudAdvisor = newdouble[NCP];
DataLoss_Trustworthiness_Value = newdouble[NCP];
DataLoss_Trustworthiness_Value_CloudAdvisor = newdouble[NCP];
DataLoss_Transparency_Score = newdouble[NCP];
DataLoss_Transparency_Value = newdouble[NCP];

double[] Total_Trustworthiness_Value;
Total_Trustworthiness_Value = newdouble[NCP];

double[] Total_Trustworthiness_Value_CloudAdvisor;
Total_Trustworthiness_Value_CloudAdvisor = newdouble[NCP];

// Start

// Need to ensure that NCP value always > 0

for (inti = 0; i<NCP; i++)
{

    CPID[i] = randomGenerator.nextInt(((100 - 1) + 1) + 1);

    System.out.println("=====");
    System.out.println("Cloud Provider (" + CPID[i] + ")");
    System.out.println("=====");

    // Years of Business Factor: Computing the Score

    intrandomInt = randomGenerator.nextInt(((35 - 1) + 1) +
1);
    YoB[i] = randomInt;

    System.out.println("Years in Business (" + YoB[i] +
");");

    // Calculating Years of Business for the CPTS

    if (YoB[i] > 5) {
        YoB_Value[i] = 1.0;
        YoB_Score[i] = YoB_Value[i] * 100;
    } else {
        YoB_Value[i] = 0.0;
        YoB_Score[i] = YoB_Value[i] * 100;
    }
}

```

```

// Calculating Years of Business for the CloudAdvisor

    if (YoB[i] > 5) {
        YoB_Value_CloudAdvisor[i] = 1.0;
        YoB_Score_CloudAdvisor[i] =
YoB_Value_CloudAdvisor[i] * 100;
    } else {
        if (YoB[i] == 5) {
            YoB_Value_CloudAdvisor[i] = 0.8;
            YoB_Score_CloudAdvisor[i] =
YoB_Value_CloudAdvisor[i] * 100;
        } elseif (YoB[i] == 4) {
            YoB_Value_CloudAdvisor[i] = 0.6;
            YoB_Score_CloudAdvisor[i] =
YoB_Value_CloudAdvisor[i] * 100;
        } elseif (YoB[i] == 3) {
            YoB_Value_CloudAdvisor[i] = 0.4;
            YoB_Score_CloudAdvisor[i] =
YoB_Value_CloudAdvisor[i] * 100;
        } elseif (YoB[i] == 2) {
            YoB_Value_CloudAdvisor[i] = 0.2;
            YoB_Score_CloudAdvisor[i] =
YoB_Value_CloudAdvisor[i] * 100;
        } elseif (YoB[i] <= 1) {
            YoB_Value_CloudAdvisor[i] = 0.0;
            YoB_Score_CloudAdvisor[i] =
YoB_Value_CloudAdvisor[i] * 100;
        }
    }

}

// Membership Factor: Computing the Score

NM[i] = randomGenerator.nextInt(10);
NE[i] = randomGenerator.nextInt(10);

// Calculating Membership Score for the CPTS

if (NM[i] == 0) {
    Membership_Trustworthiness_Score[i] = 00.0;
    Membership_Trustworthiness_Value[i] = 0.0;
} else {
    Membership_Trustworthiness_Value[i] = 1.0;
    Membership_Trustworthiness_Score[i] =
Membership_Trustworthiness_Value[i] * 100.0;
}

// Calculating Membership Score for the CloudAdvisor

if (NM[i] == 0) {
    Membership_Trustworthiness_Score_CloudAdvisor[i] =
00.0;
    Membership_Trustworthiness_Value_CloudAdvisor[i] =
0.0;
} else {
    if (NM[i] >= 1 &&NM[i] < 10) {
        Membership_Trustworthiness_Value_CloudAdvisor[i] = 1 + (0.1 * NM[i]);
    }
}

```

```

        Membership_Trustworthiness_Score_CloudAdvisor[i] =
Membership_Trustworthiness_Value_CloudAdvisor[i]
                * 100.0;
    }
    // Measuring the transparency of the Cloud Provider
based on
    // Evidence Provided
    while (NE[i] >NM[i]) {
        NE[i] = randomGenerator.nextInt(10);
    }
    System.out.println("Memberships      (" + NM[i]
+ ")");
    System.out.println("Published Evidence (" + NE[i]
+ ")");
    Membership_Transparency_Value[i] = NE[i] / NM[i];
    Membership_Transparency_Score[i] = NE[i] / NM[i] *
100;
    }

    // Security Breaches Factor: Computing the Score
    SecBreaches[i] = randomGenerator.nextInt(10);
    PublishedEvidence[i] = randomGenerator.nextInt(10);

    // Calculating Security Breach for CPTS
    if (SecBreaches[i] == 0) {
        SecBreach_Trustworthiness_Score[i] = 100.0;
        SecBreach_Trustworthiness_Value[i] = 1.0;
    } else {
        SecBreach_Trustworthiness_Score[i] = 0.0;
        SecBreach_Trustworthiness_Value[i] = 0.0;
    }

    // Calculating Security Beach for CloudAdvisor
    if (SecBreaches[i] == 0) {
        SecBreach_Trustworthiness_Score_CloudAdvisor[i] =
100.0;
        SecBreach_Trustworthiness_Value_CloudAdvisor[i] =
1.0;
    } else {
        SecBreach_Trustworthiness_Value_CloudAdvisor[i] =
1.0 - (0.1 * SecBreaches[i]);
        SecBreach_Trustworthiness_Score_CloudAdvisor[i] =
SecBreach_Trustworthiness_Value_CloudAdvisor[i] * 100;

        while (PublishedEvidence[i] >SecBreaches[i]) {
randomGenerator.nextInt(10);
        }

        System.out.println("Security Breaches      (" +
SecBreaches[i] + ")");
        System.out.println("Published Evidence      (" +
PublishedEvidence[i] + ")");

```



```

        SecBreach_Transparency_Value[i] =
PublishedEvidence[i] / SecBreaches[i];
        SecBreach_Transparency_Score[i] =
PublishedEvidence[i] / SecBreaches[i] * 100;
    }

    // Privacy Breaches Factor: Computing the Score

PrivBreaches[i] = randomGenerator.nextInt(10);
P_PublishedEvidence[i] = randomGenerator.nextInt(10);

    // Calculating Privacy Breaches for the CPTS

if (PrivBreaches[i] == 0) {

        PrivBreach_Trustworthiness_Value[i] = 1.0;
        PrivBreach_Trustworthiness_Score[i] = 100.0;

    } else {

        PrivBreach_Trustworthiness_Value[i] = 0.0;
        PrivBreach_Trustworthiness_Score[i] = 0.0;
    }

    // Calculating Privacy Breaches for the CloudAdvisor

if (PrivBreaches[i] == 0) {

        PrivBreach_Trustworthiness_Value_CloudAdvisor[i] =
1.0;
        PrivBreach_Trustworthiness_Score_CloudAdvisor[i] =
100.0;

    } else {

        PrivBreach_Trustworthiness_Value_CloudAdvisor[i] =
1.0 - (0.1 * PrivBreaches[i]);
        PrivBreach_Trustworthiness_Score_CloudAdvisor[i] =
PrivBreach_Trustworthiness_Value_CloudAdvisor[i]
        * 100;

        while (P_PublishedEvidence[i] >PrivBreaches[i]) {
            P_PublishedEvidence[i] =
randomGenerator.nextInt(10);
        }

        System.out.println("Privacy Breaches      (" +
PrivBreaches[i] + ")");
        System.out.println("Published Evidence    (" +
P_PublishedEvidence[i] + ")");

        PrivBreach_Transparency_Value[i] =
P_PublishedEvidence[i] / PrivBreaches[i];
        PrivBreach_Transparency_Score[i] =
P_PublishedEvidence[i] / PrivBreaches[i] * 100;
    }

    // Outages Factor: Computing the Score

Outages[i] = randomGenerator.nextInt(10);

```

```

        Outages_PublishedEvidence[i] =
randomGenerator.nextInt(10);

        // Calculating Outages for the CPTS

        if (Outages[i] == 0) {
            Outages_Trustworthiness_Score[i] = 100.0;
            Outages_Trustworthiness_Value[i] = 1.0;

        } else {

            Outages_Trustworthiness_Value[i] = 0.0;
            Outages_Trustworthiness_Score[i] = 0.0;
        }

        // Calculating Outages for the CloudAdvisor

        if (Outages[i] == 0) {
            Outages_Trustworthiness_Score_CloudAdvisor[i] =
100.0;
            Outages_Trustworthiness_Value_CloudAdvisor[i] =
1.0;

        } else {

            Outages_Trustworthiness_Value_CloudAdvisor[i] = 1.0
- (0.1 * Outages[i]);
            Outages_Trustworthiness_Score_CloudAdvisor[i] =
Outages_Trustworthiness_Value_CloudAdvisor[i] * 100;

            while (Outages_PublishedEvidence[i] >Outages[i]) {
                Outages_PublishedEvidence[i] =
randomGenerator.nextInt(10);
            }

            System.out.println("Outages          (" +
Outages[i] + ")");
            System.out.println("Published Evidence (" +
Outages_PublishedEvidence[i] + ")");

            Outages_Transparency_Value[i] =
Outages_PublishedEvidence[i] / Outages[i];
            Outages_Transparency_Score[i] =
Outages_PublishedEvidence[i] / Outages[i] * 100;
        }

        // DataLoss Factor: Computing the Score

        DataLoss[i] = randomGenerator.nextInt(10);
        DataLoss_PublishedEvidence[i] =
randomGenerator.nextInt(10);

        // Calculating DataLoss for the CPTS

        if (DataLoss[i] == 0) {
            DataLoss_Trustworthiness_Score[i] = 100.0;
            DataLoss_Trustworthiness_Value[i] = 1.0;

        } else {

            DataLoss_Trustworthiness_Value[i] = 0.0;

```

```

        DataLoss_Trustworthiness_Score[i] = 0.0;
    }

    // Calculating DataLoss for the CloudAdvisor

    if (DataLoss[i] == 0) {
        DataLoss_Trustworthiness_Score_CloudAdvisor[i] =
100.0;
        DataLoss_Trustworthiness_Value_CloudAdvisor[i] =
1.0;

    } else {

        DataLoss_Trustworthiness_Value_CloudAdvisor[i] =
1.0 - (0.1 * DataLoss[i]);
        DataLoss_Trustworthiness_Score_CloudAdvisor[i] =
DataLoss_Trustworthiness_Value_CloudAdvisor[i] * 100;

        while (DataLoss_PublishedEvidence[i] >DataLoss[i])
        {
            DataLoss_PublishedEvidence[i] =
randomGenerator.nextInt(10);
        }

        System.out.println("DataLoss          (" +
DataLoss[i] + ")");
        System.out.println("Published Evidence (" +
DataLoss_PublishedEvidence[i] + ")");

        DataLoss_Transparency_Value[i] =
DataLoss_PublishedEvidence[i] / DataLoss[i];
        DataLoss_Transparency_Score[i] =
DataLoss_PublishedEvidence[i] / DataLoss[i] * 100;
    }

    // ----- End of Trustworthiness Measurement -----
}

// Printing Original Results

log("-----");
log("\n");
log("=====");
log(" Trustworthiness Measurement Results ");
log("=====");
log("\n");

log(" [1] Cloud Provider Transparency Scorecard (CPTS) ");
log("\n" + "-----");
log("-----");

    for (intk = 0; k<NCP; k++) {
        System.out.print("          | CP" +
(CPID[k]));
    }

log("\n" + "-----");
log("-----");

```

```

System.out.print(" | Years of Business " + " |");
for (int m = 0; m < NCP; m++) {
    System.out.print(YoB_Value[m]);
    System.out.print(" |");
}
log("\n");
System.out.print(" | Membership " + " |");
for (int m = 0; m < NCP; m++) {
    System.out.print(Membership_Trustworthiness_Value[m]);
    System.out.print(" |");
}
log("\n");
System.out.print(" | Security Breach " + " |");
for (int m = 0; m < NCP; m++) {
    System.out.print(SecBreach_Trustworthiness_Value[m]);
    System.out.print(" |");
}
log("\n");
System.out.print(" | Privacy Breach " + " |");
for (int m = 0; m < NCP; m++) {
    System.out.print(PrivBreach_Trustworthiness_Value[m]);
    System.out.print(" |");
}
log("\n");
System.out.print(" | Outages " + " |");
for (int m = 0; m < NCP; m++) {
    System.out.print(Outages_Trustworthiness_Value[m]);
    System.out.print(" |");
}
log("\n");
System.out.print(" | Data Loss " + " |");
for (int m = 0; m < NCP; m++) {
    System.out.print(DataLoss_Trustworthiness_Value[m]);
    System.out.print(" |");
}
log("\n" + "-----");
System.out.print(" | Trustworthiness Score " + " |");
for (int m = 0; m < NCP; m++) {
    Total_Trustworthiness_Value[m] = YoB_Value[m] +
Membership_Trustworthiness_Value[m]
+ SecBreach_Trustworthiness_Value[m] +
PrivBreach_Trustworthiness_Value[m]
+ Outages_Trustworthiness_Value[m] +
DataLoss_Trustworthiness_Value[m];
    System.out.print(Total_Trustworthiness_Value[m]);
    System.out.print(" |");
}
log("\n");
System.out.print(" | Trustworthiness % " + " |");
for (int m = 0; m < NCP; m++) {
    BigDecimal value = new
BigDecimal((Total_Trustworthiness_Value[m] / 6) * 100);
    value = value.setScale(0, RoundingMode.UP);
    System.out.print(value + "%");
    System.out.print(" |");
}
log("\n" + "-----");

```

```

log("\n\n");

log(" [2] CloudAdvisor ");
log("-----");
-----");
for (intk = 0; k<NCP; k++) {
    System.out.print("          | CP" +
(CPID[k]));
}

log("\n" + "-----");
-----");
System.out.print(" | Years of Business " + " |");
for (intm = 0; m<NCP; m++) {
    System.out.print(YoB_Value_CloudAdvisor[m]);
    System.out.print(" |");
}
log("\n");
System.out.print(" | Membership " + " |");
for (intm = 0; m<NCP; m++) {

    System.out.print(Membership_Trustworthiness_Value_CloudAdvisor[m] + "
");
        BigDecimal value = new
BigDecimal(Membership_Transparency_Score[m]);
        value = value.setScale(0, RoundingMode.UP);

Computing        // If the Cloud Provider is not a member of any Cloud
                // Group, then there is no need
                // to measure its transparency

                if (Membership_Trustworthiness_Value[m] == 0)
                    System.out.print("NA");
                else
                    System.out.print(value + "%");
                if (Membership_Transparency_Score[m] < 10)
                    System.out.print("          |");
                else
                    System.out.print("          |");

            }
log("\n");
System.out.print(" | Security Breach " + " |");
for (intm = 0; m<NCP; m++) {

    System.out.print(SecBreach_Trustworthiness_Value_CloudAdvisor[m] + "
");
        BigDecimal value = new
BigDecimal(SecBreach_Transparency_Score[m]);
        value = value.setScale(0, RoundingMode.UP);

breach, then    // If the cloud provider does not suffer from security
                // there is no need to measure
                // its transparency
                if (SecBreach_Trustworthiness_Value[m] == 1)
                    System.out.print("NA");
                else
                    System.out.print(value + "%");

```

```

        if (SecBreach_Transparency_Score[m] < 10)
            System.out.print("                |");
        else
            System.out.print("                |");
    }
    log("\n");
    System.out.print("| Privacy Breach " + "                |");
    for (int m = 0; m < NCP; m++) {

        System.out.print(PrivBreach_Trustworthiness_Value_CloudAdvisor[m] + "
");
        BigDecimal value = new
BigDecimal(PrivBreach_Transparency_Score[m]);
        value = value.setScale(0, RoundingMode.UP);
        if (PrivBreach_Trustworthiness_Value[m] == 1)
            System.out.print("NA");
        else
            System.out.print(value + "%");

        if (PrivBreach_Transparency_Score[m] < 10)
            System.out.print("                |");
        else
            System.out.print("                |");
    }
    log("\n");
    System.out.print("| Outages " + "                |");
    for (int m = 0; m < NCP; m++) {

        System.out.print(Outages_Trustworthiness_Value_CloudAdvisor[m] + "
");
        BigDecimal value = new
BigDecimal(Outages_Transparency_Score[m]);
        value = value.setScale(0, RoundingMode.UP);
        if (Outages_Trustworthiness_Value[m] == 1)
            System.out.print("NA");
        else
            System.out.print(value + "%");
        if (Outages_Transparency_Score[m] < 10)
            System.out.print("                |");
        else
            System.out.print("                |");
    }
    log("\n");
    System.out.print("| Data Loss " + "                |");
    for (int m = 0; m < NCP; m++) {

        System.out.print(DataLoss_Trustworthiness_Value_CloudAdvisor[m] + "
");
        BigDecimal value = new
BigDecimal(DataLoss_Transparency_Score[m]);
        value = value.setScale(0, RoundingMode.UP);
        if (DataLoss_Trustworthiness_Value[m] == 1)
            System.out.print("NA");
        else
            System.out.print(value + "%");
        if (DataLoss_Transparency_Score[m] < 10)
            System.out.print("                |");
        else
            System.out.print("                |");
    }
}

```

```

log("\n" + "-----");
-----");
System.out.print("| Trustworthiness Score " + "|");
for (int m = 0; m < NCP; m++) {
    Total_Trustworthiness_Value_CloudAdvisor[m] =
YoB_Value_CloudAdvisor[m]
+
Membership_Trustworthiness_Value_CloudAdvisor[m] +
SecBreach_Trustworthiness_Value_CloudAdvisor[m]
+
PrivBreach_Trustworthiness_Value_CloudAdvisor[m] +
Outages_Trustworthiness_Value_CloudAdvisor[m]
+
DataLoss_Trustworthiness_Value_CloudAdvisor[m];

System.out.print(Total_Trustworthiness_Value_CloudAdvisor[m]);
System.out.print(" ");
}

log("\n");
System.out.print("| Trustworthiness % " + "|");
for (int m = 0; m < NCP; m++) {
    BigDecimal value = new
BigDecimal((Total_Trustworthiness_Value[m] / 6.9) * 100);
value = value.setScale(0, RoundingMode.UP);
System.out.print(value + "%");
System.out.print(" ");
}

log("\n" + "-----");
-----");
log("\n");

log(" [3] Security Compliance Assessment (SCA) ");
log("-----");
-----");
log(" NA");

log("\n");
log("\n");

log(" [4] Cloud Security Alliance (CSA) ");
log("-----");
-----");
log(" NA");

log("\n\n");

log("-----");
-----");
log("Cloud Providers Ranking" + "\n"
+ "-----");
-----");

int temp_value = 0;
int temp_CPID = 0;

for (int i = 0; i < Total_Trustworthiness_Value.length; i++) {
    for (int j = 1; j < (Total_Trustworthiness_Value.length -
i); j++) {

```

```

        if (Total_Trustworthiness_Value[j - 1]
<Total_Trustworthiness_Value[j]) {
            // Sorting the Trustworthiness Scores

            temp_value = (int)
Total_Trustworthiness_Value[j - 1];
Total_Trustworthiness_Value[j - 1] =
Total_Trustworthiness_Value[j];
Total_Trustworthiness_Value[j] = temp_value;

            // Sorting the Cloud Providers' IDs
temp_CPID = (int) CPID[j - 1];
CPID[j - 1] = CPID[j];
CPID[j] = temp_CPID;

        }
    }

    // Printing in Ascending order

    for (int k = 0; k < Total_Trustworthiness_Value.length; k++)
        if (CPID[k] >= 1 && CPID[k] <= 9)
            log("Rank (" + (k + 1) + ") Cloud Provider ID # " +
CPID[k] + "   Scored : "
                + Total_Trustworthiness_Value[k]);
        elseif (CPID[k] >= 10 && CPID[k] <= 99)
            log("Rank (" + (k + 1) + ") Cloud Provider ID # " +
CPID[k] + "   Scored : "
                + Total_Trustworthiness_Value[k]);
        else
            log("Rank (" + (k + 1) + ") Cloud Provider ID # " +
CPID[k] + "   Scored : "
                + Total_Trustworthiness_Value[k]);

    // Printing the CloudAdvisor's Trustworthiness Results (Second
version
// of Pauley's results)

    log("\n" + "-----");
    log("\n");
    log("+++++");
    log("+ Transparency Measurement Results +");
    log("+++++");
    log("\n");

    log("-----");
    log(" [1] Cloud Provider Transparency Scorecard (CPTS) Results
");
    log("-----");
    log("      NA");
    log("\n");

    log("-----");
    log(" [2] CloudAdvisor Transparency Results ");
    log("-----");

```



```

log("\n");

for (intk = 0; k<NCP; k++) {

    int[] ControlGroups = { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
}; // Defining
    // an
    // array
    // for
    // the
    // control
    // group
    int[] CGID = { 6, 8, 8, 3, 34, 2, 4, 5, 5, 8, 11 }; //
Defining the
    // number of
    // controls in each
    // Control Group

    int[] CO = { 1, 7, 2, 1, 2, 3 }; // Defining the number
of questions
                                                    //
in
    // each CGID
    int[] DG = { 1, 5, 2, 2, 2, 1, 2, 1 };
    int[] FS = { 1, 1, 1, 1, 1, 1, 1, 2 };
    int[] HRS = { 1, 2, 1 };
    int[] IS = { 1, 1, 3, 3, 1, 2, 2, 2, 2, 3, 2, 2, 1, 1, 1,
3, 3, 2, 4, 6, 2, 3, 2, 4, 2, 3, 2, 2, 1, 1, 2, 1,
    2, 3 };
    int[] LG = { 1, 3 };
    int[] OP = { 1, 1, 2, 5 };
    int[] RI = { 2, 2, 3, 1, 7 };
    int[] RM = { 1, 1, 1, 2, 1 };
    int[] RS = { 1, 3, 2, 1, 1, 1, 1, 2 };
    int[] SA = { 1, 7, 1, 3, 1, 2, 1, 1, 4, 3, 1, 1, 1, 3, 2
};

    log(" Cloud Provider (" + (CPID[k]) + ")");
    // log("\n");
    /*
    * for (int i = 0; i < 11; i++) { log("Control Group
:" +
    * ControlGroups[i]); log("Control Group ID :" +
CGID[i]); if (i ==
    * 0) log("Control ID Questions : " +
Arrays.toString(CO)); else if
    * (i == 1) log("Control ID Questions : " +
Arrays.toString(DG));
    * else if (i == 2) log("Control ID Questions : " +
    * Arrays.toString(FS)); else if (i == 3) log(
    * "Control ID Questions : " + Arrays.toString(HRS));
else if (i ==
    * 4) log("Control ID Questions : " +
Arrays.toString(IS)); else if
    * (i == 5) log("Control ID Questions : " +
Arrays.toString(LG));
    * else if (i == 6) log("Control ID Questions : " +
    * Arrays.toString(OP)); else if (i == 7) log(
    * "Control ID Questions : " + Arrays.toString(RI)); else
if (i ==

```

```

        * 8) log("Control ID Questions : " +
Arrays.toString(RM)); else if
        * (i == 9) log("Control ID Questions : " +
Arrays.toString(RS));
        * else log("Control ID Questions : " +
Arrays.toString(SA));
        *
        * log("\n"); }
    */

    doubleResponse;
    doubleComment;
    doubleEvidence;
    doublePublished;
    doubleAudited;

    doubleResponse_Score;
    doubleComment_Score;
    doubleEvidence_Score;
    doublePublished_Score;
    doubleAudited_Score;

    double[] CO_Scores = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0 };
    doubleCO_Scores_Percentage;
    doubleCO_Total = 0.0;

    double[] CO_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0
};

    doubleCO_Scores_Percentage_SCA;
    doubleCO_Total_SCA = 0.0;

    // Calculate the scores for Control ID Questions

    // #1 Compliance

    for (inti = 0; i<CO.length; i++) {
        while (CO[i] > 0) {

            Response = randomGenerator.nextInt(2);
            Comment = randomGenerator.nextInt(2);
            Evidence = randomGenerator.nextInt(2);
            ;
            Published = randomGenerator.nextInt(2);
            Audited = randomGenerator.nextInt(2);

            /*
            * log("CO.0" + (i + 1) + "." + (CO[i]));
log("Response  :"
            * + Response); log("Comment  :" + Comment);
log(
            * "Evidence  :" + Evidence); log("Published
:" +
            * Published); log("Audited  :" + Audited);
            * log("=====");
            */

            if (Response == 0)
                Response_Score = 0.0;
            else
                Response_Score = 1.0;
            if (Comment == 0)

```

```

        Comment_Score = 0.0;
    else
        Comment_Score = 1.0;
    if (Evidence == 0)
        Evidence_Score = 0.0;
    else
        Evidence_Score = 1.0;
    if (Published == 0)
        Published_Score = 0.0;
    else
        Published_Score = 1.0;
    if (Audited == 0)
        Audited_Score = 0.0;
    else
        Audited_Score = 1.0;

    CO_Scores[i] = CO_Scores[i]
        + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);
    CO_Scores_SCA[i] = CO_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

    /*
    * log("Compliance Score : " +
CO_Scores[i]);
    * log("=====");
    */

    CO[i] = CO[i] - 1;
}

}

// #2 Data Governance

double[] DG_Scores = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0 };

double DG_Scores_Percentage;
double DG_Total = 0.0;

double[] DG_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0 };

double DG_Scores_Percentage_SCA;
double DG_Total_SCA = 0.0;

log("=====");

for (inti = 0; i<DG.length; i++) {
    while (DG[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;
        Published = randomGenerator.nextInt(2);
        Audited = randomGenerator.nextInt(2);

        /*
        * log("DG.0" + (i + 1) + "." + (DG[i]));
log("Response : "

```

```

log(
:" +
* + Response); log("Comment   :" + Comment);
* "Evidence   :" + Evidence); log("Published
* Published); log("Audited   :" + Audited);
* log("=====");
*/

if (Response == 0)
    Response_Score = 0.0;
else
    Response_Score = 1.0;
if (Comment == 0)
    Comment_Score = 0.0;
else
    Comment_Score = 1.0;
if (Evidence == 0)
    Evidence_Score = 0.0;
else
    Evidence_Score = 1.0;
if (Published == 0)
    Published_Score = 0.0;
else
    Published_Score = 1.0;
if (Audited == 0)
    Audited_Score = 0.0;
else
    Audited_Score = 1.0;

DG_Scores[i] = DG_Scores[i]
                + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);

DG_Scores_SCA[i] = DG_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

/*
* log("Data Governance Score   : " +
* log("=====");
*/
DG[i] = DG[i] - 1;
}
}

// #3 Facility Security

double[] FS_Scores = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0 };

doubleFS_Scores_Percentage;
doubleFS_Total = 0.0;

double[] FS_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0 };

doubleFS_Scores_Percentage_SCA;
doubleFS_Total_SCA = 0.0;

for (inti = 0; i<FS.length; i++) {
    while (FS[i] > 0) {

```

```

Response = randomGenerator.nextInt(2);
Comment = randomGenerator.nextInt(2);
Evidence = randomGenerator.nextInt(2);
;
Published = randomGenerator.nextInt(2);
Audited = randomGenerator.nextInt(2);

/*
 * log("FS.0" + (i + 1) + "." + (FS[i]));
 * + Response); log("Comment   :" + Comment);
 * "Evidence   :" + Evidence); log("Published
 * Published); log("Audited   :" + Audited);
 * log("=====");
 */
if (Response == 0)
    Response_Score = 0.0;
else
    Response_Score = 1.0;
if (Comment == 0)
    Comment_Score = 0.0;
else
    Comment_Score = 1.0;
if (Evidence == 0)
    Evidence_Score = 0.0;
else
    Evidence_Score = 1.0;
if (Published == 0)
    Published_Score = 0.0;
else
    Published_Score = 1.0;
if (Audited == 0)
    Audited_Score = 0.0;
else
    Audited_Score = 1.0;

FS_Scores[i] = FS_Scores[i]
                + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);

FS_Scores_SCA[i] = FS_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

/*
 * log("Facility Security Score   : " +
 * log("=====");
 */
FS[i] = FS[i] - 1;
}

}

// #4 HR Security

double[] HR_Scores = { 0.0, 0.0, 0.0 };
doubleHR_Scores_Percentage;

```

```

doubleHR_Total = 0.0;

double[] HR_Scores_SCA = { 0.0, 0.0, 0.0 };
doubleHR_Scores_Percentage_SCA;
doubleHR_Total_SCA = 0.0;

for (inti = 0; i<HRS.length; i++) {
    while (HRS[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;
        Published = randomGenerator.nextInt(2);
        Audited = randomGenerator.nextInt(2);

        /*
        * log("HR.0" + (i + 1) + "." + (HRS[i]));
        * + Response); log("Comment   :" + Comment);
        * "Evidence   :" + Evidence); log("Published
        * Published); log("Audited   :" + Audited);
        * log("=====");
        */
        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
        else
            Evidence_Score = 1.0;
        if (Published == 0)
            Published_Score = 0.0;
        else
            Published_Score = 1.0;
        if (Audited == 0)
            Audited_Score = 0.0;
        else
            Audited_Score = 1.0;

        HR_Scores[i] = HR_Scores[i]
            + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);
        HR_Scores_SCA[i] = HR_Scores_SCA[i] +
        ((Response_Score + Comment_Score + Evidence_Score) / 5);

        /*
        * log("HR Security Score       : " +
        * log("=====");
        */

        HRS[i] = HRS[i] - 1;
    }
}

```

```

    }
}

// #5 IS Security

double[] IS_Scores = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0 };
double IS_Scores_Percentage;
double IS_Total = 0.0;

double[] IS_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0 };
double IS_Scores_Percentage_SCA;
double IS_Total_SCA = 0.0;

for (inti = 0; i<IS.length; i++) {
    while (IS[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;
        Published = randomGenerator.nextInt(2);
        Audited = randomGenerator.nextInt(2);

        /*
        * log("IS.0" + (i + 1) + "." + (IS[i]));
        * + Response); log("Comment    :" + Comment);
        * "Evidence    :" + Evidence); log("Published
        * Published); log("Audited    :" + Audited);
        * log("=====");
        */

        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
        else
            Evidence_Score = 1.0;
        if (Published == 0)
            Published_Score = 0.0;
        else
            Published_Score = 1.0;
        if (Audited == 0)
            Audited_Score = 0.0;
        else
            Audited_Score = 1.0;
    }
}

```

```

        IS_Scores[i] = IS_Scores[i]
                    + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);

        IS_Scores_SCA[i] = IS_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

        /*
        * log("IS Security Score          : " +
IS_Scores[i]);
        * log("=====");
        */

        IS[i] = IS[i] - 1;
    }

}

// #6 Legal

double[] LG_Scores = { 0.0, 0.0 };
double LG_Scores_Percentage;
double LG_Total = 0.0;

double[] LG_Scores_SCA = { 0.0, 0.0 };
double LG_Scores_Percentage_SCA;
double LG_Total_SCA = 0.0;

for (inti = 0; i<LG.length; i++) {
    while (LG[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;
        Published = randomGenerator.nextInt(2);
        Audited = randomGenerator.nextInt(2);

        /*
        * log("LG.0" + (i + 1) + "." + (LG[i]));
        * + Response); log("Comment      : " + Comment);
        * "Evidence      : " + Evidence); log("Published
log("Response      : "
log(
:" +

        * Published); log("Audited      : " + Audited);
        * log("=====");
        */

        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
    }
}

```



```

        else
            Evidence_Score = 1.0;
        if (Published == 0)
            Published_Score = 0.0;
        else
            Published_Score = 1.0;
        if (Audited == 0)
            Audited_Score = 0.0;
        else
            Audited_Score = 1.0;

        LG_Scores[i] = LG_Scores[i]
            + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);

        LG_Scores_SCA[i] = LG_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

        /*
        * log("LG Security Score      : " +
LG_Scores[i]);
        * log("=====");
        */
        LG[i] = LG[i] - 1;
    }
}

// #7 Operations Management

double[] OP_Scores = { 0.0, 0.0, 0.0, 0.0 };
doubleOP_Scores_Percentage;
doubleOP_Total = 0.0;

double[] OP_Scores_SCA = { 0.0, 0.0, 0.0, 0.0 };
doubleOP_Scores_Percentage_SCA;
doubleOP_Total_SCA = 0.0;

for (inti = 0; i<OP.length; i++) {
    while (OP[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;
        Published = randomGenerator.nextInt(2);
        Audited = randomGenerator.nextInt(2);

        /*
        * log("OP.0" + (i + 1) + "." + (OP[i]));
log("Response  : "
        * + Response); log("Comment  : " + Comment);
log(
        * "Evidence  : " + Evidence); log("Published
        * Published); log("Audited  : " + Audited);
        * log("=====");
        */
    }
}

```

```

        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
        else
            Evidence_Score = 1.0;
        if (Published == 0)
            Published_Score = 0.0;
        else
            Published_Score = 1.0;
        if (Audited == 0)
            Audited_Score = 0.0;
        else
            Audited_Score = 1.0;

        OP_Scores[i] = OP_Scores[i]
            + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);

        OP_Scores_SCA[i] = OP_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

        /*
        * log("OP Security Score          : " +
        * log("=====");
        */

OP_Scores[i]);
log("\n");

        OP[i] = OP[i] - 1;
    }

}

// #8 Risk Management

double[] RI_Scores = { 0.0, 0.0, 0.0, 0.0, 0.0 };
double RI_Scores_Percentage;
double RI_Total = 0.0;

double[] RI_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0 };
double RI_Scores_Percentage_SCA;
double RI_Total_SCA = 0.0;

for (inti = 0; i<RI.length; i++) {
    while (RI[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;
        Published = randomGenerator.nextInt(2);
        Audited = randomGenerator.nextInt(2);

        /*

```

```

log("Response  : "
log(
:" +
* log("RI.0" + (i + 1) + "." + (RI[i]));
* + Response); log("Comment  : " + Comment);
* "Evidence  : " + Evidence); log("Published
* Published); log("Audited  : " + Audited);
* log("=====");
*/

if (Response == 0)
    Response_Score = 0.0;
else
    Response_Score = 1.0;
if (Comment == 0)
    Comment_Score = 0.0;
else
    Comment_Score = 1.0;
if (Evidence == 0)
    Evidence_Score = 0.0;
else
    Evidence_Score = 1.0;
if (Published == 0)
    Published_Score = 0.0;
else
    Published_Score = 1.0;
if (Audited == 0)
    Audited_Score = 0.0;
else
    Audited_Score = 1.0;

    RI_Scores[i] = RI_Scores[i]
        + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);
    RI_Scores_SCA[i] = RI_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

/*
* log("RI Security Score      : " +
* log("=====");
*/

RI_Scores[i]);
log("\n");

    RI[i] = RI[i] - 1;
}
}

// #9 Release Management

double[] RM_Scores = { 0.0, 0.0, 0.0, 0.0, 0.0 };
doubleRM_Scores_Percentage;
doubleRM_Total = 0.0;

double[] RM_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0 };
doubleRM_Scores_Percentage_SCA;
doubleRM_Total_SCA = 0.0;

for (inti = 0; i<RM.length; i++) {
    while (RM[i] > 0) {

```

```

Response = randomGenerator.nextInt(2);
Comment = randomGenerator.nextInt(2);
Evidence = randomGenerator.nextInt(2);
;
Published = randomGenerator.nextInt(2);
Audited = randomGenerator.nextInt(2);

/*
 * log("RM.0" + (i + 1) + "." + (RM[i]));
 * + Response); log("Comment   :" + Comment);
 * "Evidence   :" + Evidence); log("Published
 * Published); log("Audited   :" + Audited);
 * log("=====");
 */

if (Response == 0)
    Response_Score = 0.0;
else
    Response_Score = 1.0;
if (Comment == 0)
    Comment_Score = 0.0;
else
    Comment_Score = 1.0;
if (Evidence == 0)
    Evidence_Score = 0.0;
else
    Evidence_Score = 1.0;
if (Published == 0)
    Published_Score = 0.0;
else
    Published_Score = 1.0;
if (Audited == 0)
    Audited_Score = 0.0;
else
    Audited_Score = 1.0;

RM_Scores[i] = RM_Scores[i]
                + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);

RM_Scores_SCA[i] = RM_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

/*
 * log("RM Security Score           : " +
 * log("=====");
 */

RM[i] = RM[i] - 1;
}

}

// #10 Resiliency

```

```

0.0 };

double[] RS_Scores = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0 };

double RS_Scores_Percentage;
double RS_Total = 0.0;

double[] RS_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0 };

double RS_Scores_Percentage_SCA;
double RS_Total_SCA = 0.0;

for (inti = 0; i<RS.length; i++) {
    while (RS[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;
        Published = randomGenerator.nextInt(2);
        Audited = randomGenerator.nextInt(2);

        /*
        * log("RS.0" + (i + 1) + "." + (RS[i]));
        * + Response); log("Comment   :" + Comment);
        * "Evidence   :" + Evidence); log("Published
        * Published); log("Audited   :" + Audited);
        * log("=====");
        */

        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
        else
            Evidence_Score = 1.0;
        if (Published == 0)
            Published_Score = 0.0;
        else
            Published_Score = 1.0;
        if (Audited == 0)
            Audited_Score = 0.0;
        else
            Audited_Score = 1.0;

        RS_Scores[i] = RS_Scores[i]
            + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);

        RS_Scores_SCA[i] = RS_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

        /*

```

```

RS_Scores[i]);
log("\n");

    * log("RS Security Score      : " +
    * log("=====");
    */
    RS[i] = RS[i] - 1;
}
}

// #11 Security Architecture

double[] SA_Scores = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0 };
double SA_Scores_Percentage;
double SA_Total = 0.0;

double[] SA_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0 };
double SA_Scores_Percentage_SCA;
double SA_Total_SCA = 0.0;

for (inti = 0; i<SA.length; i++) {
    while (SA[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;
        Published = randomGenerator.nextInt(2);
        Audited = randomGenerator.nextInt(2);

        /*
        * log("SA.0" + (i + 1) + "." + (SA[i]));
        * + Response); log("Comment      : " + Comment);
        * "Evidence      : " + Evidence); log("Published
        * Published); log("Audited      : " + Audited);
        * log("=====");
        */

        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
        else
            Evidence_Score = 1.0;
        if (Published == 0)
            Published_Score = 0.0;
        else
            Published_Score = 1.0;
        if (Audited == 0)

```

```

        Audited_Score = 0.0;
    else
        Audited_Score = 1.0;

    SA_Scores[i] = SA_Scores[i]
        + ((Response_Score +
Comment_Score + Evidence_Score + Published_Score + Audited_Score) / 5);

    SA_Scores_SCA[i] = SA_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

    /*
    * log("SA Security Score          : " +
SA_Scores[i]);
    * log("=====");
    */

    SA[i] = SA[i] - 1;
}

}

// CloudAdvisor Transparency Results
// Printing Total Compliance Score
for (
int j = 0; j<CO.length; j++)
{
    CO_Total = CO_Total + CO_Scores[j];
    CO_Total_SCA = CO_Total_SCA + CO_Scores_SCA[j];
}

log("Total Compliance Score          : " + CO_Total +
"/16");

CO_Scores_Percentage = Math.round((CO_Total / 16) * 100);
log("Compliance Percentage          : " +
CO_Scores_Percentage + "/100.0");

log("=====");

// Printing Total Data Governance Score
for (int j = 0; j<DG.length; j++) {
    DG_Total = DG_Total + DG_Scores[j];
    DG_Total_SCA = DG_Total_SCA + DG_Scores_SCA[j];
}

log("Total Data Governance Score      : " + DG_Total +
"/16");

DG_Scores_Percentage = Math.round((DG_Total / 16) * 100);
log("Data Governance Percentage      : " +
DG_Scores_Percentage + "/100.0");

```

```

log("=====");

// Printing Total Facility Security Score
for (int j = 0; j<FS.length; j++) {
    FS_Total = FS_Total + FS_Scores[j];
    FS_Total_SCA = FS_Total_SCA + FS_Scores_SCA[j];
}

log("Total Facility Security Score      : " + FS_Total +
"/11");
FS_Scores_Percentage = Math.round((FS_Total / 11) * 100);
log("Facility Security Percentage      : " +
FS_Scores_Percentage + "/100.0");

log("=====");

// Printing Total HR Security Score
for (int j = 0; j<HRS.length; j++) {
    HR_Total = HR_Total + HR_Scores[j];
    HR_Total_SCA = HR_Total_SCA + HR_Scores_SCA[j];
}

log("Total HR Security Score            : " + HR_Total +
"/4");
HR_Scores_Percentage = Math.round((HR_Total / 4) * 100);
log("HR Security Percentage            : " +
HR_Scores_Percentage + "/100.0");

log("=====");

// Printing Total IS Security Score
for (int j = 0; j<IS.length; j++) {
    IS_Total = IS_Total + IS_Scores[j];
    IS_Total_SCA = IS_Total_SCA + IS_Scores_SCA[j];
}

log("Total IS Security Score            : " + IS_Total +
"/74");
IS_Scores_Percentage = Math.round((IS_Total / 74) * 100);
log("IS Security Percentage            : " +
IS_Scores_Percentage + "/100.0");

log("=====");

// Printing Total LG Score
for (int j = 0; j<LG.length; j++) {
    LG_Total = LG_Total + LG_Scores[j];
    LG_Total_SCA = LG_Total_SCA + LG_Scores_SCA[j];
}

```



```

        log("Total Legal Score           : " + LG_Total +
"/4");
        LG_Scores_Percentage = Math.round((LG_Total / 4) * 100);
        log("Legal Percentage           : " +
LG_Scores_Percentage + "/100.0");

    log("=====");

    // Printing Total OP Score

    for (int j = 0; j<OP.length; j++) {
        OP_Total = OP_Total + OP_Scores[j];
        OP_Total_SCA = OP_Total_SCA + OP_Scores_SCA[j];
    }

    log("Total Operation Management Score : " + OP_Total +
"/9");
    OP_Scores_Percentage = Math.round((OP_Total / 9) * 100);
    log("Operation Management Percentage : " +
OP_Scores_Percentage + "/100.0");

    log("=====");

    // Printing Total RI Score

    for (int j = 0; j<RI.length; j++) {
        RI_Total = RI_Total + RI_Scores[j];
        RI_Total_SCA = RI_Total_SCA + RI_Scores_SCA[j];
    }

    log("Total Risk Management Score     : " + RI_Total +
"/15");
    RI_Scores_Percentage = Math.round((RI_Total / 15) * 100);
    log("Risk Management Percentage     : " +
RI_Scores_Percentage + "/100.0");

    log("=====");

    // Printing Total RM Score

    for (int j = 0; j<RM.length; j++) {
        RM_Total = RM_Total + RM_Scores[j];
        RM_Total_SCA = RM_Total_SCA + RM_Scores_SCA[j];
    }

    log("Total Release Management Score   : " + RM_Total +
"/6");
    RM_Scores_Percentage = Math.round((RM_Total / 6) * 100);
    log("Release Management Percentage   : " +
RM_Scores_Percentage + "/100.0");

    log("=====");

```

```

// Printing Total RS Score

for (int j = 0; j < RS.length; j++) {
    RS_Total = RS_Total + RS_Scores[j];
    RS_Total_SCA = RS_Total_SCA + RS_Scores_SCA[j];
}

log("Total Resiliency Score           : " + RS_Total +
"/12");
RS_Scores_Percentage = Math.round((RS_Total / 12) * 100);
log("Resiliency Percentage           : " +
RS_Scores_Percentage + "/100.0");

log("=====");

// Printing Total SA Score

for (int j = 0; j < SA.length; j++) {
    SA_Total = SA_Total + SA_Scores[j];
    SA_Total_SCA = SA_Total_SCA + SA_Scores_SCA[j];
}

log("Total Security Architecture Score : " + SA_Total +
"/32");
SA_Scores_Percentage = Math.round((SA_Total / 32) * 100);
log("Security Architecture Percentage : " +
SA_Scores_Percentage + "/100.0");

log("=====");
log("\n");
}

// Printing Security Compliance Assessment Transparency Results
log("-----");
log(" [3] Security Compliance Assessment (SCA) Transparency
Results ");
log("-----");
log("\n");

for (int k = 0; k < NCP; k++) {
    int[] ControlGroups = { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
}; // Defining
    // an
    // array
    // for
    // the
    // control
    // group
    int[] CGID = { 6, 8, 8, 3, 34, 2, 4, 5, 5, 8, 11 }; //
Defining the
    // number of
    // controls in each
    // Control Group

```

```

of questions      int[] CO = { 1, 7, 2, 1, 2, 3 }; // Defining the number
                                                           //
in
    // each CGID
    int[] DG = { 1, 5, 2, 2, 2, 1, 2, 1 };
    int[] FS = { 1, 1, 1, 1, 1, 1, 1, 2 };
    int[] HRS = { 1, 2, 1 };
    int[] IS = { 1, 1, 3, 3, 1, 2, 2, 2, 2, 3, 2, 2, 1, 1, 1,
3, 3, 2, 4, 6, 2, 3, 2, 4, 2, 3, 2, 2, 1, 1, 2, 1,
                2, 3 };
    int[] LG = { 1, 3 };
    int[] OP = { 1, 1, 2, 5 };
    int[] RI = { 2, 2, 3, 1, 7 };
    int[] RM = { 1, 1, 1, 2, 1 };
    int[] RS = { 1, 3, 2, 1, 1, 1, 1, 2 };
    int[] SA = { 1, 7, 1, 3, 1, 2, 1, 1, 4, 3, 1, 1, 1, 3, 2
};

    log(" Cloud Provider (" + (CPID[k]) + ")");

    doubleResponse;
    doubleComment;
    doubleEvidence;

    doubleResponse_Score;
    doubleComment_Score;
    doubleEvidence_Score;

    double[] CO_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0
};

    doubleCO_Scores_Percentage_SCA;
    doubleCO_Total_SCA = 0.0;

    // Calculate the scores for Control ID Questions

    // #1 Compliance

    for (inti = 0; i<CO.length; i++) {
        while (CO[i] > 0) {

            Response = randomGenerator.nextInt(2);
            Comment = randomGenerator.nextInt(2);
            Evidence = randomGenerator.nextInt(2);
            ;

            if (Response == 0)
                Response_Score = 0.0;
            else
                Response_Score = 1.0;
            if (Comment == 0)
                Comment_Score = 0.0;
            else
                Comment_Score = 1.0;
            if (Evidence == 0)
                Evidence_Score = 0.0;
            else
                Evidence_Score = 1.0;
            CO_Scores_SCA[i] = CO_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

```

```

        CO[i] = CO[i] - 1;
    }
}

// #2 Data Governance
double[] DG_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0 };
double DG_Scores_Percentage_SCA;
double DG_Total_SCA = 0.0;

log("=====");

for (inti = 0; i<DG.length; i++) {
    while (DG[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;

        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
        else
            Evidence_Score = 1.0;

        DG_Scores_SCA[i] = DG_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

        DG[i] = DG[i] - 1;
    }
}

// #3 Facility Security
double[] FS_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0 };
double FS_Scores_Percentage_SCA;
double FS_Total_SCA = 0.0;

for (inti = 0; i<FS.length; i++) {
    while (FS[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;

        if (Response == 0)

```

```

        Response_Score = 0.0;
    else
        Response_Score = 1.0;
    if (Comment == 0)
        Comment_Score = 0.0;
    else
        Comment_Score = 1.0;
    if (Evidence == 0)
        Evidence_Score = 0.0;
    else
        Evidence_Score = 1.0;
    FS_Scores_SCA[i] = FS_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

    FS[i] = FS[i] - 1;
}

}

// #4 HR Security

double[] HR_Scores_SCA = { 0.0, 0.0, 0.0 };
doubleHR_Scores_Percentage_SCA;
doubleHR_Total_SCA = 0.0;

for (inti = 0; i<HRS.length; i++) {
    while (HRS[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;

        /*
        * log("HR.0" + (i + 1) + "." + (HRS[i]));
        * + Response); log("Comment   :" + Comment);
        * "Evidence   :" + Evidence); log("Published
        * Published); log("Audited   :" + Audited);
        * log("=====");
        */
        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
        else
            Evidence_Score = 1.0;
        HR_Scores_SCA[i] = HR_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

        /*
        * log("HR Security Score       : " +
HR_Scores[i]);

```

```

log("\n");

        * log("=====");
        */

        HRS[i] = HRS[i] - 1;
    }

}

// #5 IS Security

    double[] IS_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
                                0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0 };
    double IS_Scores_Percentage_SCA;
    double IS_Total_SCA = 0.0;

    for (int i = 0; i < IS.length; i++) {
        while (IS[i] > 0) {

            Response = randomGenerator.nextInt(2);
            Comment = randomGenerator.nextInt(2);
            Evidence = randomGenerator.nextInt(2);
            ;

            /*
            * log("IS.0" + (i + 1) + "." + (IS[i]));
log("Response  :",
log(
:" +
            * + Response); log("Comment  :", Comment);
            * "Evidence  :", Evidence); log("Published
            * Published); log("Audited  :", Audited);
            * log("=====");
            */

            if (Response == 0)
                Response_Score = 0.0;
            else
                Response_Score = 1.0;
            if (Comment == 0)
                Comment_Score = 0.0;
            else
                Comment_Score = 1.0;
            if (Evidence == 0)
                Evidence_Score = 0.0;
            else
                Evidence_Score = 1.0;

            IS_Scores_SCA[i] = IS_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

            /*
            * log("IS Security Score  :",
IS_Scores[i]);
log("\n");
            * log("=====");
            */

            IS[i] = IS[i] - 1;
        }
    }
}

```

```

    }
}

// #6 Legal

double[] LG_Scores_SCA = { 0.0, 0.0 };
double LG_Scores_Percentage_SCA;
double LG_Total_SCA = 0.0;

for (int i = 0; i < LG.length; i++) {
    while (LG[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;

        /*
        * log("LG.0" + (i + 1) + "." + (LG[i]));
log("Response  :"
log(
:" +
        * + Response); log("Comment  :" + Comment);
        * "Evidence  :" + Evidence); log("Published
        * Published); log("Audited  :" + Audited);
        * log("=====");
        */

        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
        else
            Evidence_Score = 1.0;

        LG_Scores_SCA[i] = LG_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

        /*
        * log("LG Security Score      : " +
LG_Scores[i]);
        * log("=====");
        */

        LG[i] = LG[i] - 1;
    }
}

// #7 Operations Management

double[] OP_Scores_SCA = { 0.0, 0.0, 0.0, 0.0 };
double OP_Scores_Percentage_SCA;

```

```

double OP_Total_SCA = 0.0;

for (inti = 0; i<OP.length; i++) {
    while (OP[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;

        /*
        * log("OP.0" + (i + 1) + "." + (OP[i]));
log("Response  :"
        * + Response); log("Comment  :" + Comment);
log(
        * "Evidence  :" + Evidence); log("Published
:" +
        * Published); log("Audited  :" + Audited);
        * log("=====");
        */

        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
        else
            Evidence_Score = 1.0;

        OP_Scores_SCA[i] = OP_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

        /*
        * log("OP Security Score      : " +
log(OP_Scores[i]);
        * log("=====");
log("\n");
        */

        OP[i] = OP[i] - 1;
    }
}

// #8 Risk Management

double[] RI_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0 };
double RI_Scores_Percentage_SCA;
double RI_Total_SCA = 0.0;

for (inti = 0; i<RI.length; i++) {
    while (RI[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);

```



```

;
/*
* log("RI.0" + (i + 1) + "." + (RI[i]));
log("Response  :"
* + Response); log("Comment  :" + Comment);
log(
* "Evidence  :" + Evidence); log("Published
:" +
* Published); log("Audited  :" + Audited);
* log("=====");
*/

if (Response == 0)
    Response_Score = 0.0;
else
    Response_Score = 1.0;
if (Comment == 0)
    Comment_Score = 0.0;
else
    Comment_Score = 1.0;
if (Evidence == 0)
    Evidence_Score = 0.0;
else
    Evidence_Score = 1.0;
RI_Scores_SCA[i] = RI_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

/*
* log("RI Security Score      : " +
* log("=====");
*/

RI_Scores[i]);
log("\n");

RI[i] = RI[i] - 1;
}
}

// #9 Release Management

double[] RM_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0 };
doubleRM_Scores_Percentage_SCA;
doubleRM_Total_SCA = 0.0;

for (inti = 0; i<RM.length; i++) {
    while (RM[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;

/*
* log("RM.0" + (i + 1) + "." + (RM[i]));
log("Response  :"
* + Response); log("Comment  :" + Comment);
log(
* "Evidence  :" + Evidence); log("Published
:" +

```

```

        * Published); log("Audited      :" + Audited);
        * log("=====");
        */

        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;
        else
            Evidence_Score = 1.0;

        RM_Scores_SCA[i] = RM_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

        /*
        * log("RM Security Score      : " +
RM_Scores[i]);
        * log("=====");
        */

        RM[i] = RM[i] - 1;
    }
}

// #10 Resiliency
double[] RS_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0 };
double RS_Scores_Percentage_SCA;
double RS_Total_SCA = 0.0;

for (inti = 0; i<RS.length; i++) {
    while (RS[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;

        /*
        * log("RS.0" + (i + 1) + "." + (RS[i]));
log("Response  : "
        * + Response); log("Comment      : " + Comment);
log(
        * "Evidence  : " + Evidence); log("Published
:" +
        * Published); log("Audited      : " + Audited);
        * log("=====");
        */

        if (Response == 0)
            Response_Score = 0.0;
        else

```

```

        Response_Score = 1.0;
    if (Comment == 0)
        Comment_Score = 0.0;
    else
        Comment_Score = 1.0;
    if (Evidence == 0)
        Evidence_Score = 0.0;
    else
        Evidence_Score = 1.0;

    RS_Scores_SCA[i] = RS_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

    /*
    * log("RS Security Score      : " +
RS_Scores[i]);
    * log("=====");
    */
    RS[i] = RS[i] - 1;
}

}

// #11 Security Architecture

double[] SA_Scores_SCA = { 0.0, 0.0, 0.0, 0.0, 0.0, 0.0,
0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0, 0.0 };
doubleSA_Scores_Percentage_SCA;
doubleSA_Total_SCA = 0.0;

for (inti = 0; i<SA.length; i++) {
    while (SA[i] > 0) {

        Response = randomGenerator.nextInt(2);
        Comment = randomGenerator.nextInt(2);
        Evidence = randomGenerator.nextInt(2);
        ;

        /*
        * log("SA.0" + (i + 1) + "." + (SA[i]));
log("Response  : "
        * + Response); log("Comment  : " + Comment);
log(
        * "Evidence  : " + Evidence); log("Published
:" +
        * Published); log("Audited  : " + Audited);
        * log("=====");
        */

        if (Response == 0)
            Response_Score = 0.0;
        else
            Response_Score = 1.0;
        if (Comment == 0)
            Comment_Score = 0.0;
        else
            Comment_Score = 1.0;
        if (Evidence == 0)
            Evidence_Score = 0.0;

```

```

        else
            Evidence_Score = 1.0;

            SA_Scores_SCA[i] = SA_Scores_SCA[i] +
((Response_Score + Comment_Score + Evidence_Score) / 5);

            /*
            * log("SA Security Score          : " +
SA_Scores[i]);
            * log("=====");
            */

            SA[i] = SA[i] - 1;
        }
    }

    // CloudAdvisor Transparency Results

    // Printing Total Compliance Score

    for (
    int j = 0; j<CO.length; j++)
    {
        CO_Total_SCA = CO_Total_SCA + CO_Scores_SCA[j];
    }

    log("Total Compliance Score          : " +
CO_Total_SCA + "/16");
    CO_Scores_Percentage_SCA = Math.round((CO_Total_SCA / 16)
* 100);
    log("Compliance Percentage          : " +
CO_Scores_Percentage_SCA + "/100.0");

    log("=====");

    // Printing Total Data Governance Score

    for (int j = 0; j<DG.length; j++) {
        DG_Total_SCA = DG_Total_SCA + DG_Scores_SCA[j];
    }

    log("Total Data Governance Score      : " +
DG_Total_SCA + "/16");
    DG_Scores_Percentage_SCA = Math.round((DG_Total_SCA / 16)
* 100);
    log("Data Governance Percentage      : " +
DG_Scores_Percentage_SCA + "/100.0");

    log("=====");

    // Printing Total Facility Security Score

```

```

        for (int j = 0; j<FS.length; j++) {
            FS_Total_SCA = FS_Total_SCA + FS_Scores_SCA[j];
        }

        log("Total Facility Security Score      : " +
FS_Total_SCA + "/11");
        FS_Scores_Percentage_SCA = Math.round((FS_Total_SCA / 11)
* 100);
        log("Facility Security Percentage      : " +
FS_Scores_Percentage_SCA + "/100.0");

        log("=====");

        // Printing Total HR Security Score

        for (int j = 0; j<HRS.length; j++) {
            HR_Total_SCA = HR_Total_SCA + HR_Scores_SCA[j];
        }

        log("Total HR Security Score              : " +
HR_Total_SCA + "/4");
        HR_Scores_Percentage_SCA = Math.round((HR_Total_SCA / 4)
* 100);
        log("HR Security Percentage            : " +
HR_Scores_Percentage_SCA + "/100.0");

        log("=====");

        // Printing Total IS Security Score

        for (int j = 0; j<IS.length; j++) {
            IS_Total_SCA = IS_Total_SCA + IS_Scores_SCA[j];
        }

        log("Total IS Security Score              : " +
IS_Total_SCA + "/74");
        IS_Scores_Percentage_SCA = Math.round((IS_Total_SCA / 74)
* 100);
        log("IS Security Percentage            : " +
IS_Scores_Percentage_SCA + "/100.0");

        log("=====");

        // Printing Total LG Score

        for (int j = 0; j<LG.length; j++) {
            LG_Total_SCA = LG_Total_SCA + LG_Scores_SCA[j];
        }

```

```

        log("Total Legal Score           : " +
LG_Total_SCA + "/4");
        LG_Scores_Percentage_SCA = Math.round((LG_Total_SCA / 4)
* 100);
        log("Legal Percentage           : " +
LG_Scores_Percentage_SCA + "/100.0");

        log("=====");

        // Printing Total OP Score
        for (int j = 0; j<OP.length; j++) {
                OP_Total_SCA = OP_Total_SCA + OP_Scores_SCA[j];
        }

        log("Total Operation Management Score : " +
OP_Total_SCA + "/9");
        OP_Scores_Percentage_SCA = Math.round((OP_Total_SCA / 9)
* 100);
        log("Operation Management Percentage : " +
OP_Scores_Percentage_SCA + "/100.0");

        log("=====");

        // Printing Total RI Score
        for (int j = 0; j<RI.length; j++) {
                RI_Total_SCA = RI_Total_SCA + RI_Scores_SCA[j];
        }

        log("Total Risk Management Score           : " +
RI_Total_SCA + "/15");
        RI_Scores_Percentage_SCA = Math.round((RI_Total_SCA / 15)
* 100);
        log("Risk Management Percentage           : " +
RI_Scores_Percentage_SCA + "/100.0");

        log("=====");

        // Printing Total RM Score
        for (int j = 0; j<RM.length; j++) {
                RM_Total_SCA = RM_Total_SCA + RM_Scores_SCA[j];
        }

        log("Total Release Management Score           : " +
RM_Total_SCA + "/6");
        RM_Scores_Percentage_SCA = Math.round((RM_Total_SCA / 6)
* 100);
        log("Release Management Percentage           : " +
RM_Scores_Percentage_SCA + "/100.0");

```

```

log("=====");

    // Printing Total RS Score

    for (int j = 0; j<RS.length; j++) {

        RS_Total_SCA = RS_Total_SCA + RS_Scores_SCA[j];

    }

    log("Total Resiliency Score           : " +
RS_Total_SCA + "/12");
    RS_Scores_Percentage_SCA = Math.round((RS_Total_SCA / 12)
* 100);
    log("Resiliency Percentage           : " +
RS_Scores_Percentage_SCA + "/100.0");

log("=====");

    // Printing Total SA Score

    for (int j = 0; j<SA.length; j++) {

        SA_Total_SCA = SA_Total_SCA + SA_Scores_SCA[j];

    }

    log("Total Security Architecture Score : " +
SA_Total_SCA + "/32");
    SA_Scores_Percentage_SCA = Math.round((SA_Total_SCA / 32)
* 100);
    log("Security Architecture Percentage : " +
SA_Scores_Percentage_SCA + "/100.0");

log("=====");
    log("\n");

}

log("-----");
log(" [4] Cloud Security Alliance      (CSA) ");
log("-----");
log("      NA");

}
}

```

# Appendix C

## Simulation

### C.1 Data and Results

Number of Cloud Providers: 4

=====

Cloud Provider (2)

=====

Years in Business (4.0)

Memberships (9.0)

Published Evidence (3.0)

Security Breaches (2.0)

Published Evidence (1.0)

Privacy Breaches (6.0)

Published Evidence (3.0)

Outages (3.0)

Published Evidence (3.0)

DataLoss (7.0)

Published Evidence (4.0)



=====

Cloud Provider (91)

=====

Years in Business (22.0)

Memberships (2.0)

Published Evidence (0.0)

Privacy Breaches (4.0)

Published Evidence (4.0)

Outages (2.0)

Published Evidence (2.0)

DataLoss (8.0)

Published Evidence (7.0)

=====

Cloud Provider (14)

=====

Years in Business (15.0)

Memberships (5.0)

Published Evidence (5.0)

Security Breaches (4.0)

Published Evidence (1.0)

Privacy Breaches (7.0)

Published Evidence (4.0)

Outages (6.0)

Published Evidence (1.0)

DataLoss (2.0)

Published Evidence (0.0)

=====

Cloud Provider (49)

=====

Years in Business (22.0)

Memberships (3.0)

Published Evidence (2.0)

Security Breaches (1.0)

Published Evidence (0.0)

Privacy Breaches (2.0)

Published Evidence (0.0)

Outages (5.0)

Published Evidence (0.0)

-----

=====

## Trustworthiness Measurement Results

=====

**[1] Cloud Provider Transparency Scorecard (CPTS)**

	CP2	CP91	CP14	CP49	
Years of Business	0.0	1.0	1.0	1.0	
Membership	1.0	1.0	1.0	1.0	
Security Breach	0.0	1.0	0.0	0.0	
Privacy Breach	0.0	0.0	0.0	0.0	
Outages	0.0	0.0	0.0	0.0	
Data Loss	0.0	0.0	0.0	1.0	
Trustworthiness Score	1.0	3.0	2.0	3.0	
Trustworthiness %	17%	50%	34%	50%	

## [2] CloudAdvisor

---

	CP2	CP91	CP14	CP49
Years of Business	0.6	1.0	1.0	1.0
Membership	1.9 34%	1.2 0%	1.5 100%	1.3 67%
Security Breach	0.8 50%	1.0 NA	0.6 25%	0.9 0%
Privacy Breach	0.40 50%	0.6 100%	0.30 58%	0.8 0%
Outages	0.7 100%	0.8 100%	0.40 17%	0.5 0%
Data Loss	0.30 58%	0.20 0%	0.8 0%	1.0 NA
Trustworthiness Score	4.7	4.8	4.6	5.5
Trustworthiness %	69%	70%	67%	80%

---

## [3] Security Compliance Assessment (SCA)

NA

## [4] Cloud Security Alliance (CSA)

NA

---

### **Cloud Providers Ranking**

---

Rank (1) Cloud Provider ID # 49 Scored: 5.5

Rank (2) Cloud Provider ID # 91 Scored: 4.8

Rank (3) Cloud Provider ID # 14 Scored: 4.7

Rank (4) Cloud Provider ID # 2 Scored: 4.6

---

+++++

**+ Transparency Measurement Results +**

+++++

-----  
**[1] Cloud Provider Transparency Scorecard (CPTS) Results**  
-----

NA

-----  
**[2] CloudAdvisor Transparency Results**  
-----

**Cloud Provider (49)**

=====

Total Compliance Score : 8.6/16

Compliance Percentage : 54.0/100.0

=====

Total Data Governance Score : 7.0/16

Data Governance Percentage : 44.0/100.0

=====

Total Facility Security Score : 4.4/11

Facility Security Percentage : 40.0/100.0

=====

Total HR Security Score : 1.80/4

HR Security Percentage : 45.0/100.0

=====

Total IS Security Score : 35.8/74

IS Security Percentage : 48.0/100.0

=====  
Total Legal Score : 2.6/4

Legal Percentage : 65.0/100.0  
=====

Total Operation Management Score : 4.0/9

Operation Management Percentage : 44.0/100.0  
=====

Total Risk Management Score : 8.2/15

Risk Management Percentage : 55.0/100.0  
=====

Total Release Management Score : 3.0/6

Release Management Percentage : 50.0/100.0  
=====

Total Resiliency Score : 6.4/12

Resiliency Percentage : 53.0/100.0  
=====

Total Security Architecture Score: 14.4/32

Security Architecture Percentage : 45.0/100.0

=====  
**Cloud Provider (91)**  
=====

Total Compliance Score : 7.2/16

Compliance Percentage : 45.0/100.0  
=====

Total Data Governance Score : 9.0/16

Data Governance Percentage : 56.0/100.0  
=====

Total Facility Security Score : 4.8/11

Facility Security Percentage : 44.0/100.0  
=====

Total HR Security Score : 1.2/4

HR Security Percentage : 30.0/100.0  
=====

Total IS Security Score : 36.6/74

IS Security Percentage : 49.0/100.0  
=====

Total Legal Score : 2.4/4

Legal Percentage : 60.0/100.0  
=====

Total Operation Management Score : 4.8/9

Operation Management Percentage : 53.0/100.0  
=====

Total Risk Management Score : 7.2/15

Risk Management Percentage : 48.0/100.0  
=====



Total Release Management Score : 3.2/6

Release Management Percentage : 53.0/100.0

=====

Total Resiliency Score : 5.6/12

Resiliency Percentage : 47.0/100.0

=====

Total Security Architecture Score: 15.0/32

Security Architecture Percentage : 47.0/100.0

=====  
**Cloud Provider (14)**  
=====

Total Compliance Score : 7.2/16

Compliance Percentage : 45.0/100.0

=====  
Total Data Governance Score : 7.0/16

Data Governance Percentage : 44.0/100.0

=====  
Total Facility Security Score : 5.0/11

Facility Security Percentage : 45.0/100.0

=====  
Total HR Security Score : 1.8/4

HR Security Percentage : 45.0/100.0

=====  
Total IS Security Score : 37.4/74

IS Security Percentage : 51.0/100.0

=====  
Total Legal Score : 2.2/4

Legal Percentage : 55.0/100.0

=====  
Total Operation Management Score : 4.2/9

Operation Management Percentage : 47.0/100.0

=====  
Total Risk Management Score : 7.6/15

Risk Management Percentage : 51.0/100.0  
=====

Total Release Management Score : 3.4/6

Release Management Percentage : 57.0/100.0

=====

Total Resiliency Score : 6.2/12

Resiliency Percentage : 52.0/100.0

=====

Total Security Architecture Score: 14.6/32

Security Architecture Percentage : 46.0/100.0

=====

### Cloud Provider (2)

=====

Total Compliance Score : 7.2/16

Compliance Percentage : 45.0/100.0

=====

Total Data Governance Score : 7.6/16

Data Governance Percentage : 48.0/100.0

=====

Total Facility Security Score : 4.6/11

Facility Security Percentage : 42.0/100.0

=====

Total HR Security Score : 1.2/4

HR Security Percentage : 30.0/100.0

=====

Total IS Security Score : 40.2/74

IS Security Percentage : 54.0/100.0

=====

Total Legal Score : 2.0/4

Legal Percentage : 50.0/100.0

=====

Total Operation Management Score : 4.0/9

Operation Management Percentage : 44.0/100.0

=====

Total Risk Management Score : 8.4/15

Risk Management Percentage : 56.0/100.0

=====

Total Release Management Score : 2.6/6

Release Management Percentage : 43.0/100.0

=====

Total Resiliency Score : 6.4/12

Resiliency Percentage : 53.0/100.0

=====

Total Security Architecture Score: 15.4/32

Security Architecture Percentage : 48.0/100.0

=====

-----  
**[3] Security Compliance Assessment (SCA) Transparency Results**  
-----

**Cloud Provider (49)**

=====

Total Compliance Score : 3.8/16

Compliance Percentage : 24.0/100.0

=====

Total Data Governance Score : 4.8/16

Data Governance Percentage : 30.0/100.0

=====

Total Facility Security Score : 2.2/11

Facility Security Percentage : 20.0/100.0

=====

Total HR Security Score : 0.6/4

HR Security Percentage : 15.0/100.0

=====

Total IS Security Score : 21.2/74

IS Security Percentage : 29.0/100.0

=====

Total Legal Score : 1.2/4

Legal Percentage : 30.0/100.0

=====

Total Operation Management Score : 3.0/9

Operation Management Percentage : 33.0/100.0

=====

Total Risk Management Score : 4.6/15

Risk Management Percentage : 31.0/100.0

=====

Total Release Management Score : 0.8/6

Release Management Percentage : 13.0/100.0

=====

Total Resiliency Score : 4.4/12

Resiliency Percentage : 37.0/100.0

=====

Total Security Architecture Score: 10.4/32

Security Architecture Percentage : 33.0/100.0

=====

**Cloud Provider (91)**

=====

Total Compliance Score : 5.2/16

Compliance Percentage : 33.0/100.0

=====

Total Data Governance Score : 4.0/16

Data Governance Percentage : 25.0/100.0

=====

Total Facility Security Score : 2.8/11

Facility Security Percentage : 25.0/100.0

=====

Total HR Security Score : 1.2/4

HR Security Percentage : 30.0/100.0

=====

Total IS Security Score : 24.0/74

IS Security Percentage : 32.0/100.0

=====

Total Legal Score : 1.8/4

Legal Percentage : 45.0/100.0

=====

Total Operation Management Score : 3.8/9

Operation Management Percentage : 42.0/100.0

=====

Total Risk Management Score : 4.8/15

Risk Management Percentage : 32.0/100.0

=====

Total Release Management Score : 2.6/6

Release Management Percentage : 43.0/100.0

=====

Total Resiliency Score : 3.4/12

Resiliency Percentage : 28.0/100.0

=====

Total Security Architecture Score: 12.2/32

Security Architecture Percentage : 38.0/100.0

=====  
**Cloud Provider (14)**  
=====

Total Compliance Score : 4.8/16

Compliance Percentage : 30.0/100.0

=====  
Total Data Governance Score : 5.0/16

Data Governance Percentage : 31.0/100.0

=====  
Total Facility Security Score : 2.6/11

Facility Security Percentage : 24.0/100.0

=====  
Total HR Security Score : 1.2/4

HR Security Percentage : 30.0/100.0

=====  
Total IS Security Score : 22.4/74

IS Security Percentage : 30.0/100.0

=====  
Total Legal Score : 0.8/4

Legal Percentage : 20.0/100.0

=====  
Total Operation Management Score : 2.6/9

Operation Management Percentage : 29.0/100.0

=====  
Total Risk Management Score : 5.0/15

Risk Management Percentage : 33.0/100.0  
=====



Total Release Management Score : 1.6/6

Release Management Percentage : 27.0/100.0

=====

Total Resiliency Score : 3.2/12

Resiliency Percentage : 27.0/100.0

=====

Total Security Architecture Score: 7.8/32

Security Architecture Percentage : 24.0/100.0

=====

**Cloud Provider (2)**

=====

Total Compliance Score : 3.8/16

Compliance Percentage : 24.0/100.0

=====

Total Data Governance Score : 5.2/16

Data Governance Percentage : 33.0/100.0

=====

Total Facility Security Score : 1.0/11

Facility Security Percentage : 9.0/100.0

=====

Total HR Security Score : 1.6/4

HR Security Percentage : 40.0/100.0

=====

Total IS Security Score : 20.1/74

IS Security Percentage : 28.0/100.0

=====

Total Legal Score : 1.2/4

Legal Percentage : 30.0/100.0

=====

Total Operation Management Score : 2.8/9

Operation Management Percentage : 31.0/100.0

=====

Total Risk Management Score : 4.6/15

Risk Management Percentage : 31.0/100.0

=====

Total Release Management Score : 2.0/6

Release Management Percentage : 33.0/100.0

=====

Total Resiliency Score : 4.0/12

Resiliency Percentage : 33.0/100.0

=====

Total Security Architecture Score: 10.4/32

Security Architecture Percentage : 33.0/100.0

=====

-----

**[4] Cloud Security Alliance (CSA)**

-----

NA

## References

- [1]. P. Mell and T. Grance, *The NIST Definition of Cloud Computing*. Gaithersburg: National Institute of Standards and Technology, 2009.
- [2]. J. Geelan, 2009, "Twenty-One Experts Define Cloud Computing," [Online] Available: <http://cloudcomputing.sys-con.com/node/612375>. Accessed: 10 February 2014.
- [3]. Google Docs, Available: <http://docs.google.com>.
- [4]. Google App Engine, Available: <http://code.google.com/appengine/>.
- [5]. Amazon EC2, Available: <http://aws.amazon.com/ec2/>.
- [6]. P. Patel, A. Ranabahu and A. Sheth, "Service Level Agreement in Cloud Computing," in *Proc. Workshop Best Practices Cloud Computing: Implementation and Operational Implications for the Cloud* at ACM Int. Conf. Object-Oriented Programming, Systems, Languages, and Applications, Orlando, FL, Oct. 2009.
- [7]. W. Dawoud, I. Takouna and C. Meinel, "Infrastructure as a service security: Challenges and solutions," presented at INFOS2010 - 2010 7th Int. Conf. Informatics and Systems, 2010.
- [8]. M. Almorsy, J. Grundy and I. Mueller, I, "An analysis of the cloud computing security problem," in *Proc. 2010 Asia Pacific Cloud Workshop*, collocated with APSEC2010, Australia, 2010.
- [9]. D. Mohammed, "Security in cloud computing: An analysis of key drivers and constraints," *Information Security J.*, vol. 20, no. 3, pp. 123-127, 2011.
- [10]. S. Pearson, "Toward accountability in the cloud," *IEEE Internet Computing*, vol. 15, no. 4, pp. 64-69, 2011.
- [11]. K. M. Khan and Q. MALLUHI, "Establishing trust in cloud computing," *IT Professional*, vol. 12, no. 5, pp. 20-27, 2010.
- [12]. R. M. Savola, A. Juhola and I. Uusitalo, "Towards wider cloud service applicability by security, privacy and trust measurements," in *4th Int. Conf. Application of Information and Communication Technologies*, AICT2010, 2010.
- [13]. Sun Microsystems, Inc., "Building customer trust in cloud computing with transparent security". White Paper. Santa Clara: Sun Microsystems, 2009.

- [14]. M. Ouedraogo and H. Mouratidis, "Selecting a cloud service provider in the age of cybercrime," *Computers and Security*, vol. 38, pp.3-13, 2013.
- [15]. T. Lambo, "Why you need a cloud rating system" [Online] <https://www.cloudeassurance.com/why-you-need-a-cloud-rating-score> Accessed: December 31, 2013.
- [16]. A. Amato and S. Venticinque, "Multi-objective decision support for brokering of cloud SLA," in *Proc. - 27th Int. Conf. Advanced Information Networking and Applications Workshops, WAINA 2013*, p.1241, 2013.
- [17]. P. Bedi, H. Kaur and B. Gupta, "Trustworthy service provider selection in cloud computing environment," in *Proc. -Int. Conf. Communication Systems and Network Technologies, CSNT 2012*, p.714, 2012.
- [18]. S. Gagnono, V. Nabelsi, K. Passerini and K. Calisi, "The next web apps architecture: Challenges for SaaS vendors," *IT Professional*, vol. 13, no. 5, pp.44-50, 2011.
- [19]. Cloud Security Alliance, "About the CSA Security, trust & assurance registry (STAR)," [Online] Cloud Security Alliance <https://cloudsecurityalliance.org/star> Accessed: December 15, 2013.
- [20]. M. Ouedraogo and H. Mouratidis, "Selecting a cloud service provider in the age of cybercrime". *Computers and Security*, vol. 38, pp.3-13, 2013.
- [21]. R. Knode and D. Egan, *Digital Trust in the Cloud: Into the Cloud with CTP: A précis for the CloudTrust Protocol*. Fulls Church: Computer Sciences Corporation, 2010.
- [22]. W. Pauley, "Cloud provider transparency: an empirical evaluation," *IEEE Security and Privacy*, vol. 8, no. 6, pp.32-39, 2010.
- [23]. A. Sumetanupap and T. Senivongse, "Enhancing service selection with a provider trustworthiness model," in *Proc. 8th Int. Joint Conf. Computer Science and Software Engineering (JCSSE 2011)*, IEEE CS Press, May 2011, pp.281-286.
- [24]. S.K. Garg, S. Versteeg, and R. Buyya, *A Framework for Ranking of Cloud Computing Services*. Future Generation Computer Systems, 2012.
- [25]. S.K. Garg, S. Versteed and R. Buyya, "SMICloud: A framework for comparing and ranking cloud services," in *Proc. - 2011 4th IEEE Int. Conf. Utility and Cloud Computing, UCC 2011*, pp.210-218.
- [26]. A. Li, X. Yang, S. Kandula and M. Zhang, "Comparing public-cloud providers," *IEEE Internet Computing*, vol. 15, no. 2, pp.50-53, 2011.

- [27]. D. Catteddu and G. Hogben, "Cloud computing benefits, risks and recommendations for information security,"[Online].European Network and Information Security Agency (ENISA), Available: [www.enisa.europa.eu/](http://www.enisa.europa.eu/);2009 Accessed: August 10, 2014
- [28]. Cloud Security Alliance. [Online].Available: CSA <https://cloudsecurityalliance.org/>. Accessed: August 10, 2014.
- [29]. SurveyMonkey. [Online]. Available: <https://www.surveymonkey.com/>. Accessed: October 01, 2012.
- [30]. Cloud Security Alliance. Cloud Controls Matrix (CCM). [Online]. Available: <https://cloudsecurityalliance.org/research/ccm>. Accessed on: December 15, 2013.
- [31]. Cloud Security Alliance. Consensus Assessment Initiative. Available: <https://cloudsecurityalliance.org/research/cai>. Accessed: December 15, 2013.
- [32]. S. M. Habib, V. Varadharajan and M. Muhlhauser, "A trust-aware framework for evaluating security controls of service providers in cloud marketplaces," in *12th IEEE Int. Conf. Trust, Security and Privacy Computing and Communications (TrustCom)*, vol., no., pp.459-468, 16-18 July, 2013
- [33]. N. Bhensook and T. Senivongse, "An assessment of security requirements compliance of cloud providers," in *CloudCom – Proc.: 2012 4th IEEE Int. Conf. Cloud Computing Technology and Science*, 520-525.
- [34]. IEEE. [Online]. Available: <http://www.ieee.org/index.html>.Accessed: August 10, 2014.
- [35]. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Network and Computer Applications*, vol. 34, issue 1, pp. 1-11, Jan. 2011.
- [36]. M. Dekker, D. Liveri and M. Lakka, *Cloud security incident reporting: Framework for reporting about major cloud security incidents*. ENISA. [Online]. Available: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/incident-reporting-for-cloud-computing>. Accessed: December 15, 2013.
- [37]. CloudAudit. CloudAudit: Automated Audit, Assertion, Assessment, and Assurance. [Online]. Available: [www.cloudaudit.org](http://www.cloudaudit.org). Accessed on: June 15, 2011.
- [38]. OCCI. Open Cloud Computing Interface. [Online]. Available:[www.occ-wg.org](http://www.occ-wg.org) Accessed: December 15, 2013.
- [39]. Gartner, Available: <http://www.gartner.com/technology/home.jsp>

- [40]. IDC, Available: <http://www.idc.com/>
- [41]. L. Columbus, "Cloud Computing and Enterprise Software Forecast Update," [Online]. Available: <http://www.forbes.com/sites/louiscolumbus/2012/11/08/cloud-computing-and-enterprise-software-forecast-update-2012/>. Accessed: December 10, 2013.
- [42]. IDC. The Cloud Movement [Online]. Available: [http://www.idc.com/prod\\_serv/FourPillars/Cloud/index.jsp](http://www.idc.com/prod_serv/FourPillars/Cloud/index.jsp). Accessed: December 10, 2013.
- [43]. Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.*, 2009. [Online]. Available: <https://cloudsecurityalliance.org/wp-content/uploads/2011/07/csaguide.v2.1.pdf>. Accessed: June 10, 2012.
- [44]. J. Brodtkin, "Gartner: Seven cloud computing security risks," 2008. [Online]. Available: <http://www.infoworld.com/article/2652198/security/gartner--seven-cloud-computing-security-risks.html>. Accessed: April 10, 2011.
- [45]. Mimecast, "Cloud computing vendor selection: Evaluating business practices, data protection, and regulatory compliance," 2013. [Online]. Available: <http://www.mimecast.co.uk/resources/whitepapers/dates/2012/6/cloud-computing-vendor-selection/>. Accessed: December 15, 2013.
- [46]. F. Shimba, "Cloud Computing: Strategies for Cloud Computing Adoption," MSc Thesis. Dublin Inst. Technol., 2010.
- [47]. S. M. Habib, S. Ries, S. and M. Mühlhäuser "Cloud computing landscape and research challenges regarding trust and reputation," Paper presented at the *Proc. - Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing in Conjunction with the UIC 2010 and ATC 2010 Conferences, UIC-ATC 2010*, 410-415.
- [48]. D. Catteddu and G. Hogben, "Cloud computing information assurance framework," European Network and Information Security Agency (ENISA), [www.enisa.europa.eu/](http://www.enisa.europa.eu/). 2010
- [49]. ISO. International Standards Organisation. [Online]. Available: <http://www.iso.org/>. Accessed: December 15, 2013.
- [50]. National Institute of Standards and Technology (NIST). [Online]. Available: <http://www.nist.gov/>. Accessed: December 31, 2013.

- [51]. Cloud Security Alliance. CSA STAR Terms and Conditions. [Online]. Available: <https://cloudsecurityalliance.org/star/terms/>. Accessed: December 15, 2013.
- [52]. Cloud Security Alliance. Open Certification Framework: Cloud Security Alliance. [Online]. Available: <https://cloudsecurityalliance.org/research/ocf/>. Accessed: December 15, 2013.
- [53]. PCI Security Standards Council. [Online]. Available: <https://www.pcisecuritystandards.org/>. Accessed: December 15, 2013.
- [54]. FedRamp. [Online]. Available: [http://www.gsa.gov/HP\\_13\\_SpecialTopics\\_fedramp](http://www.gsa.gov/HP_13_SpecialTopics_fedramp). Accessed: December 15, 2013.
- [55]. HIPAA. U.S. Department of Health & Human Services, Office of Civil Rights, HIPAA. [Online]. Available: <http://www.hhs.gov/ocr/hipaa/privacy.html>. Accessed: December 15, 2013.
- [56]. H. Koziolok, "Goal Question Metric" in *Dependability Metrics*, vol, pp.39-42, 2008
- [57]. MKS. *Bring Goal Question Metric (GQM) To Life with MKS Portfolios*. White Paper. [Online] Available: Accessed: December 15, 2013
- [58]. V.R. Basili, G. Caldiera and D.H. Rombach,. "The Goal Question Metric Approach," in *Encyclopaedia of Software Engineering*, Wiley, 1994.
- [59]. S. Ristov, M. Gusev and M. Kostoska, "A new methodology for security evaluation in cloud computing," in *MIPRO, 2012 Proc. 35th Int. Conv.*, IEEE Conference Publications, pp. 1808-1813.
- [60]. A. Omerovic, V. Munte-Mulero, P. Matthews and A. Gunka, "Towards a method for decision support in multi cloud environments," in 4th CLOUD COMPUTING, 2013, pp. 162–180
- [61]. A. B. Ryan, "Methodology: Collecting Data," in *Researching and Writing your Thesis: a guide for postgraduate students*, M. Antonesa et al, Eds. , MACE: Maynooth, 2006.
- [62]. I. Brace, *Questionnaire Design, How to Plan, Structure, and Write Survey Material for Effective Market Research*. Kogan Page, London, 2004.
- [63]. SurveyMonkey. Survey Introduction. [Online]. Available: [http://help.surveymonkey.com/articles/en\\_US/kb/Tip-Creating-an-effective-survey-introduction](http://help.surveymonkey.com/articles/en_US/kb/Tip-Creating-an-effective-survey-introduction). Accessed: April 10, 2014.
- [64]. LinkedIn, Available: <https://www.linkedin.com/home>.

- [65]. J. Luna, H. Ghani, D. Germanus and N. Suri, "A security metrics framework for the Cloud," *2011 Proc. Int. Conf. Security and Cryptography (SECRYPT)*, vol., no., pp.245-250, 18-21 July 2011
- [66]. M. Kassou and L. Kjiri, "A goal question metric approach for evaluating security in a service oriented architecture context," *Int. J. Comput. Sci. Issues*, vol. 9, issue 4, no. 1, pp. 238 -249, July 2012.
- [67]. J. Luna, H. Ghani, T. Vateva and N. Suri., "Quantitative assessment of cloud security level agreements: A case study," in *SECRYPT 2012 – Proc. Int. Conf. Security and Cryptography 2012*, pp. 64-73.
- [68]. R. M. Svola and H. Abie, "Development of security metrics for a distributed messaging system," 2009 Int. Conf. Appl. of Inform. Commun. Technol., AICT 2009.
- [69]. SANS Institute, *A Guide to Security Metrics*, 2006. [Online]. Available: <http://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55>. Accessed: April 10, 2014.
- [70]. CAMM, Common Assurance Maturity Model, 2010. [Online]. Available: <http://common-assurance.com/>. Accessed: April 10, 2014
- [71]. G. Hogben, "ENISA Cloud Computing Strategy," 2011. [Online]. Available: <http://www.terena.org/activities/tfcsirt/meeting30>. Accessed: April 10, 2014
- [72]. E. Chew *et al.*, "Performance measurement guide for information security," Tech. Report, Nat. Inst. Standards Techn., July 2008.
- [73]. J. Wang, "Information Security Models and Metrics," in *ACM Southeast Regional Conf.*, 2005, M. Guimarães, Ed., vol. 2, pp.178–184.
- [74]. National Institute of Standards and Technology (NIST), "NIST Cloud Computing Reference Architecture Cloud Service Metrics Description," NIST Draft Publication, April 3, 2013. [Online]. Available: [http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/RATax\\_CloudMetrics\\_Meeting\\_04112013](http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/RATax_CloudMetrics_Meeting_04112013) Accessed: April 10 2014
- [75]. P. Berander and P Jönsson, "A goal question metric based approach for efficient measurement framework definition," in *ISESE'06 –Proc. 5th ACM-IEEE Int. Symp. Empirical Software Eng., 2006*, pp. 316-325.
- [76]. N. R. Putri and M. C. Mganga, "Enhancing information security in cloud computing services using SLA based metrics," M.S. thesis, Blekinge Instit. Tech. [Online]. Available from: [http://www.bth.se/fou/cuppsats.nsf/all/780daa1ef3027f82c1257864001c2d87/\\$file/MCS-2011-03.pdf](http://www.bth.se/fou/cuppsats.nsf/all/780daa1ef3027f82c1257864001c2d87/$file/MCS-2011-03.pdf). Accessed: April, 10 2014.



- [77]. F. Moyano, K. Beckers and C. Fernandez-Gago, Trust-aware decision-making methodology for cloud sourcing, 2014.
- [78]. S. M. Habib, S. Hauke, S. Ries and M. Mühlhäuser, “Trust as a facilitator in cloud computing: a survey,” *J. Cloud Computing*, vol. 1, no. 1, 2012, pp. 1-18.
- [79]. A. Cardoso and S. Paulo, “Cloud computing: Concepts, technologies and challenges,” *Virtual and Networked Organisations, Emergent Technologies and Tools*. Springer Berlin Heidelberg, 2012. 127-136
- [80]. N. Leavitt, “Is cloud computing really ready for prime time?,” *Computer*, vol. 42, pp. 15-20, 2009.
- [81]. D. Catteddu and G. Hogben, *An SME perspective on Cloud Computing: Survey*. [Online] ENISA. Available: [https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-sme-survey/at\\_download/fullReport](https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-sme-survey/at_download/fullReport) Accessed: April, 10 2014.
- [82]. Mimecast, “Cloud computing adoption survey,” 2010. [Online]. Available: [https://system.netsuite.com/core/media/media.nl?id=181214&c=601905&h=2ef3796f7c4d9c8a585e&\\_xt=.pdf](https://system.netsuite.com/core/media/media.nl?id=181214&c=601905&h=2ef3796f7c4d9c8a585e&_xt=.pdf). Accessed: April 10, 2014.
- [83]. G. Feuerlicht, L. Burkon and M. Sebesta, “Cloud computing adoption: What are the issues?” *Systemova Integrace*, 2011, pp.187-192.
- [84]. C. Hinde and J. P. Van Belle, “Cloud computing in South African SMMEs: Risks and rewards for playing at altitude,” *Int. J. Comp. Sci. Elect. Eng*, vol. 1, no.1, 2012, pp. 1-10.
- [85]. G. Feuerlicht and N. Margaris, “Cloud Computing Adoption: A comparative study,” in *Proc. 1<sup>st</sup> WSEAS Int. Conf. Cloud Computing (CLC '12)*, Vienna, Austria, November 10-12, 2012, Available: <http://www.wseas.us/e-library/conferences/2012/Vienna/COMPUTERS/COMPUTERS-71.pdf>
- [86]. R. Cohen, “Is the middle east the next big market for cloud computing?,” 2013. [Online]. Available: <http://www.forbes.com/sites/reuvencohen/2013/03/12/is-the-middle-east-the-next-big-market-for-cloud-computing/> Accessed: April 15, 2014.
- [87]. S. T. Alharbi, “Users' acceptance of cloud computing in Saudi Arabia: An extension of technology acceptance model,” *Int. J. Cloud Appl. and Comput.*, vol. 2, no. 2, pp. 1-11, April-June 2012. Available from: <http://www.igi-global.com/gateway/article/full-text-pdf/67543>
- [88]. SurveyMonkey, “Understand your audiences with demographic surveys”. [Online]. Available: <https://www.surveymonkey.com/mp/demographic-survey/>. Accessed: April 15, 2014.
- [89]. T. F. Burgess, *Guide to the Design of Questionnaires. A General Introduction to the Design of Questionnaires for Survey Research*, 2001

- [90]. Bitcurrent, “Bitcurrent cloud computing survey 2011: Cloud adoption, concerns, and motivation” .[Online]. Available: <http://www.bitcurrent.com/download/cloud-computing-survey-2011>. Accessed: April 15, 2014.
- [91]. M. Bamiah, S. Brohi, S. Chuprat and J. Ab Manan, “A study on significance of adopting cloud computing paradigm in healthcare sector,” in *Proc. 2012 Int. Conf. Cloud Comput. Technol., Appl. Manage., ICCCTAM*, 2012, pp. 65-68.
- [92]. M. Armbrust *et al.*, “Above the clouds: A berkeley view of cloud computing,” Technical Report No. UCB/Eecs-2009-28, University of California at Berkley, USA, Feb. 10, 2009.
- [93]. J. Chen and H. Song, “Industrial clusters’ information based on SaaS model,” *Intl Conf. Bus. Manage. Electron. Inform. (BMEI)*, 13-15 May, 2011
- [94]. Q. Zhang, L. Cheng and R. Boutaba, “Cloud computing: state-of-the-art and research challenges,” *J. Internet Services Appl.*, vol. 1, no. 1, 2010.
- [95]. D. Sullivan, “Reducing risks with multiple cloud service providers,” 2012. [Online]. Available:<http://searchcloudcomputing.techtarget.com/tip/Reducing-risks-with-multiple-cloud-service-providers>. Accessed: June 7, 2014.
- [96]. R. Sahandi, A. Alkhalil and J. and Opara-Martins, “Cloud computing from SMEs perspective: a survey based investigation,” *J. of Inform. Technol. Manage.*, vol. 24, no. 1, 2, 2013.
- [97]. KPMG, “Breaking through the cloud adoption barriers,”(2012)[Online]. Available: <https://www.kpmg.com/SG/en/IssuesAndInsights/ArticlesPublications/Documents/Advisory-ICE-Breaking-through-the-Cloud-Adoption-Barriers-Glob.pdf>. Accessed: December 14, 2014.
- [98]. Rackspace, “Cloud Survey Infographic,” 2013. [Online]. Available: <http://www.rackspace.co.uk/innovation/cloud-resources/cloud-benefits>. Accessed: December14, 2014.
- [99]. G-Cloud Framework. [Online]. Available: <https://www.gov.uk/how-to-use-cloudstore>. Accessed: May 10, 2014.
- [100]. KPMG, “From hype to future KPMG’s 2010 cloud computing survey,”2010. [Online]. Available: <https://www.kpmg.com/ES/es/ActualidadNovedades/ArticulosyPublicaciones/Documents/2010-Cloud-Computing-Survey.pdf>. Accessed: April 15, 2014.

- [101]. N. Ghosh, S. Ghosh and S. Das, “Selcsp A framework to facilitate selection of cloud service providers,” *IEEE Transactions on Cloud Computing*, 2014
- [102]. CloudSigma. Available: <https://www.cloudsigma.com>
- [103]. Terramark. Available: <http://www.terramark.co.uk>.
- [104]. Windows Azure. Available: <http://azure.microsoft.com/en-gb/>.
- [105]. J. Banks, “Introduction to simulation,” in *Proc. 1998 Winter Simulation Conf.*, P.A. Farrington *et al.*, Eds, 1999, pp. 7-13.
- [106]. M. Alhamad, T. Dillon and E. Chang, “A trust-evaluation metric for cloud applications”, *Int. J. Mach. Learning Comput.*, Vol. 1, No.4, October 2011, pp. 416-421.
- [107]. Wikipedia, *Longitudinal Study*. [Online]. Available: [http://en.wikipedia.org/wiki/Longitudinal\\_study](http://en.wikipedia.org/wiki/Longitudinal_study). Accessed: November 10, 2014.
- [108]. N. M. Goldberg and M. Wildon-Byrne, “Securing Communications on the Cloud,” *Bloomberg Law Reports – Technology Law*, vol. 1, no. 10, 2009. [Online]. Available: <http://www.infolawgroup.com/uploads/file/Goldberg%20Article.pdf>. Accessed: December 18, 2014.
- [109]. C. S. M. I. C. (CSMIC) *SMI Framework*. [Online]. Available: <http://www.cloudcommons.com/ar/about-smi>. Accessed: April 10, 2014.
- [110]. O.S. Vaidya and S. Kumar, “Analytic hierarchy process: An overview of applications,” *Eur. J. Oper. Res.*, vol. 169, no. 1, pp. 1-29, 2006.
- [111]. Amazon AWS. Available: <http://aws.amazon.com/>.
- [112]. CloudHarmony. Available: <https://cloudharmony.com/>.
- [113]. A. Jøsang, R. Ismail and C. Boyd, “A survey of trust and reputation systems for online service provision,” *Decision Support Systems*, vol. 43, no. 2, pp. 618-644, 2007.
- [114]. Oxford Dictionaries. [Online]. Available: <http://www.oxforddictionaries.com/definition/english/reputation>. Accessed: May 10, 2014.
- [115]. Cloud Security Alliance, STAR Registry Entries. [Online] Available: [https://cloudsecurityalliance.org/star/?r=8489#\\_registry](https://cloudsecurityalliance.org/star/?r=8489#_registry) Accessed: December 29, 2014.
- [116]. COBIT. [Online]. Available: <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx> Accessed: December 30, 2014

- [117]. ISO27001. [Online]. Available: <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm> Accessed: December 30, 2014.
- [118]. SP800-53. [Online]. Available: [http://www.nist.org/nist\\_plugins/content/content.php?content.18](http://www.nist.org/nist_plugins/content/content.php?content.18) Accessed: December 30, 2014.
- [119]. BITS. [Online]. Available: <https://sharedassessments.org/> Accessed: December 30, 2014.
- [120]. GAPP. [Online]. Available: <http://www.iwg-swf.org/pubs/gapplist.htm> Accessed: December 30, 2014.
- [121]. P.A. Pavlou., “Trustworthiness as a source of competitive advantage in online auction markets”. Academy of Management Proceedings, A1–A7, 2002.
- [122]. Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts. [Online]. Available: [http://www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE\\_NT\(2013\)507476\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE_NT(2013)507476_EN.pdf) Accessed: September 25, 2015.
- [123]. Privacy and Your Business. [Online]. Available: [https://www.priv.gc.ca/resource/pb-avp/pb\\_hb\\_e.pdf](https://www.priv.gc.ca/resource/pb-avp/pb_hb_e.pdf) Accessed: September 25, 2015.
- [124]. NICCS, Explore Terms: A Glossary of Common Cybersecurity Terminology. [Online]. Available: <https://niccs.us-cert.gov/glossary> Accessed: September 25, 2015.
- [125]. Cloud Outage. [Online]. Available: <http://searchcloudstorage.techtarget.com/definition/cloud-outage> Accessed: September 25, 2015.
- [126]. Outage. [Online]. Available: <https://en.wikipedia.org/wiki/Outage> Accessed: September 25, 2015.
- [127]. A. Josang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision. Decis. Support Syst., 2006.
- [128]. J. Abawajy, "Determining Service Trustworthiness in Intercloud Computing Environments," in *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on* , vol., no., pp.784-788, 14-16 Dec. 2009
- [129]. S.M., Habib, S., Ries,; and M., Muhlhauser, "Towards a Trust Management System for Cloud Computing," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on* , vol., no., pp.933-939, 16-18 Nov. 2011
- [130]. L. Conner and L. DuBois, “Key Criteria in Selecting a Cloud Backup Provider That’s Built to Last” 2013. [Online]. Available: <https://community.emc.com/docs/DOC-24841> Accessed: August 15, 2015.

- [131]. Cloud Security Alliance Membership. [Online]. Available: <https://cloudsecurityalliance.org/membership/corporate/> Accessed: August 15, 2015.
- [132]. W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST: National Institute of Standards and Technology, Technical Report 800-144, 2011.
- [133]. Commercial off-the-shelve. [Online]. Available: [https://en.wikipedia.org/wiki/Commercial\\_off-the-shelf](https://en.wikipedia.org/wiki/Commercial_off-the-shelf) Accessed: September 25, 2015.
- [134]. Lie Qu; Yan Wang; Orgun, M.A., "Cloud Service Selection Based on the Aggregation of User Feedback and Quantitative Performance Assessment," in *Services Computing (SCC), 2013 IEEE International Conference on* , vol., no., pp.152-159, June 28 2013-July 3 2013