Development and Evaluation of a Holistic Framework and Maturity Assessment Tools for Data Governance in Cloud Computing Environments

Majid Saliman Al-Ruithe

Staffordshire University

A Doctoral Thesis submitted in partial fulfilment of the requirements of Staffordshire University for the degree of Doctor of Philosophy

January 2018

Abstract

Cloud computing is an emerging technology that is changing the way that public sector organisations consume Information and Communication Technology (ICT) in different countries. The adoption rate of cloud computing services is still very low to none in many countries. Saudi Arabia, for instance, despite their huge investments in the Digital Transformation, as part of the recent Vision 2030, the loss of governance and control of data is one of their major barriers facing the adoption of cloud computing services. Cloud Data Governance, is not only a Saudi concern, it is actually a worldwide challenge, which is under researched and mostly not practiced. This research attempted, for the first time to unlock this challenge in Saudi Arabia, more specifically, for the Public Sector, by advancing research in this field and proposing means by which Cloud Data Governance programmes can be implemented. In this research, existing data governance frameworks were analysed – these frameworks were limited as they lacked consideration of the cloud computing perspective. Hence, the purpose of this research is to develop a generalised Strategy Framework that can be utilised to design, deploy and sustain an effective cloud data governance programme; it also aims to provide knowledge for organisations that wish to apply a cloud data governance programme, to empower them to control their data in cloud environments. Understanding data governance taxonomy and its key dimensions for non-cloud and cloud computing was an important step in developing the proposed Framework. To support the development of the proposed Framework, the Analytic Theory and concept of Critical Success Factors (CSFs) were adopted. The Framework includes a number of complex operations, therefore, to ensure an effective Cloud Data Governance programme, organisations need to have means by which they can assess their current state and define their requirements. To facilitate this, a Maturity Model was proposed together with an Assessment Matrix. The proposed Framework and Maturity Model alongside the Assessment Matrix, were then validated and evaluated for the Public Sector in Saudi Arabia, as a Case Study. Mixed research methods, Qualitative and Quantitative, were adopted for this purpose, where the State of the Art of cloud adoption, data governance and cloud data governance, in the Saudi Public Sector were all analysed. Moreover, a number of Barriers and Critical Success Factors were identified for the case study. For validation purposes, the Focus Group approach was adopted, with appropriate representations from the Saudi Public Sector. The Structural Equation Modelling was adopted for the evaluation of the proposed Framework, using quantitative results from the questionnaire. The Evaluation of the Assessment Matrix was done by developing a Tool, which allows organisations to identify their levels of maturity for cloud data governance programmes, and define requirements for target levels

Keywords: Data governance, Cloud computing, Cloud data governance, Cloud data governance framework, Cloud Data Governance Maturity Model, Structural Equation Modelling

Acknowledgements

Firstly, I am grateful to Almighty Allah for the good health that was necessary to complete this thesis.

I would like to express my sincere gratitude to my parents, my mother Hameda and my father Saliman, for their support, which enabled me to reach this stage. After sincerely thanking my parents, my greatest indebtedness goes to my wife Samirah and my lovely daughters and sons, Lana, Tala, Abdulaziz and Mohammed for their support, patience, prayers and encouragement, which were positive influences on me to complete this thesis. Also, I owe special thanks to my brothers and sisters in Saudi Arabia for their moral support, endless patience and continuous prayers.

I would like to extend my thanks and appreciation to my advisors Prof. Elhadj Benkhelifa and Khawar Hameed for their continuous support of my PhD study and related research, and for their motivation, immense knowledge, and patience. Their guidance helped me throughout my studies and with the completion of my thesis. I would also like to express my thanks to all the specialists in the public sector organisations and cloud providers in Saudi Arabia for their participation in the survey; they supported my work in this way and helped me to achieve results of better quality. I am also grateful to all my friends and colleagues who provided me with support and guidance.

Finally, I am grateful to the Saudi Arabia government for giving me the opportunity to expand my expertise and knowledge in academic research, and their financial support throughout this PhD journey at Staffordshire University.

Dedication

I would like to dedicate the completion of my PhD thesis to:

My parents

My wife and children

My brothers and sisters

My friends and colleagues

List of Publications

Poster:

1. A Framework for designing, deploying, and sustaining an effective data governance programme for the cloud services. Accepted at 4th postgraduate research student conference, hosted by Staffordshire University, 16th May 2016. The poster was awarded with the merit of "*Highly Commended Submission*" in the conference.

Conferences:

1. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2016). A Conceptual Framework for Designing Data Governance for Cloud Computing. Procedia Computer Science, 94, 160-167.

2. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2016). Key Dimensions for Cloud Data Governance. In Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on (pp. 379-386). IEEE.

3. Al-Ruithe, M., Benkhelifa, E., & Mthunzi, S. (2016). Data Governance for Security in IoT & Cloud Converged Environments.13th ACS/IEEE International Conference on Computer Systems and Applications AICCSA 2016.

4. Al-Ruithe, M., & Benkhelifa, E. (2017). Cloud Data Governance Maturity Model. In Proceedings of the second international conference on Internet of Things, Data and Cloud Computing (ICC 2017). ACM.

5. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2017). Current State of Cloud Computing Adoption–An Empirical Study in Major Public Sector Organizations of Saudi Arabia (KSA). Procedia Computer Science, 110, 378-385.

6. Al-Ruithe, M., & Benkhelifa, E. (2017). Analysis and Classification of Barriers and Critical Success Factors for Implementing a Cloud Data Governance Strategy. Procedia Computer Science, 113, 223-232.

7. Al-Ruithe, M., and Benkhelifa, (2017). Cloud Data Governance In-Light of the Saudi Vision 2030 for Digital Transformation. 4th ACS/IEEE International Conference on Computer Systems and Applications AICCSA 2017. IEEE.

8. Al-Ruithe, M., & Benkhelifa, E. (2017). A Conceptual Framework for Cloud Data Governance-Driven Decision Making. 1$^{\mathbf{st}}$ International Conference on the Frontiers and Advances in Data Science. IEEE.

9. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018). Key Issues for Embracing the Cloud Computing to Adopt a Digital Transformation: A study of Saudi Public Sector. Procedia Computer Science, - (in press).

Journals:

1. Al-Ruithe, M., Benkhelifa, E., Jararweh, Y., & Ghedira, C. (2017). Addressing Data Governance in Cloud Storage: Survey, Techniques and Trends. Journal of Internet Technology, - (in press).

2. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018). A Systematic Literature Review of Data Governance and Cloud Data Governance. Personal and Ubiquitous Computing, DOI: 10.1007/s00779-017-1104-3.

3. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018). Data Governance Taxonomy: Cloud versus Non-Cloud. Sustainability. [Online]. 10 (1). p.p. 95. Available from: http://www.mdpi.com/2071-1050/10/1/95.

4. Al-Ruithe, M., & Benkhelifa, E. (2018). Determining the Enabling Factors for Implementing Cloud Data Governance in the Saudi Public Sector by Structural Equation Modelling. Future Generation Computer Systems. DOI10.1016/j.future.2017.12.057

5. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018). A Strategy Framework Development for Cloud Data Governance Programme. Cluster Computing Journal. (Submitted).

Awards

Highly commended submission poster award at 4th postgraduate research student conference, hosted by Staffordshire University, 16th May 2016. The poster title: "*A framework for designing, deploying, and sustaining an effective data governance programme for the cloud services*". (See Appendix F).

Table of Contents

List of Figures

List of Tables

List of Abbreviations

CG	Corporate Governance
ITG	Information Technology Governance
IG	Information Governance
CCG	Cloud Computing Governance
NIST	National Institute of Standards and Technology
SLR	Systematic Literature Review
CSFs	Critical Success Factors
SEM	Structural Equation Modelling
SLA	Service Level Agreement
KPIs	Key Performance Indicators
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CobiT	Control Objectives for Information and Related Technologies
SOA	Service-Oriented Architecture
SSE-CMM	Systems Security Engineering Capability Maturity Model
OPM3	Organizational Project Management Maturity Model
NIMM	NHS Infrastructure Maturity Model
R-CMM	Requirements Capability Maturity Model
CFA	Confirmatory Factor Analysis
EFA	Exploratory Factor Analysis
PA	Path Analysis
Ha	Associative hypotheses
Hb	Causal hypotheses
CDGO	Cloud Data Governance Office
PR	Preparation Requirements
CDF	Cloud Data Governance Functions
CA	Contextual Alignment
CI	Contextual Integration
SR	Sustain Requirements
MR	Monitor Requirements
CC	Contractual Context
DPC	Deploy Context
CR	Composite Reliability
AVE	Average Variance Extracted
KMO	Kaiser-Meyer-Olkin
X2	Chi-Square
df	Digress of Freedom
GFI	Goodness-of-fit index
AGFI	The adjusted goodness-of-fit index
IFI	Incremental-fit index
TLI	Tucker-Lewis index
CFI	Comparative Fit Index
RMSEA	The Root Mean Square Error of Approximation
MARS-CDG	The Maturity Assessment & Recommendation System of Cloud Data Governance

Chapter 1. Introduction to This Study

1.1. Introduction

Data governance is an emerging research area and it has attracted significant attention in the information systems (IS) field (De Hert & Papakonstantinou, 2013). However, the interest shown in data governance by industry researchers has not been matched by that of academia; in addition, the research on data governance in general and on its implementation in the cloud in particular is still in its early stages and more research efforts are required (Wende, 2007; Begg & Caira, 2012). Data governance is a big challenge for chief information officers (CIOs), and businesses are becoming increasingly interested in this domain, due to the benefits it brings regarding the governance of the use of data inside and outside an organisation (Fu et al., 2011). Data governance started to attract more attention only in the early 2000s; the US federal government established rules to improve the accuracy and reliability of corporate information, because of the collapse of companies like Adelphia, Enron and others (Hilton, 2006). Therefore, good data governance practices are clearly essential for organisations to ensure that all this data is well understood, trusted, accessible, accurate and secure. Data governance and data business planning are important strategies that state-of-the-art government agencies can use to maximise the effectiveness of data-driven decision making for key organisational objectives.

This chapter aims to highlight the purpose of this study. The chapter starts with the definition of data governance. Understanding data governance and cloud computing technology also introduced in this chapter. The overview and background of Kingdom of Saudi Arabia (KSA) is presented, followed by the research problem statement and motivation. In addition, the research aim and objectives of this study are presented in this chapter. The research question and methodologies also discusses in the current chapter. Research contributions to knowledge and ethical considerations of the research are highlighted in this chapter. Finally, this chapter conclude by providing the structure of the thesis.

1.2. Definition of Data Governance

In the literature there is no commonly accepted definition of data governance among researchers, and corresponding research is still in the early stages. There are numerous definitions of data governance in the literature, each of which tends to reflect the particular researcher's specialisations and interests. Therefore, there is no one official definition of this term. In order to determine what data governance is, this study referred to some different definitions offered in the literature. These definitions are highlighted in Table 1.1.

Table 1.1 Popular data governance definitions

Definition	Reference
"*Data governance specifies the framework for decision rights and accountabilities to encourage desirable behaviour in the use of data. To promote desirable behaviour, data governance develops and implements corporate-wide data policies, guidelines and standards that are consistent with the organisation's mission, strategy, values, norms and culture*".	Weber et al. (2009)
"*Data governance is the formal execution and enforcement of authority over the management of data and data-related assets*".	Seiner (2014)
"*Data governance refers to the overall management of the availability, usability, integrity and security of the data employed in an enterprise. A sound data governance program includes a governing body or council, a defined set of procedures and a plan to execute those procedures*".	whatis.com
"*Data governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods*".	The Data Governance Institute (2015)
"*Total of data-related processes and decisions that encourage desirable behaviour for an organisation in the use and production of data*".	Choi and Kröschel (2013)

However, these definitions emphasise the significance of the terms through which data governance activities can be executed on data-related assets that support the organisation's strategy. Most authors agree that the term 'data governance' refers to the entirety of decision rights and responsibilities concerning the management of data assets in organisations. These definitions do not give equal prominence to data governance within the context of cloud computing. Therefore, the definition of data governance which was reported by (Weber et al., 2009) in the table above will be using in this study by integrating this definition within the cloud computing context to achieve the aim of this study. Thus, this requires an in-depth understanding of data governance and cloud computing.

1.3. Understanding Data Governance

Governance in general refers to "*the way the organisation goes about ensuring that strategies are set, monitored, and achieved*"(Rau, 2004, p.35). This concept has been enhanced to give rise to many terms, such as corporate governance, information governance, Information Technology (IT) governance and data governance. Thus, it is important to discuss the relation between data governance and other domains of governance. Data governance is high-level planning and control over data management (Alhassan et al., 2016). The roots of data governance research can be traced back to the early 1980s; it has now become a hot topic for industry and academic research (De Hert & Papakonstantinou, 2013). The first efforts to create a framework for data governance were published in 2007. Both academic and practical sources assume that one size does not fit all; thus, each organisation should develop a specific programme for its data governance (Weber et al., 2009). It is important to confirm that data governance and IT governance have to follow corporate governance principles (Wende, 2007). Business value can be lost due to poor data quality in organisations, which leads organisations to engage in data governance in order to achieve higher data quality (Weber et al., 2009).

Furthermore, good data governance practices are clearly essential for organisations to ensure that all this data is well understood, trusted, accessible, accurate and secure. A good data governance framework also can help people within that organisation to create a clear mission, achieve clarity, increase confidence in using the organisational data, establish accountabilities, maintain scope and focus, and define measurable successes (Panian, 2010; Fu et al., 2011). Experts in this field have shown that if organisations do not implement data governance, the chaos is not obvious, but the indicators are easy to see: dirty data, redundant data, inconsistent data, inability to integrate, poor performance, terrible availability, little accountability, users who are increasingly dissatisfied with IT performance, and a general feeling that things are out of control (Niemi, 2011; Seiner, 2014).

Seiner (2014) argues that an organisation must design a data governance model of role responsibilities in order to identify people who have a level of accountability for defining, producing and using data in the organisation. Redman (2013) argues that organisations should move responsibility for data out of the IT department. Therefore, data governance requires the participation and commitment of IT staff and business management, and senior-level executive sponsorship in the organisation. Furthermore, the organisation needs a strategy framework that can be easily implemented in accordance with the needs and sources of the information (Fu et al., 2011; Prasetyo & Surendro, 2015).

The recent trend in data governance concentrates on the data assets and value in cloud computing services. This trend will contribute to changing an organisation's current data governance strategy, such as the organisation's structure and regulations, people, technology, process, roles and responsibilities. Accordingly, this study undertakes a detailed study of data governance and the role it plays in organisations today when they move their data to the cloud computing environment, and how cloud technology affects data governance.

1.3.1. Data Governance and Other Governance Domains

With the emergence of new governance domains – to name but the most relevant ones: Corporate Governance (CG), Information Technology Governance (ITG), Information Governance (IG), Internet Governance and, more recently, Cloud Computing Governance (CCG) – it is easy to confuse them. This has been observed by the researcher in examples in the literature where authors have interchanged these governance domains as if they were the same thing. It is important therefore to differentiate between these domains and, more importantly, to define how they are linked to each other, particularly with respect to data governance. Figure 1.1. is a simplified view of the interrelations between these domains.

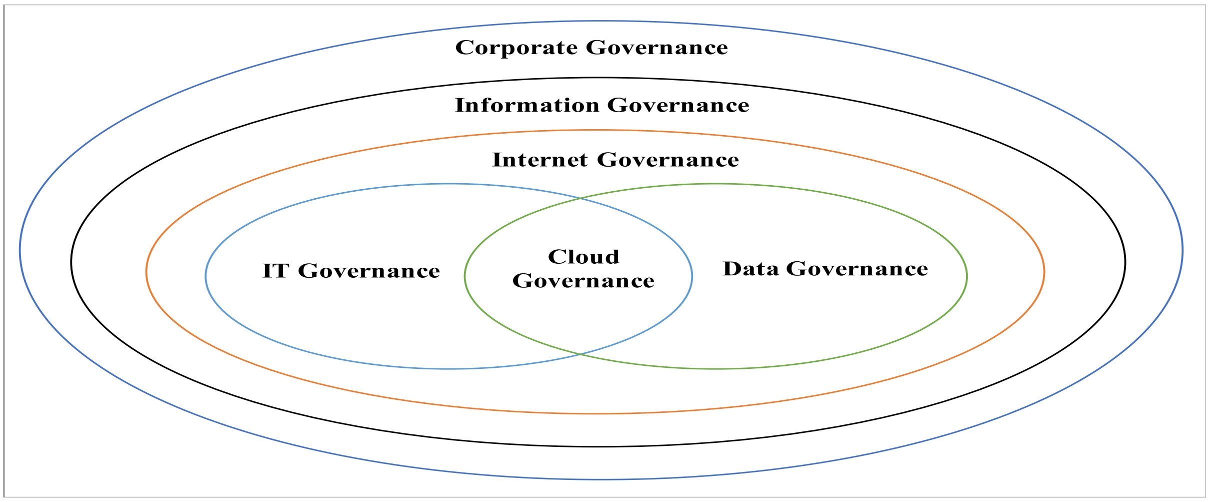

Figure 1.1 The interrelations between governance domains

- **Corporate Governance**

Corporate governance has become important because good governance ensures that the business environment is fair and transparent, and that companies can be held accountable for their actions(Dahlberg & Nokkala, 2015). In contrast, weak corporate governance leads to waste, mismanagement and corruption. Corporate governance can be defined as "*a set of* *relationships between a company's management, its board, its shareholders,* and other *stakeholders, corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining the objectives and monitoring performance are determined*"(Abu-Tapanjeh, 2009, p.558).

- **Internet Governance**

Internet governance can be defined as "*the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet*"(Bauer, 2005, p.5). In addition, the term 'internet governance' was initially used in the technical community to designate the technical management of the Domain Name System and the corresponding root servers, for example of the network infrastructure itself (DeNardis, 2010). However, internet/web governance is not merely about the Domain Name System; that is just one part of internet/web governance. Furthermore, internet contain can be classified into two parts: network infrastructure and data. Thus, in terms of an organisation domain, the internet governance should be merged with other governance domains such as IT governance, data governance and cloud governance.

- **Information Technology Governance (IT Governance)**

In recent years, IT has become the backbone of every business (Preittigun & Chantatub, 2012). As a result, the concept of IT governance has become more important for organisations. IT governance, similar to corporate governance, is the process of establishing authority, responsibility and communication along with policy, standards, control mechanisms and measurement to enable the fulfilment of defined roles and responsibilities (Fernández & Llorens, 2009). Thus, corporate governance can provide a starting point in the definition of IT governance (Weber et al., 2009b). IT governance is defined as "*procedures and policies established in order to assure that the IT system of an organization sustains its goals and strategies*"(Gheorghe, 2011, p.545). It is pertinent, however, to note that there is a difference between IT governance and IT functions; this difference is not just about the centralisation or decentralisation of IT structures, but whether they are also the sole responsibility of the CIO (Debreceny & Gray, 2013).

- **Information Governance (IG)**

The term 'information governance' was introduced by (Donaldson and Walker (2004) as a framework to support the work of the National Health Society in the USA. Unfortunately, many organisations have not yet established a clear distinction between information governance and IT governance (Davis, 2011). Information governance can be viewed as a subset of corporate governance, with the main objectives being to improve the effectiveness and speed of decisions and processes, to reduce the costs and risks to the business or organisation, and to make maximum use of the information in terms of value creation (Williams, 2007). Information governance can be defined as "*the specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information*"(Silic & Back, 2013, p.75). The information governance (IG) approach focuses on controlling information that is generated by IT and office systems or their output, but it does focus on detailed IT or data capture and quality processes.

- **Cloud Governance**

Cloud governance is a new term in the IT field; however, it has not been given a clear definition yet (Woldu, 2013). Microsoft defines cloud governance as "*defining policies around managing the factors: availability, security, privacy, location of cloud services and compliance and tracking for enforcing the policies at run time when the applications are running*"(Woldu, 2013, p.13). The core of cloud governance revolves around the relationships between provider and consumer, across different business models (Saidah & Abdelbaki, 2014). The business model should define the way in which an offer is made and how it is consumed. In order to function at all cloud levels (HaaS, IaaS, PaaS, and SaaS), the business model should be devoid of the type of resources involved.

The literature contains different views on what drives what within these governance domains; this study argues that data governance should be the key driver for all other governance domains, sitting at the heart of it all. The most debated relationship among these governance domains has been between information governance and data governance, where numerous schools of thought, including the Data Governance Institute, have consistently used information and data governance interchangeably, connoting the understanding that the two terms mean the same thing. A very recent paper, published only in 2016 as part of the proceedings of the 28th Annual Conference of the Southern African Institute of Management Scientists, presented a systematic analysis to prove that data governance is indeed a prerequisite for information governance, and hence the argument was extended to state that data governance has to become an ingrained part of both corporate governance and IT governance (Olaitan et al., 2016). Figure 1.2 provides an illustration of the advocated hierarchy of these governance domains, showing also the difference between management and governance.

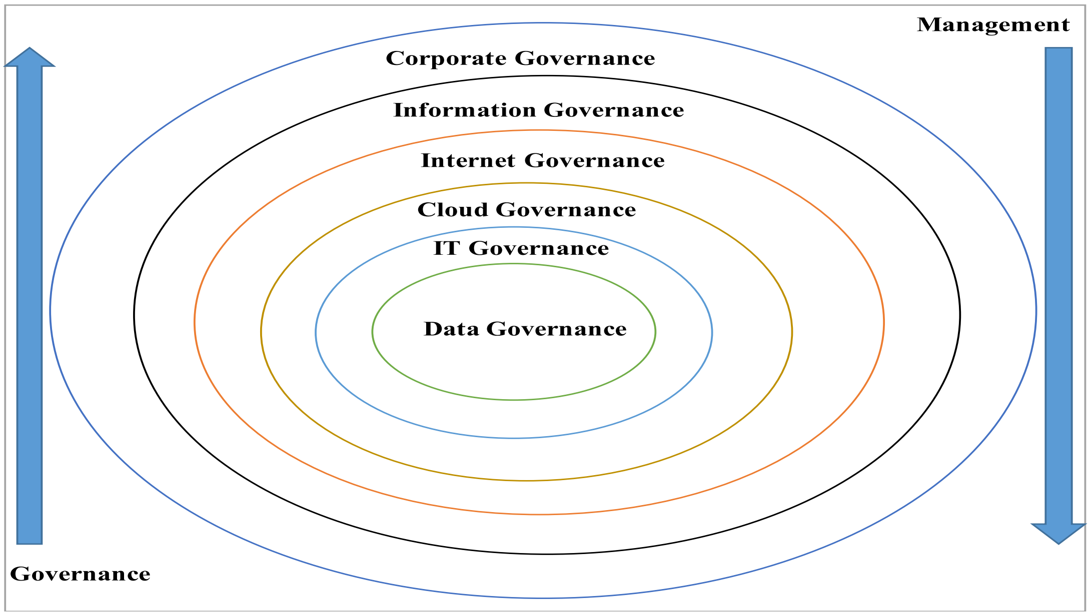

Figure 1.2 The hierarchy between management and governance domains

1.4. Understanding Cloud Computing Technology

Recently, cloud computing has become one of the most significant debated issues of IT, and it has motivated research on related technologies by academia and the industry. In 2007, cloud computing was introduced as an important new topic in the technical and academic fields (Vats et al., 2012). Cloud computing is also an emerging trend and is undergoing serious adoption in both public and private sector organisations. As organisations of all shapes and sizes have begun to adapt to cloud computing, this technology is evolving like never before. Industry experts believe that this new technology will continue to grow and develop even further in the coming few years (Apostu et al., 2013). There are differences between cloud computing and traditional computing in many respects. Khajeh-Hosseini et al. (2010) reiterated this view by pointing out that cloud computing is a shift from computing as a product to computing as a service that is delivered to consumers over the internet. Suri & Mittal (2012) states that the main differences between cloud computing and traditional computing are in the areas of what to manage, the form of the contract, accounting treatment, increments of functionality, development and maintenance tasks, infrastructure tasks, units of measure and cost structure. Cloud computing is composed of various elements from other computational models such as autonomic computing, grid computing and utility computing; it now forms one of the most innovative computational deployment architectures in the modern world.

Cloud computing can be defined as a set of services in IT that are provided to a customer on demand over a network. Hence, for some researchers, Cloud computing promises to be an alternative to supercomputers, clusters and grids (Goyal & Sidhu, 2014). The definition of cloud computing mainly used today is the one expressed by the National Institute of Standards and Technology (NIST) (Jansen & Grance, 2011). The NIST defines cloud computing as "*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*"(Mell & Grance, 2011, p.2). In addition, cloud computing architecture is composed of five essential characteristics, four deployment models, three service delivery models and five cloud actors (Mell & Grance, 2011). NIST was categorised the essential characteristics of cloud computing as: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Cloud computing deployment models are classified into four types: public, private, hybrid and community. Additionally, the fundamental cloud service delivery models include: Infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a Service (SaaS). According to the NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud auditor, cloud carrier and cloud broker, (for more details see Appendix A). Figure 1.3 shows the cloud computing architecture.

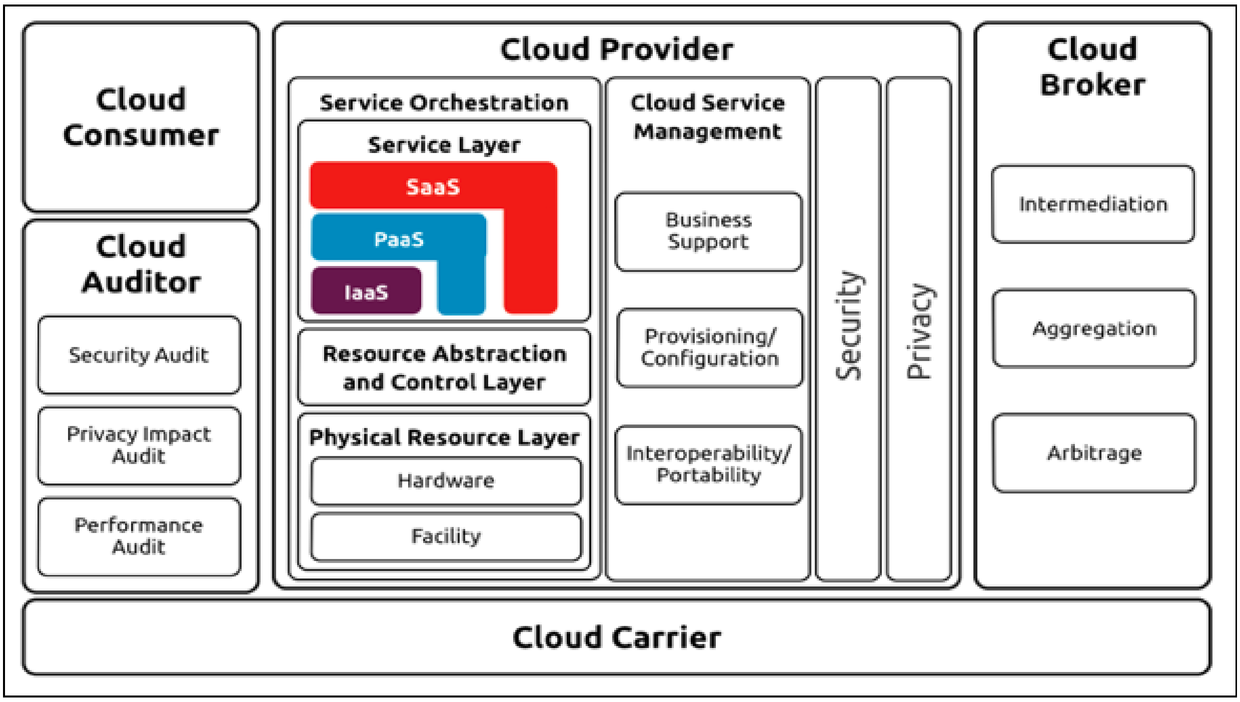

Figure 1.3 Cloud computing architecture. Sources (Jansen & Grance, 2011)

1.5. The Kingdom of Saudi Arabia (KSA)

The Kingdom of Saudi Arabia (KSA) is the official name of the country; internationally, it is widely called Saudi Arabia. Arabic is the official language in the KSA; however, English is widely spoken in the business community. The country is located in the Southern-Eastern part of the Asian continent, with a land area of approximately 2,150,000 km^2 or around 830,000 square miles. According to the General Authority for Statistics in the KSA, the total population was 32,612,641 million in 2016, divided into 57% male and 43% female, and more than half of the population is under the age of 30 (General Authority for Statistics, 2017). Therefore, this high youth rate might allow the KSA to adopt technological solutions more easily because young people might more readily accept technology. Figure 1.4 shows the population of the KSA.

Age Catgory	Saudi			Non-Saudi			Total		
	MALE	FEMALE	Total	MALE	FEMALE	Total	MALE	FEMALE	Total
4 - 0	1106701	1067283	2,173,984	287003	273329	560,332	1,393,704	1,340,612	2,734,316
9 - 5	1081142	1043747	2,124,889	363070	347698	710,768	1,444,212	1,391,445	2,835,657
14 - 10	964304	937211	1,901,515	298963	283506	582,469	1,263,267	1,220,717	2,483,984
19 - 15	911303	880048	1,791,351	245053	229068	474,121	1,156,356	1,109,116	2,265,472
24 - 20	1054864	965980	2,020,844	289368	215931	505,299	1,344,232	1,181,911	2,526,143
29 - 25	979569	958219	1,937,788	736427	437555	1,173,982	1,715,996	1,395,774	3,111,770
34 - 30	882178	866771	1,748,949	963851	435030	1,398,881	1,846,029	1,301,801	3,147,830
39 - 35	773509	754795	1,528,304	1415664	559211	1,974,875	2,189,173	1,314,006	3,503,179
44 - 40	654842	630501	1,285,343	1336843	509983	1,846,826	1,991,685	1,140,484	3,132,169
49 - 45	550260	520676	1,070,936	983252	273808	1,257,060	1,533,512	794,484	2,327,996
54 - 50	438873	414863	853,736	669537	102938	772,475	1,108,410	517,801	1,626,211
59 - 55	342010	314325	656,335	400875	67287	468,162	742,885	381,612	1,124,497
64 - 60	247814	231960	479,774	214599	48138	262,737	462,413	280,098	742,511
69 - 65	150818	159559	310,377	74465	29692	104,157	225,283	189,251	414,534
74 - 70	110039	112808	222,847	34081	19175	53,256	144,120	131,983	276,103
79 - 75	70770	72831	143,601	15918	4718	20,636	86,688	77,549	164,237
+ 80	85286	91498	176,784	12595	6653	19,248	97,881	98,151	196,032
Total	10404282	10023075	20427357	8341564	3843720	12185284	18745846	13866795	32612641

Figure 1.4 The Kingdom of Saudi Arabia's population. Source: (General Authority for Statistics, 2017)

The vital importance of the Kingdom of Saudi Arabia location is as a bridge between the Asia and Western world (Al-shehry, 2009). With Africa on one side and Iran and South Asia on the other, it is in the middle of the strategically important Indian Ocean area, as can be seen on the map in Figure 1.5. Regarding the economy, the KSA's economy is oil-based, and it has the largest reserves of petroleum in the world (Al-shehry, 2009).

The petroleum sector accounts for roughly 75% of budget revenues, 45% of GDP, and 90% of export earnings. Around 40% of GDP comes from the private sector (General Authority for Statistics, 2017). However, there are many other resources that enhance the Saudi economy, such as natural gas, iron ore, gold and copper. In 2016, the Saudi government established Saudi Vision 2030, which aims to encourage private sector growth in order to reduce the Kingdom's dependence on oil (Saudi Vision 2030, 2017). As a contribution to achieving the goals of the Saudi Vision 2030, the digital transformation of industry in Saudi Arabia is a big opportunity to improve and grow businesses.

Figure 1.5 The map of the Kingdom of Saudi Arabia.

Information and Communication Technology (ICT) is now playing an essential role in the economies of many nations, and the government of the KSA has given it top priority (Kurdi, 2013; Salem Basamh et al., 2014). Governments around the world are adopting web-based technologies and the internet in their daily tasks for cost reductions and better resource utilisation purposes. Thus, the concept of electronic government (e-government) has emerged over recent years (Almarabeh et al., 2016). E-government utilises ICT to deliver government services. The government of the KSA attaches high significance to the e-government concept and the transformation process that leads to its realisation, as it is a way of reducing costs, improving services, saving time and increasing effectiveness and efficiency across the public sector (Kurdi, 2013; Salem Basamh et al., 2014). As a result, the government of the KSA has already started the process of implementing an e-government strategy. ‘YESSER’ has been the umbrella organisation and the overall controller of all procedures, activities and all other issues and acts related to e-government implementation in the Kingdom (Salem Basamh et al., 2014). In spite of this, IT in the KSA is still a relatively young technology if compared to some developed countries like the UK, the USA, Canada and Japan.

The Saudi Arabian government has realised the importance of using ICT to provide high-quality services in its organisations (Alharbi et al., 2016). ICT investments have been increasing in the recent past, based on the government’s strategic aims. Among Saudi organisations, key strategic aims for ICT investments involve improving operational efficiency, improving the alignment of ICT with business needs, skills development, and enhancing innovation and customer relationships (CITC, 2015). Cloud computing is considered to be one of the most significant technology initiatives being prioritised as an investment target by organisations in Saudi Arabia (CITC, 2015). In 2010, the government and telecommunications companies initiated efforts to adopt cloud computing in Saudi Arabia (Alkhater et al., 2014; Alsanea, 2015). Nevertheless, government organisations have still not widely adopted cloud computing in their work (Tashkandi & Al-Jabri, 2015; Alsanea, 2015). Thus, inevitably, Saudi Arabia’s government organisations need to outsource their IT functions while they focus on their core business areas.

Furthermore, a few studies have made several attempts to help decision makers in Saudi organisations address their concerns about cloud computing adoption. The majority of these studies focus on factors influencing the adoption of cloud computing in Saudi Arabia (Alhammadi, 2013; Alsanea, 2015). A few other studies have also focused on the adoption of cloud computing in specific government organisations such as healthcare and the higher education sector (Alkhater et al., 2014; Tashkandi & Al-Jabri, 2015; Alsanea, 2015; Alharbi et al., 2016). These studies divided the issues influencing the adoption of cloud computing in Saudi government organisations into three key dimensions, namely: organisational, environmental and technology factors. The organisational factor includes enterprise size, top management support, organisation readiness and enterprise status. The environmental factor includes competitive pressure, external support, government support, regulatory policies and compliance with regulations. Finally, the technology factor includes technology readiness, security, privacy, availability, reliability, vendor lock-in, trust and technical barriers. Moreover, one of the main reasons why cloud services are not adopted in government organisations in Saudi Arabia is that there are no rules or regulations governing the organisation's sensitive data when it moves to a cloud services provider (Alkhater et al., 2014).

According to an ICT investment report published by the Communications and Information Technology Commission in Saudi Arabia in 2015, private cloud services are the most important area of ICT investment, at approximately 47%, and public cloud services account for around 24%. This report also forecasts strong growth for cloud services within the KSA, equating to a Compound Annual Growth Rate (CAGR) of 57.7% over the period extending to 2017. Also, a recent survey conducted by EMC Corporation showed that nearly 32% of Saudi Arabia organisations are using hybrid cloud deployment (MCIT, 2014). It forecast that, by 2016, the government of Saudi Arabia would have invested approximately $83 billion into cloud computing services, which will help government organisations to increase their adoption of cloud computing technology (MCIT, 2014). In 2014, there was a high order from the Saudi government regarding the formation of a higher committee to build regulations and governance requirements for the cloud, to increase its use in government organisations (MCIT, 2014).

1.5.1. Saudi Arabia's Vision 2030

The KSA has a leading position in the world through its geographic, cultural, socio, demographic and economic advantages. The government launched Saudi Vision 2030 to build the best future for Saudi Arabia (Saudi Vision 2030, 2017). The digital transformation of industry in Saudi Arabia is a big opportunity to improve and grow business, which would help to achieve the goals of Saudi Vision 2030.

With regard to digital transformation, IT professionals are witnessing its impact from a unique perspective. The proliferation of technology means there is more complexity to manage, and the elevated role of technology in businesses means that the impact and outcome of the services IT provides have never been more visible or more valued. Emerging technologies such as mobile apps, cloud computing and smart infrastructure will be considered in this vision. Therefore, the transfer of sensitive data between these technologies requires a governance strategy to reduce the digital transformation challenge.

However, the Council of Economic and Development Affairs has developed a comprehensive governance model aimed at institutionalising and enhancing its work, facilitating the coordination of efforts among relevant stakeholders and effectively following up progress for achieving Saudi Arabia's Vision 2030 (Saudi Vision 2030, 2017). Figure 1.6 illustrates the governance model for achieving Saudi Arabia's Vision 2030. This model will encourage public sector organisations in Saudi Arabia to develop a governance model in order to implement their digital transformation programmes, and to govern their digital data.

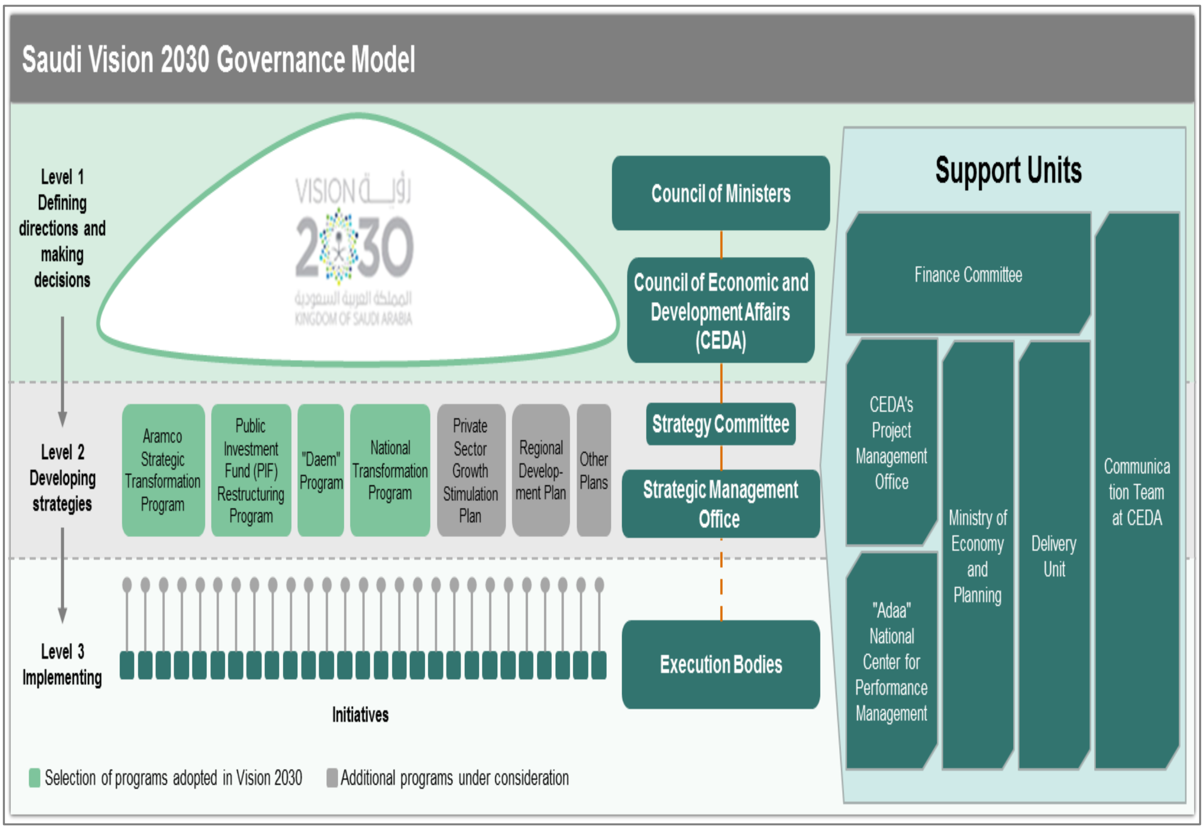

Figure 1.6 The governance model for achieving Saudi Arabia's Vision 2030. Source: (Saudi Vision 2030, 2017)

In Saudi Arabia's Vision 2030, public sector organisations will adopt cloud computing in their businesses; thus, this requires them to expend more efforts to build a strong strategy to get control of their data when it moves to the cloud environment. As data governance is one of the main impediments to the wider adoption of cloud computing in most organisations, public sector organisations in Saudi Arabia should consider the concept of a governance model when deciding how to govern their data in the cloud computing environment, as this will contribute to the achievement of Saudi Vision 2030.

1.6. Research Problem Statement and Motivation

In today’s world it is impossible not to acknowledge the impact of technology on development and organisational growth. The use of technology is practically indispensable; it is present in every sector and industry, in small, medium or large enterprises. As IT has become a backbone of every organisation, IT governance has become an integral part of any business strategy, falling under the category of corporate governance(Héroux & Fortin, 2016). Historically, data emerged out of disparate legacy transactional systems, being seen as a by-product of running the business, with little value beyond the transaction and the application that processed it. As such, data was not treated as a valuable shared asset. This was the trend until the early 1990s, when the value of data, beyond that of recording transactions, started to be recognised. Business decisions and processes increasingly became driven by data and data analysis (Kamioka et al., 2017). Further investment in data management approaches aimed to tackle the increasing volume, velocity and variety of data that came to the fore. Among such approaches were complex data repositories, data warehouses, ERP and CRMs. Data links became very complex and were shared amongst multiple systems; the need for providing a single point of reference in order to simplify daily functions became crucial, which gave birth to Master Data Management.

Data complexity and volume continue to explode, as businesses have grown more sophisticated in their use of data. This growth drives new demands, which entail different ways of combining, manipulating, storing and presenting information. In response, forward-thinking companies recognise that data management solutions on their own are becoming very expensive and unable to cope with business reality; thus they need to solve data problems in a different way, through the implementation of an effective data governance (Imhanwa et al., 2013). Data governance needs to take a policy-centric approach to data models, data quality standards, data security and lifecycle management, and the processes for defining, implementing and enforcing these policies(Benfeldt, 2017). On the same note, the notion of data governance underwent an important transformation towards a new direction. Previous attempts at governing data failed as they were driven by IT, and affected by rigid processes and fragmented activities carried out on a system-by-system basis. Until very recently, governance has been largely informal, in siloes around specific enterprise repositories, lacking structure and the wider support of the organisation.

Cloud computing is one of the most popular recent technological trends. Despite the numerous benefits of cloud computing, it is still not widely adopted by public sectors in many countries, due to a number of issues and challenges(Owuonda et al., 2016). Central to these concerns is the loss of control over data, the security and privacy of data, data quality and assurance, and data stewardship, which are all attributes of data governance. Therefore, in the literature, the cloud computing model was discussed as a highly disruptive technology, requiring extremely rigorous data governance strategies and programmes that may be complex, but necessary. However, very few studies have reported on data governance for cloud services, despite its significance. Furthermore, digital transformation in Saudi Arabia is one of the core elements of achieving the goals of Saudi Vision 2030. In this thesis, the author argues that data governance plays a vital role in the success of this vision. This role is further emphasised when considering the country’s appetite for emerging technologies such as cloud computing solutions. Cloud computing is expected to be one of the main foundational enablers in future digital transformation projects; in Saudi Arabia it will offer the scale and speed that is needed for businesses and public organisations to achieve the vision’s goals. However, the literature review gathered evidence that the fear of the loss of data governance is one of the main obstacles to the adoption of the cloud model.

As discussed above, a central point of concern is the lack of understanding about data governance in most organisations in different countries. This is particularly crucial considering that data governance is a major concern for organisations when they move their data to the cloud. This concern is borne from the fact that a loss of data governance would mean that cloud consumers would lose control of their sensitive data in the cloud environment (Ko et al., 2011). The partnership between cloud consumers and providers in terms of designing, building, deploying and operating cloud computing technology presents new issues in providing adequate security and privacy, and protecting data in different delivery models(The Data Governance Institute, 2015). A collaborative process between cloud consumers and providers, meaning that they share the responsibilities of implementing the necessary controls, therefore becomes crucial. In this way, cloud consumers have a sense of security and reliability as they understand exactly how the process of data control functions and runs in the cloud computing environment. An effective data governance process will achieve this by clarifying responsibilities to cloud consumers when they move their data into cloud environments. Figure 1.7 presents the research problem statement.

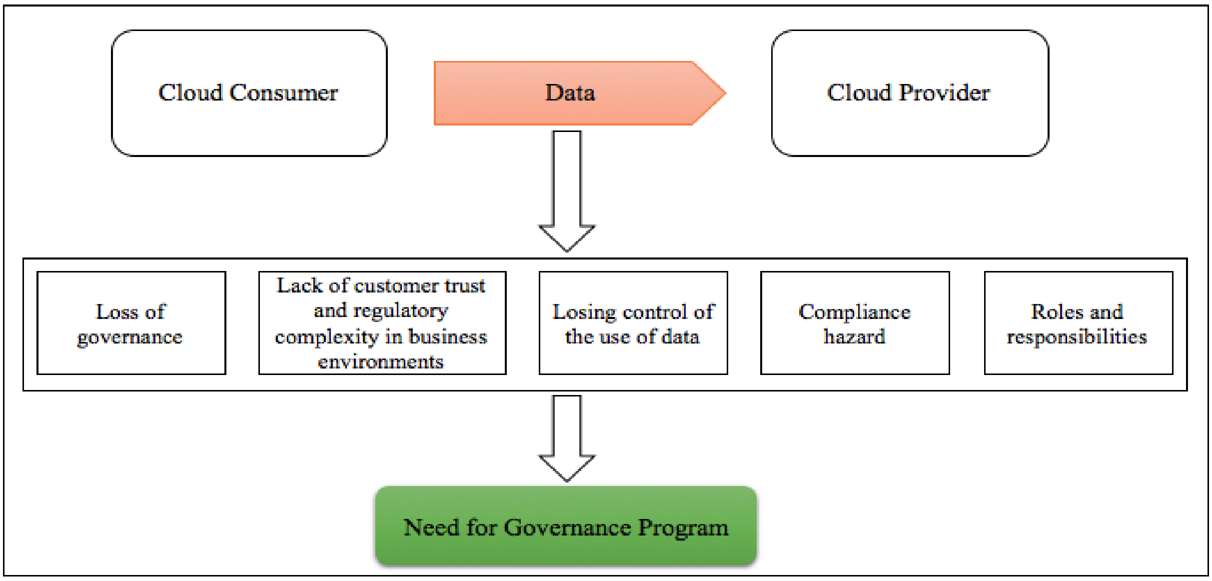

Figure 1.7 Research Problem Statement.

As one size does not fit all, currently there is no single approach to implementing data governance programmes in all organisations (Weber et al., 2009; Begg & Caira, 2012). Therefore, each organisation should develop its data governance programme based on its own requirements to achieve its strategy. The motivation for this research is the need to determine the important requirements for the development of an effective cloud data governance programme, which will help organisations to maintain control of their data in cloud computing environments. Therefore, the following five factors emphasise the motivation of this study:

- The majority of the current research focuses on data governance aspects for traditional IT (non-cloud) environments, and there is a lack of research on data governance for cloud computing services.
- Consideration of special features in data governance that arise as a result of the differences between cloud computing and traditional IT (non-cloud).
- Almost no research on data governance for traditional IT and cloud computing services in Saudi Arabia.
- The lack of empirical studies that investigate data governance in general, and more specifically cloud computing.
- The lack of knowledge in public sector organisations in Saudi Arabia about how to design data governance programmes in general, and for the cloud computing environment.

1.7. Aim and Objectives of the Study

The aim of this study is to develop a strategy framework to design, deploy and sustain an effective cloud data governance programme. The objectives are:

1. To conduct a systematic literature review (SLR) to understand the state of the art of data governance, including:
   - Data governance for non-cloud environments.
   - Data governance for cloud computing environments.
   - Existing strategies and frameworks for implementing data governance.
   - The development of a Cloud data governance Taxonomy.
   - Defining the key dimensions of cloud data governance.
2. To propose and develop a Strategy Framework to understand how to design, deploy and sustain an effective cloud data governance programmes in organisations.
3. To propose and develop a cloud data governance Maturity Model.
4. To propose and develop an assessment matrix to assess cloud data governance.
5. To conduct a Case Study for the Saudi Arabia Public Sector, including:
   - To investigate the current state of cloud data governance in the Saudi Public Sector
   - To investigate the Barriers to implementing cloud data governance in the Saudi public sector
   - To investigate the Critical Success Factors (CSFs) for implementing cloud data governance in the Saudi Public Sector.
   - To validate and evaluate the research findings for the Case Study, including:
     - To validate and evaluate the proposed Strategy Framework for cloud data governance for the Saudi Public Sector.
     - To evaluate the cloud data governance maturity model for the Saudi Public Sector.
     - To evaluate the cloud data governance assessment matrix for the Saudi Public Sector.

1.8. Research Questions

Based on the research aims and objectives in this study, the following question is addressed:
RQ 1: How to Design, Deploy, and Sustain Cloud Data Governance Programme in the Saudi Public Sector?

1.9. Research Methodology

The research methodology of this research is based on the concept of the research onion developed by Saunders et al. (2009), which defines the research philosophy, research approach, research strategy, techniques and procedures. These are illustrated in Figure 1.8 below and described in the sub-sections that follow.

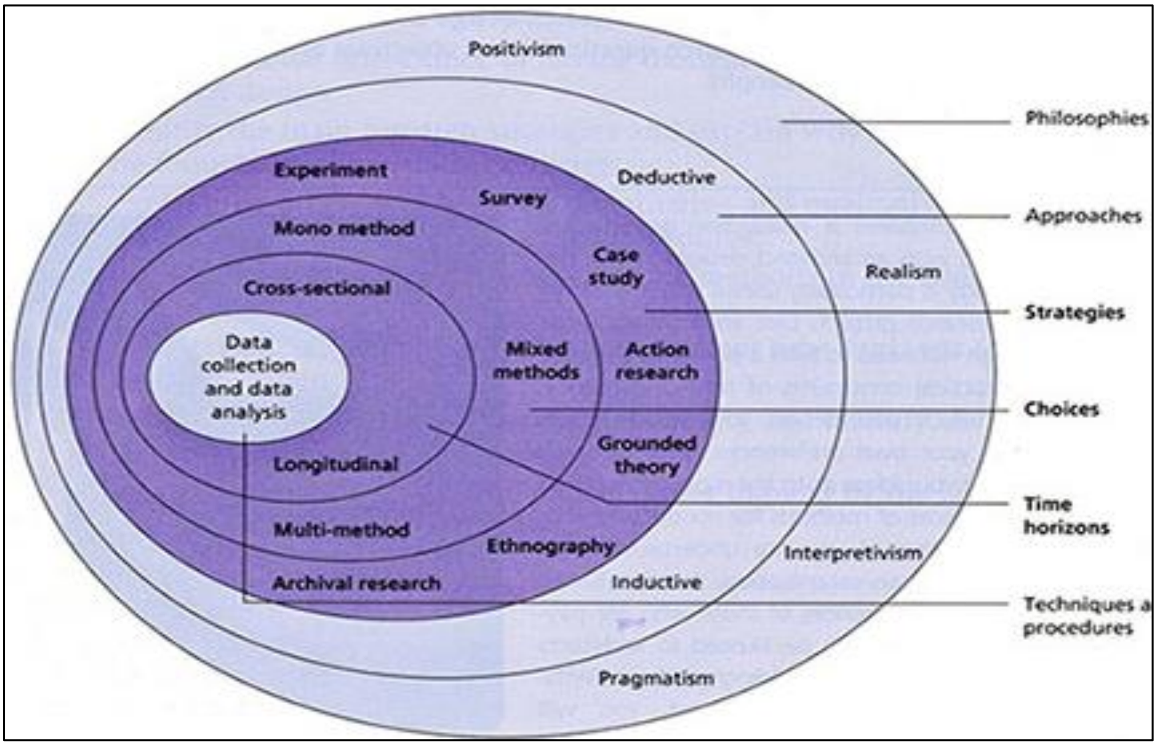

Figure 1.8 The research onion. Source: Saunders et al. (2009)

1.9.1. Research Philosophy

A research philosophy is a belief that affects how the researcher gathers, analyses and uses data about a specific phenomenon (Davidson, 2004). Four types of research philosophies have been recognised: positivism, realism, interpretivism and pragmatism (Saunders et al., 2009). These philosophies have different views on directing all of the phases of research – from the theoretical basis to the collection and analysis of data. In the positivism philosophy, "*positivists believe that reality is stable and can be observed and described from an objective viewpoint, i.e. without interfering with the phenomena being studied*"(Gicheru, 2013, p.131). In the interpretivism philosophy, interpretivists contend that only through the subjective interpretation of and intervention in reality can that reality be fully understood. The study of phenomena in their natural environment is key to the interpretivist philosophy, together with the acknowledgement that scientists cannot avoid affecting the phenomena they study. They admit that there may be many interpretations of reality, but maintain that these interpretations are in themselves a part of the scientific knowledge they are pursuing. Interpretivism has a tradition that is no less glorious than that of positivism, nor is it shorter.

Regarding the realism philosophy, it was defined by Phillips in 1987 as “*the view that entities exist independently of being perceived, or independently of our theories about them*.” Schwandt adds that “*scientific realism is the view that theories refer to real features of the world. ‘Reality’ here refers to whatever it is in the universe (i.e., forces, structures, and so on) that causes the phenomena we perceive with our senses*” (Maxwell, 2012, p.3). With regard to the fourth philosophy, which is the pragmatism philosophy, it involves an interest in actions (Goldkuhl, 2004). Goldkuhl (2004,p.3) has argued that "*the primary concern, following a pragmatist position, in the empirical world is actions; this does not mean that a pragmatist is only concerned with actions and disregards other issues*". Additionally, this philosophy provides the researcher with the freedom to use any of the methods, techniques and procedures to conduct the research (Kolberg & Magill, 2002). The research procedure of this study was designed in order to capture a pre-existing phenomenon, which is data governance in the cloud computing environment, and to investigate the CSFs and barriers affecting its implementation by observations in the real world, using different methods and techniques. Thus, the pragmatic philosophy is adopted and it is suitable for this research because it provides holistic views of the research problem under discussion.

1.9.2. Research Approach

Research approaches can be classified into two types – inductive and deductive (Burney, 2008). The inductive approach is a bottom-up approach, which means that the researcher therefore infers the implications of his or her findings, and a theory is the outcome of this approach (Burney, 2008). On the other hand, the deductive approach is the opposite of the inductive approach in that it is a top-down approach, which means that the researcher has a clear theoretical position before starting the data collection process (Saunders et al., 2006). The theoretical position will be based on an existing body of theory. Then the researcher will examine the application of this theory to specific instances (Burney, 2008). Therefore, the deductive approach is used in this study because it is the most suitable for this study and it gives the researcher the opportunity to identify more explanations for the phenomenon under investigation (Burney, 2008). Furthermore, this study will start with an analytic theory. In the literature chapter, the state of the art of data governance for non-cloud and cloud computing environments and a set of critical success factors (CSFs) will be reviewed based upon existing published work. In this step a set of CSFs will be produced as a hypothesis. Subsequently, this thesis describes the way in which will data will be collected through a questionnaire, and then the results of the data collection will be analysed. Finally, each of the CSFs will be evaluated and will be either confirmed or rejected.

1.9.3. Research Strategy and Data Collection Method

The research strategy can be divided into two methods: qualitative and quantitative (Saunders et al., 2006). The qualitative method emphasises words rather than quantification in the collection and analysis of data, and it aims to gain an in-depth explanation or understanding of a given topic or phenomenon (Mack et al., 2011). On the other hand, the quantitative method entails the collection of numeric data, hence the results will often be presented in numbers; the data is usually collected by using a questionnaire (Burney, 2008). Therefore, this research adopts the triangulation method, which is used to combine the advantages of both the qualitative and the quantitative research approaches (Yeasmin & Rahman, 2012). This research will include the use of primary research tools such as a questionnaire and focus group. In addition, secondary research sources will be used in this research, such as articles, journals, books and industry reports, etc.

An online survey (questionnaire) was used in this study to investigate the state of cloud data governance in public sector organisations in Saudi Arabia. The online survey was chosen for this study because it yields faster responses, with a centralised database of responses that are easier to analyse (Saunders et al., 2006). Additionally, the case study will allow the researcher to retain the holistic characteristics of real-life events while investigating empirical events (Fletcher et al., 2007). Therefore, this research uses a case study in Saudi Arabia to validate and evaluate the proposed framework, maturity model and assessment matrix for the cloud data governance through a focus group.

1.9.4. Research Design and Investigation Procedure

In order to address the different objectives to be achieved in this research, the findings of this research will be identified by a two-sequential phase approach. The steps to achieve these phases are listed as follows:

- ***Phase One:*** To conduct secondary research, which covered the following steps, also summarised in Figure 1.9:

1. The research started with a systematic, extensive literature review to understand the state of the art of data governance in both non-cloud and cloud computing environments. Existing strategies and frameworks for implementing data governance are considered in this review. The CSFs and barriers that affect the implementation of cloud data governance are also considered in this review. In addition, the results of a systematic review are evaluated and analysed to develop the data governance taxonomy and to identify the key dimensions of data governance for both non-cloud and cloud computing. Therefore, the research gap will be considered in this step. This step is presented in Chapter Two.
2. The proposed Strategy Framework: this framework is based on the outcome of the systematic literature review and analytic theory process, which includes the CSFs, existing frameworks and cloud data governance key dimensions. The proposed framework is formulated as a strategy to understand how to design, deploy and sustain an affective cloud data governance programme. This step is presented in Chapter Three.
3. Developing the cloud data governance Maturity Model: this model aims to help organisations understand the current level of their cloud data governance. More importantly, the maturity model can identify a path for the growth of cloud data governance in the future. This phase is based on the results of the literature review, existing maturity models and the cloud data governance framework developed in Chapter Three. This step is presented in Chapter Four.
4. Developing an assessment matrix to assess the cloud data governance’s level of maturity, in organisations. This assessment matrix aims to build a roadmap to assess organisations and to enable them to obtain an effective cloud data governance. This step will be based on the proposed framework, the cloud data governance maturity model and the existing assessment matrices in the literature. This step is presented in Chapter Four.
5. To develop means for practical evaluation

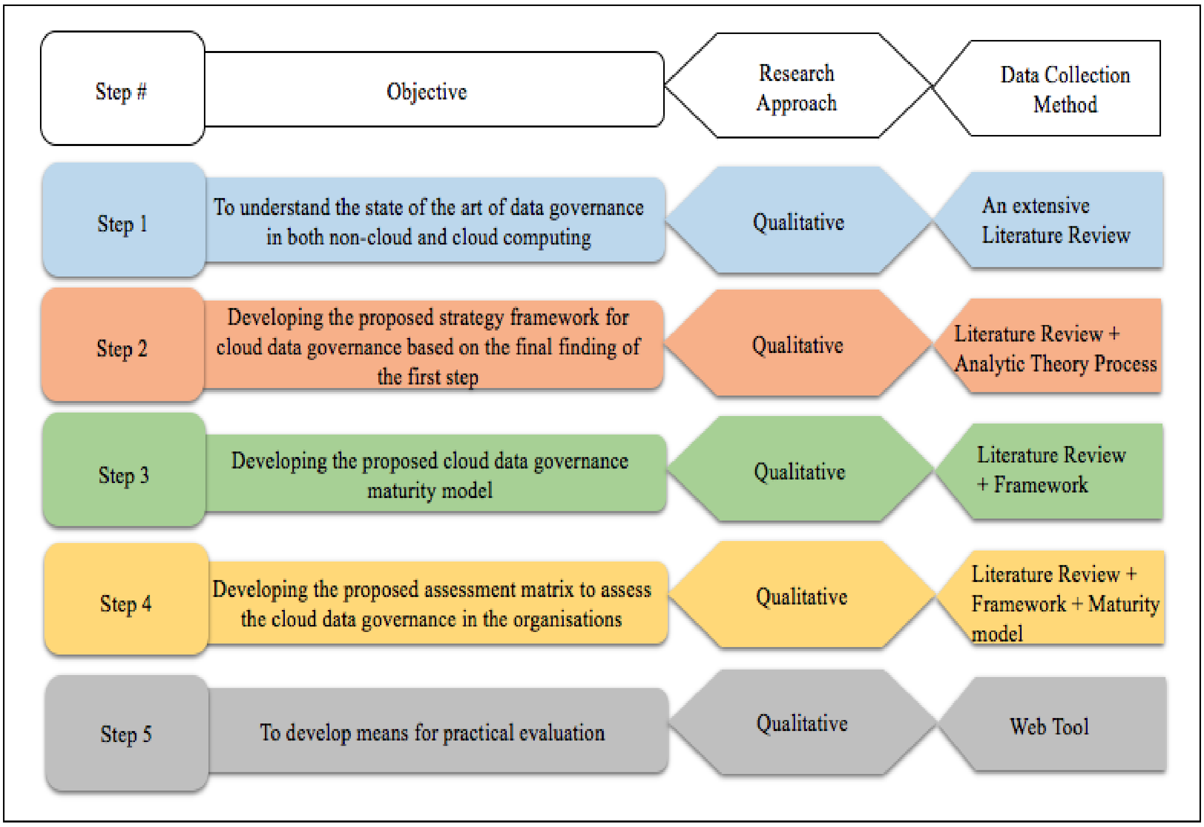

Figure 1.9 The steps to achieve phase one for addressing the research objectives

- <u>***Phase Two:*** To validate and evaluate the research findings for the defined Case Study. This Phased covered the following steps, also summarised in Figure 1.10:</u>

1. Empirical study of the current state of cloud data governance in the public Sector in Saudi Arabia. This step conducted a primary research to investigate the current state of cloud data governance, cloud computing, CSFs for the implementation of cloud data governance and the barriers to doing so from the perspectives of public sector organisations via a questionnaire. This step is presented in Chapter Five.
2. Validating the proposed Strategy Framework through a case study in Saudi Arabia. The validation will be conducted by a focus group comprising experts from several different public sector organisations and the largest cloud providers in Saudi Arabia. This step is presented in Chapter Six.
3. Evaluating the proposed Strategy Framework through structural equation modelling techniques based on the results of the questionnaire. This step is presented in Chapter Six.
4. Validating the proposed Maturity Model through a case study in Saudi Arabia. The validation will be conducted by a focus group comprising experts from several different

public sector organisations, the largest cloud providers, and academics in Saudi Arabia. This step is presented in Chapter Seven.

5. Validating the proposed Assessment Matrix through a case study in Saudi Arabia. The validation will be conducted by a focus group comprising experts from several different public sector organisations, the largest cloud providers, and academics in Saudi Arabia. This step is presented in Chapter Seven.
6. Conducting practical evaluation of the cloud data governance assessment matrix for selected organisations as case scenario of Saudi public sectors.

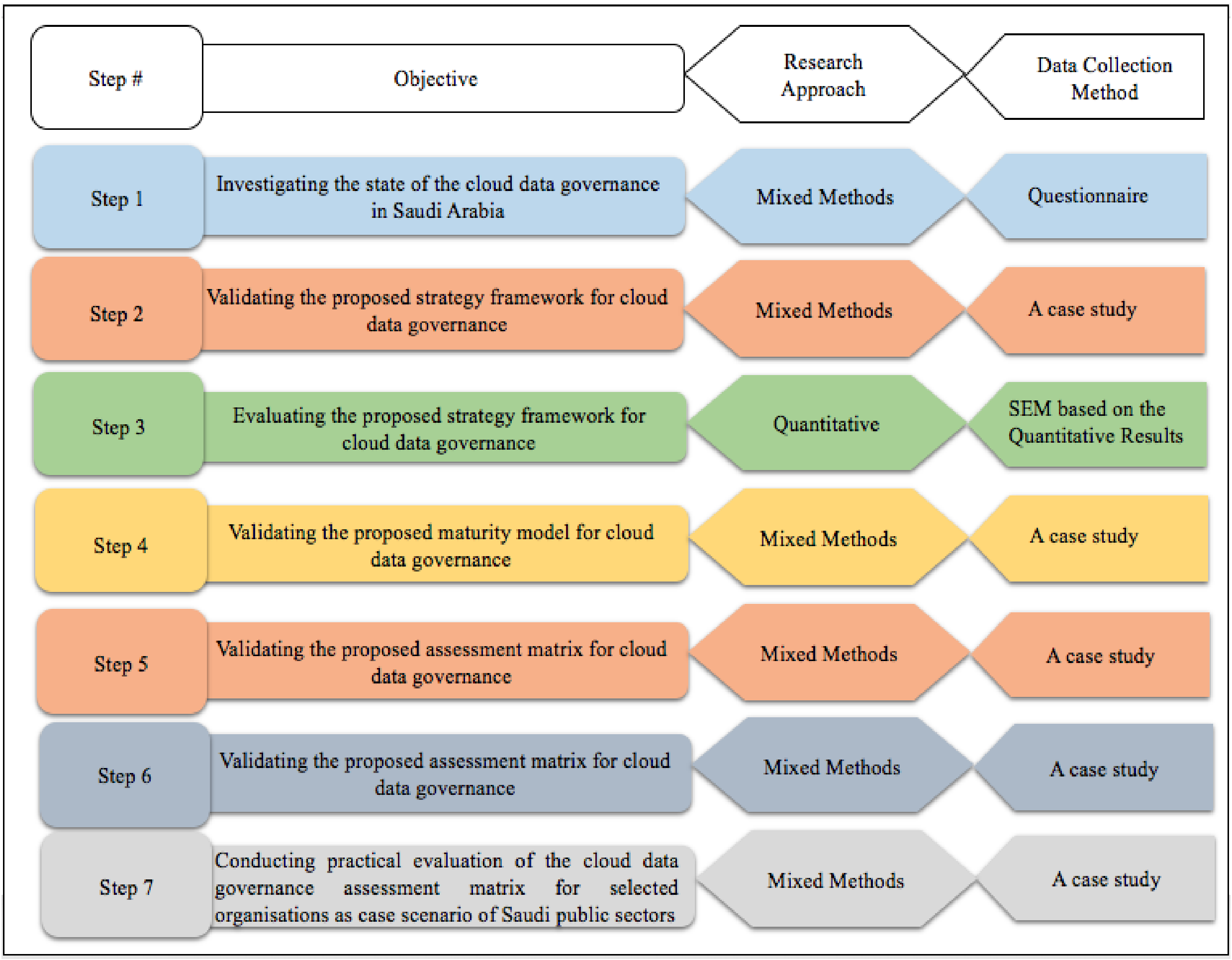

Figure 1.10 The steps to achieve phase two for addressing the research objectives

1.10. Research Contributions to Knowledge

The contributions to knowledge in this research project include the following:

1. Identifying the research gaps and the significance of the defined scope of the research. The impact of the results from the study could be significant for organisations in

different countries. This is justified by the lack of research and development and practice on cloud data governance.

2. A critical evaluation of the state of the art of data governance in non-cloud and, more specifically, in cloud computing, including the identification of Critical Success Factors and Barriers to implementing effective cloud data governance in organisations.
3. Developed a Data Governance Taxonomy to understand the Key Dimensions of Cloud Data Governance.
4. Developed a Strategy Framework to understand how to Design, Deploy and Sustain an effective cloud data governance programme.
5. Developed a cloud data governance Maturity Model to assess the utility of the strategy framework.
6. Developed a cloud data governance Assessment Matrix to support the cloud data governance maturity model.
7. Developed and tested a Tool to facilitate the assessment activity in a real case scenario.
8. Validated and evaluated the research outcomes (1-7 above) for the Case Study of this Thesis.

1.11. Ethical Considerations

Ethical considerations are a significant aspect of any research design (Fox et al., 2003). In this study, a number of steps were implemented to meet the standards of ethical research practice. Firstly, the proportionate review form was approved by the university's ethics committee (see Appendix C). Secondly, all participants were informed about the researcher's topic and that participation in the survey was voluntary and anonymous.

Thirdly, a consent form was used in the questionnaire and in the focus group to tell participants that their participation was voluntary and that they could withdraw at any time for any reason. The contact details of the researcher and supervisor were also given in the cover letter so that they could be contacted if the respondents had any ethical concerns. Finally, the participants were informed that their data would be treated with full confidentiality and that, if published, it would not be identifiable as theirs.

1.12. Structure of the Thesis

The thesis is organised into eight chapters (see Figure 1.11), the content of which is summarised as follows:

Chapter One: Introduction to the Study

This chapter presents the background of the research, the research questions, aims and objectives, and the research methods. The research problem statements and motivation are also considered in this chapter. This chapter provides an overview of data governance, cloud computing, and the research case study background (KSA). The major contributions to knowledge made by this research and its ethical consideration are also presented in this chapter. Finally, the chapter presents the structure of the whole thesis.

Chapter Two: Systematic Literature Review of Data Governance

This chapter investigates the relevant studies in the literature, and provides a systematic review to conduct the state of the art of the data governance for non-cloud and cloud environments. The chapter takes account of previously published works on data governance by accredited scholars and researchers in academia and industry. Critical success factors (CSFs) and barriers that influence the implementation of data governance for non-cloud and cloud computing will be considered in this chapter.

Chapter Three: A Strategy Framework for Cloud Data Governance

This chapter presents a framework for designing, deploying and sustaining effective data governance for cloud computing services. The framework is based on the results of the systematic literature review, and the existing frameworks and important CSFs are considered when developing the framework.

Chapter Four: Cloud Data Governance Maturity Model and Assessment Matrix

This chapter presents the maturity model for cloud data governance, which will help cloud consumers to understand the state of their data governance, and to identify the appropriate data governance target level for their organisations. An assessment matrix to assess cloud data governance is also presented in this chapter.

Chapter Five: State of Cloud Data Governance in Saudi Arabia

This chapter presents the details of the research methodology used to design the questionnaire and it discusses the results of the online survey. The questionnaire aims to understand the state of data governance and cloud computing in Saudi Arabia's public sector. The CSFs and barriers to implementation of cloud data governance will also be investigated and the results will be analysed in this chapter.

Chapter Six: Validation and Evaluation of the Cloud Data Governance Framework

This chapter discusses and highlights the validation and evaluation process and results of the proposed framework in order to develop a strategy to design, deploy and sustain an effective cloud data governance programme. The validation process aims to determine whether the research findings used for developing the framework are sound and to establish whether these findings are reliable. In addition, a focus group was held to validate the cloud data governance framework through a case study in Saudi Arabia. In addition, Structural Equation Modelling (SEM) has been used to evaluate and assess the research framework and to test the research hypotheses based on the questionnaire findings.

Chapter Seven: Evaluation of the Cloud Data Governance Maturity Model and Assessment Matrix

This chapter discusses and highlights the validation of the proposed cloud data governance maturity model and the assessment matrix. The validation process aims to determine whether the research findings used for developing the maturity model and assessment matrix are sound and to establish whether these findings are reliable. In addition, a focus group was held to validate the cloud data governance maturity model and assessment matrix through a case study in Saudi Arabia. The cloud data governance tool will be used in this study to assess and evaluate the current state of cloud data governance in two organisations based on the assessment matrix.

Chapter Eight: Research Conclusions and Recommendation

This chapter summarises the research outcomes and outlines future directions.

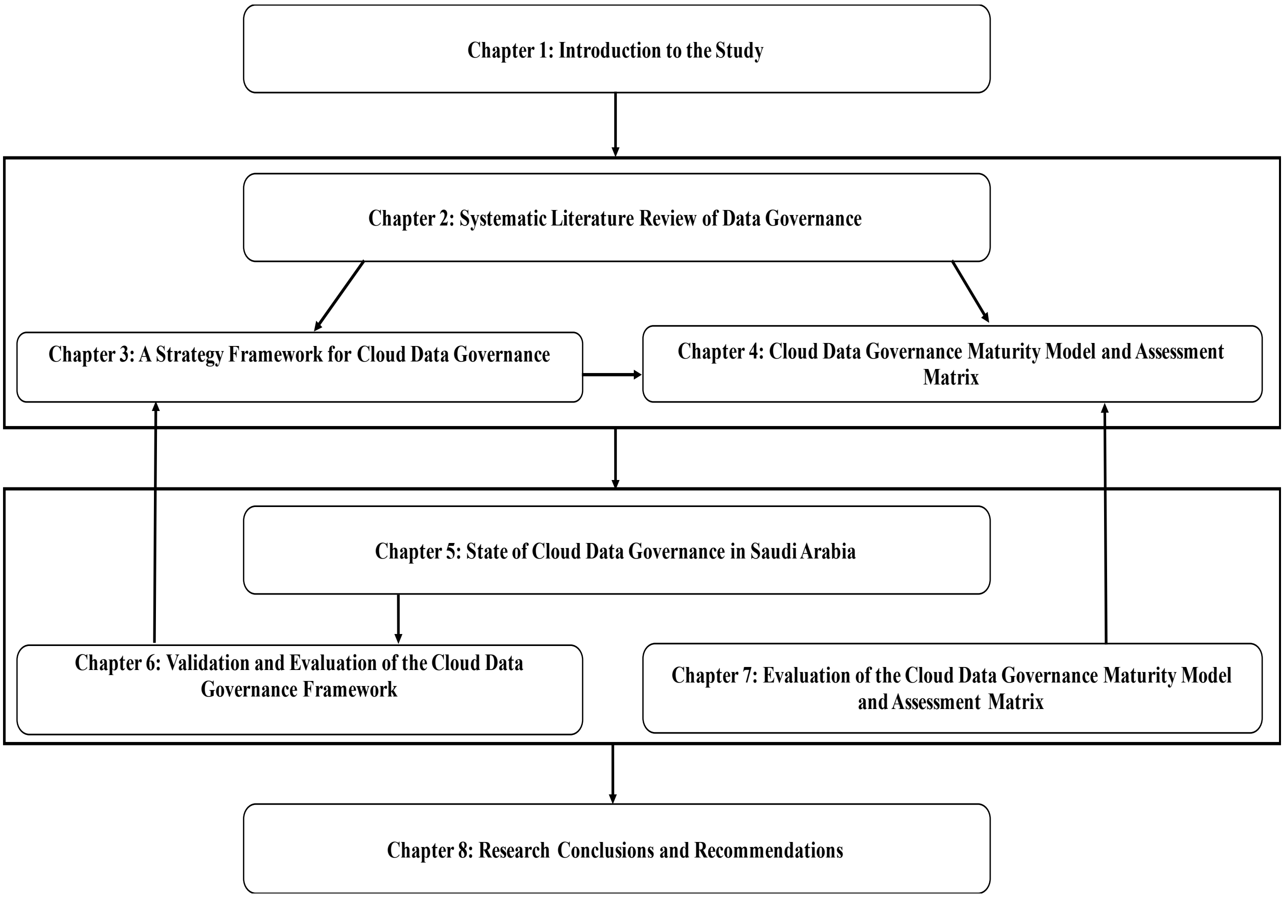

Figure 1.11 Thesis Structure

1.13. Chapter Summary

In summary, this chapter outlines the introduction and background of this study, the research questions, and the aims and objectives. This chapter also provides an overview of data governance, cloud computing, and the research case study background (KSA), the research methodology and the major contributions to knowledge. Ethical considerations and research problem statements and motivation have also been presented in this chapter. Finally, the chapter presents the structure of the whole thesis. The following chapter will present the systematic literature review.

Chapter 2. Systematic Literature Review of Data Governance

2.1. Introduction

This chapter aims to review and examine the existing research on data governance with a particular interest in cloud computing. The systematic review takes account of previously published works on data governance by researchers from academia and industry practitioners. The main goal is to identify the state of the art of data governance in cloud and non-cloud environments and to pinpoint challenges and possible directions for researchers based on the current literature. In this study, the systematic review is carried out to identify data governance requirements, existing frameworks, and CSFs and barriers to implementation of cloud data governance from previous publications. Accordingly, this study undertakes a detailed study of data governance and the role it plays in organisations today.

2.2. Review Process Description

This section describes the process followed to carry out a literature review using a well-studied methodology. The aim of a literature review is to compile and evaluate all the existing research related to the research objectives of interest, therefore achieving unbiased, auditable and repeatable results. The research objectives drive the literature review methodology, which is a critical step in this process. In this study, the research objectives focus on identifying existing data governance frameworks, initiatives and proposals that have been designed to be applied in cloud computing services and in non-cloud services. This study set out to achieve the objectives of the research questions listed in Table 2.1. It used these research questions to determine the content and structure of the literature review and to determine and select the primary studies, critically evaluate these studies, and analyse their results. This study adopted the systematic literature review structure proposed in 2004 by Kitchenham et al. and preferred reporting items for systematic reviews and meta-analysis, to allow the researcher to conduct the research in the field of data governance. The systematic literature review also has been used to answer the stated research questions. A systematic literature review can be defined as "*a means of identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomena of interest*"(Kitchenham & Charters, 2007, p.3). The review protocol used in this study was published by Kitchenham (2004) and Kitchenham and Brereton (2013). These study's inclusion eligibility criteria were fully scientific and practice-oriented sources (big companies interested in the data governance area) that dealt with data governance. The selected articles also had to be full articles that dealt with the data governance of the technical and non-technical implementations of data governance programmes, published in English in format peer-reviewed journals, conference proceedings, books and theses between 2000 and 2017. Exclusion criteria were also adopted in this study (see Table 2.2).

2.3. Systematic Literature Review Research Questions

The most important activity during a systematic literature review is to formulate the research question(s) (Kitchenham & Charters, 2007). In this study, two research questions can be addressed by systematic review (see Table 2.1):

Table 2.1 Research Questions and Motivation.

Research Questions	Motivation
What is the state of the art of research on data governance for cloud computing?	The aim is to find out which aspects of data governance in the cloud have been researched and which have not been researched. This review helps this study to identify what solutions are offered for data governance in cloud and non-cloud environments. Also, the aim is to understand the existing gaps in the data governance framework and process in cloud computing.
What is the state of the art of research on data governance for non-cloud computing?	The aim is to find out what aspects of data governance in non-cloud computing environments have been researched, and to identify the gap in this area to support the main aim of this study.

2.4. Inclusion and Exclusion Criteria

In a systematic literature review (SLR), the researcher needs to explicitly define the search boundaries, in order to ensure the quality of the review with a focused scope; these boundaries are referred to as the inclusion and exclusion criteria and have been defined in (Kitchenham & Charters, 2007). Table 2.2 defines these criteria as applied in the search protocol. According to Kitchenham and Charters (2007), the main purpose of study selection is to identify those primary studies that provide direct evidence about the research question. Selection criteria are based on inclusion and exclusion criteria. The term ‘data governance’ was used in this search, but the researcher also tried a combination of keywords in order to test for synonyms used in the literature and to cover all relevant publications. The following search strings were also used: ‘data governance organisation’, ‘governance data’, ‘data governance in cloud computing’, ‘data governance for cloud computing’ and ‘cloud data governance'. All these search strings were combined by using the Boolean 'OR' operator as follows: ((data governance) OR (data governance organisation) OR (governance data) OR (data governance in cloud computing) OR (data governance for cloud computing) OR (cloud data governance)).

Table 2.2 Inclusion and exclusion criteria for the systematic review

Inclusion criteria	Exclude criteria
• Directly related to data governance in cloud and non-cloud environments. • Data governance framework design in the cloud and in non-cloud environments. • Data governance solutions applied in organisations and in the cloud. • Cloud data governance challenges. • Peer-reviewed. • Written in English.	• Irrelevant to the study of data governance or data governance in the cloud. • Not peer-reviewed papers. • Duplicate publication. • Journals not accessible online. • Not written in English.

2.5. Defining the Review Protocol

The literature review is concept-centric as it classifies and presents the publications according to the data governance areas that are addressed. The research protocol is one of the most important methods in this research because it adds value to the research objectives and goals. This section aims to define the review protocol to review existing research on data governance in the cloud and non-cloud environments (see Figure 2.1). The review protocol comprises four steps:

Step 1: Start with an exploration of the scientific and practice-oriented literature related to data governance. The term data governance was used in this search, but also related terms such as data governance organisation, govern data or data governance in cloud computing or cloud data governance were also employed. The search protocol was applied to many popular academic online libraries (see Table 2.3). Practice-oriented literature was also considered; the searches included paper and report publications by industry associations, software vendors and analysts that have been published by major companies and consultancies, IBM, Microsoft, Gartner, and Cloud Security Alliance. The search focused on the article title, abstract, keywords and dates between 2000 and 2017 for data governance for non-cloud computing, and from 2007 to 2017 for data governance in cloud computing.

Step 2: All sources were analysed by dividing them into two types according to the nature of their contribution: scientific and practice oriented. The scientific format includes papers in journals and conference proceedings, book, working reports and theses. The practice-oriented format includes papers and report publications by industry associations, software vendors and analysts (see Table 2.4). In this step, the table contains important parameters, which are related to the resources: nature of contribution, format type and source's reference.

Step 3: Use the critical literature review techniques to discuss in detail the state of the art of data governance studies in cloud and in non-cloud environments to support the research arguments. Also, in this step the researcher compared the work from different authors in the data governance area, to identify contradictions and inconsistencies in these works. In addition, this technique contributes to knowledge for this research by identifying gaps that do not appear to have been tackled by other authors.

Step 4: Identify the research gap and explain how to fill this gap.

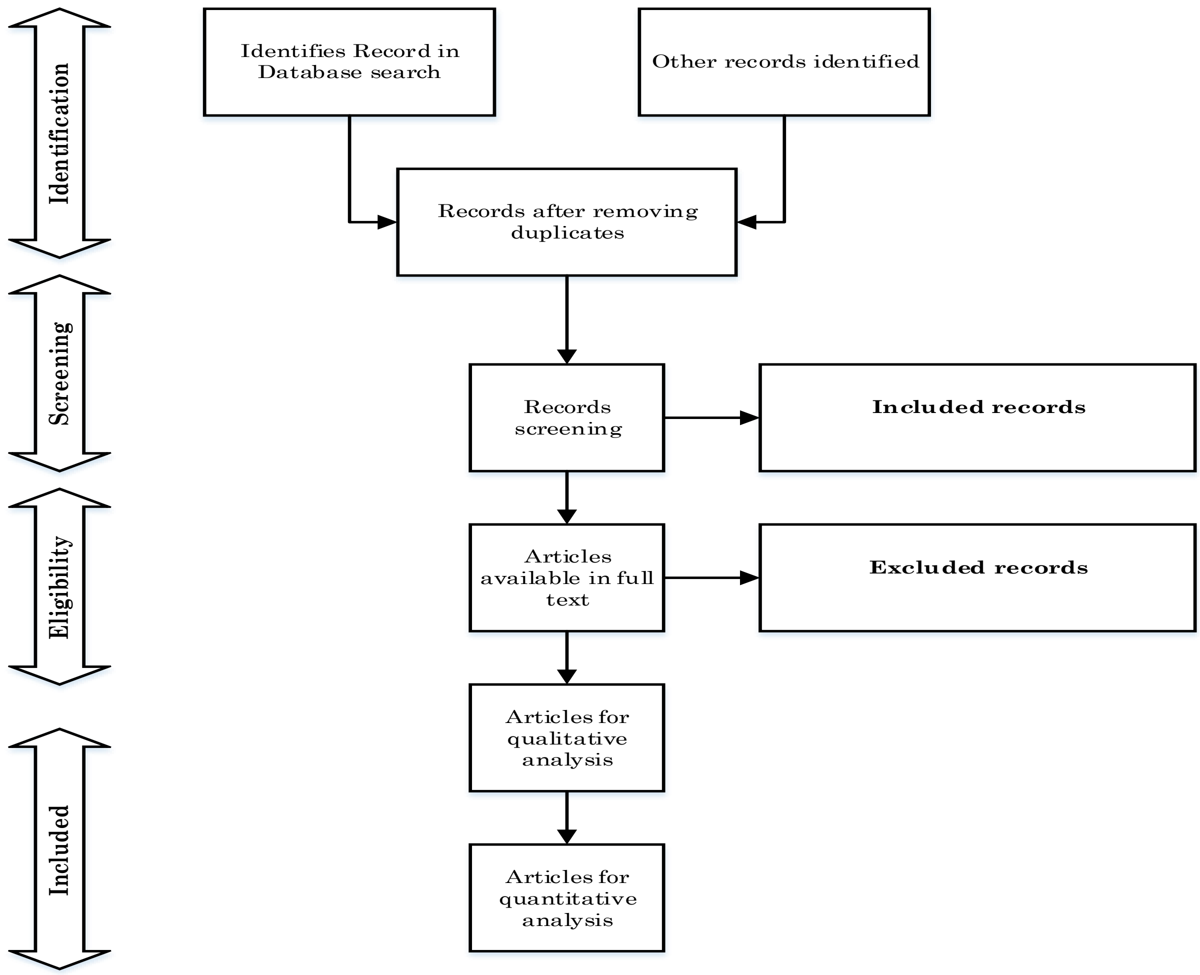

Figure 2.1 The main process used to conduct the systematic literature review.

Table 2.3 Database of sources used for searching academic literature.

N	Name of the Electronic Database
1.	Google Scholar
2.	ACM Digital Library
3.	Compendex
4.	IEEE Xplore
5.	ISI Web of Science
6.	Kluwer Online
7.	ScienceDirect- Elsevier
8.	SpringerLink
9.	Wiley Inter Science Journal Finder

2.6. Search Results and Study Selection

Based on applying the search protocol with all the search strings and the study selection process described in Section 2.5, the primary studies are selected. Figure 2.2 shows the process of primary study selection for data governance; the study selection is based on 4 stages and the number of papers identified at each stage is shown in this figure. Stage 1 identified 7800 sources from different databases, based on a pilot search. Stage 2 analysed those 7800 sources based on their titles, and this stage identified 476 articles. At the next stage, a total of 383 articles was excluded, and at stage 4 duplicate papers were also removed from the study, leaving 52 papers for the final review.

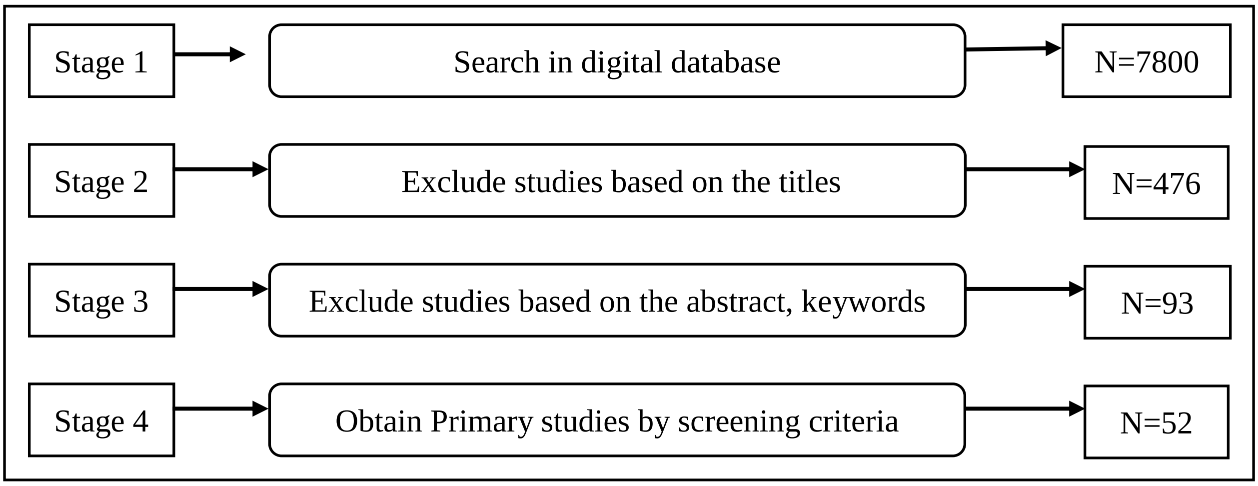

Figure 2.2 The selection process for the primary studies for data governance

In terms of the study selection process, this study collected the following data from each article: format type, name of source, data of publication, author(s), title of source and source outlines (see Table 2.4).

Table 2.4 Categorisation of 52 records on data governance from the defined search protocol

Nature of Contribution	Format	Reference
Academic	Papers in journals and conference proceedings, books, working reports and theses.	*Non-cloud:* (Weber et al., 2009),(Fu et al., 2011),(Prasetyo & Surendro, 2015),(Buffenoir & Bourdon, 2012),(Otto, 2011),(Badrakhan, 2010),(Wende, 2007),(Weber et al., 2008),(Rifaie et al., 2009) (Panian, 2010),(Neff et al., 2013),(Loshin, 2010),(Allen et al., 2014),(Sandra Nunn, 2009),(Imhanwa et al., 2013), (Ladley, 2012),(Seiner, 2014),(Bhansali, 2014),(Sarsfield, 2009),(Reeves & Bowen, 2013),(Niemi, 2011),(Pennanen, 2014),(Ndamase, 2014),(Poor, 2011),(Nwabude et al., 2014),(Fruehauf et al., 2015),(Hallikas, 2015),(Alhassan et al., 2016),(Koltay, 2016),(Olaitan et al., 2016),(Benfeldt, 2017),(Lee et al., 2017) *Cloud Computing:* (Felici et al., 2013), (Groß & Schill, 2012), (Wendy., 2011),(Tountopoulos et al., 2014),(Rimal et al., 2011)
Practice oriented	Publications by industry associations, software vendors and analysts	*Non-cloud:* (Guillory, 2008), (HIMSS), 2015), (Mustimuhw Information Solutions Inc., 2015), (Rausch et al., 2013),(Russom, 2008), Brett (2010), (Thomas, 2009), (Australian Institute of Health and Welfare, 2014), (Loshin, 2010),(Adler, 2007), (Office, 2013),(Kunzinger et al., 2010). *Cloud Computing:* (Mary et al., 2011),(Cloud Security Alliance, 2012), (Javier Salido, 2010), (Hunter, 2015), (Salido et al., 2010), (Solutions, 2013).

2.7. Results and Analysis

This section presents and analyses the systematic review results based on the systematic review objectives. Fifty-two studies on data governance were identified based on a selection of primary study processes that covered different study areas, such as surveys, industry experience reports, case studies, data governance frameworks, data governance maturity models, etc. Based on this process, each study was reviewed by analysing its context and research questions; thus, the studies cover a range of research topics within the data governance area. In addition, this study reviewed all eligible sources in academic and practice-oriented literature during the period from 2000 to 2017. The studies were categorised into the following main groups:

- ***State of the art of data governance for non-cloud computing.***
- ***State of the art of data governance for cloud computing.***

Based on the main categories mentioned above, the results will be described in relation to publication year and nature of contribution (academic and practice oriented). These results are briefly explained in the following:

2.7.1. Publication Year

Table 2.5 shows the number of articles published on data governance for non-cloud computing in each year during the period 2000-2017. Out of 52 records, the total number of studies on data governance for non-cloud computing were 41 records (78.85%). Based on the search protocol and the study selection process, the first interesting article on data governance was published in 2005. The highest number of papers was published in 2009 and 2014 (17.07% each year), followed by 12.20% in 2015. Table 2.6 shows the distribution of these records.

Table 2.5 The distribution of sources over the studied years for data governance for non-cloud computing

Years	N	%
2005	1	2.44
2006	0	0
2007	2	4.88
2008	3	7.32
2009	7	17.07
2010	3	7.32

Years	N	%
2011	3	7.32
2012	3	7.32
2013	2	4.88
2014	7	17.07
2015	5	12.20
2016	3	7.32
2017	2	4.88

Table 2.6 shows the number of articles published on data governance for cloud computing in each year during 2007-2017. Out of 52 records, the total number of studies on data governance for cloud computing were 11 records (21.15%). The highest number of papers were published in 2011 (n=3), follow by 2010, 2012 and 2013 (n=2 each year). In addition, the results show that the other two articles were published in 2014 and 2015, one article for each year. Table 2.6 shows the distribution of these records.

Table 2.6 The distribution of sources over the studied years for data governance for cloud computing.

Year	2009	2010	2011	2012	2013	2014	2015
N	0	2	3	2	2	1	1
%	0	18.18	27.27	18.18	18.18	9.09	9.09

Based on the results above, Figure 2.3 shows the number of studies across the years.

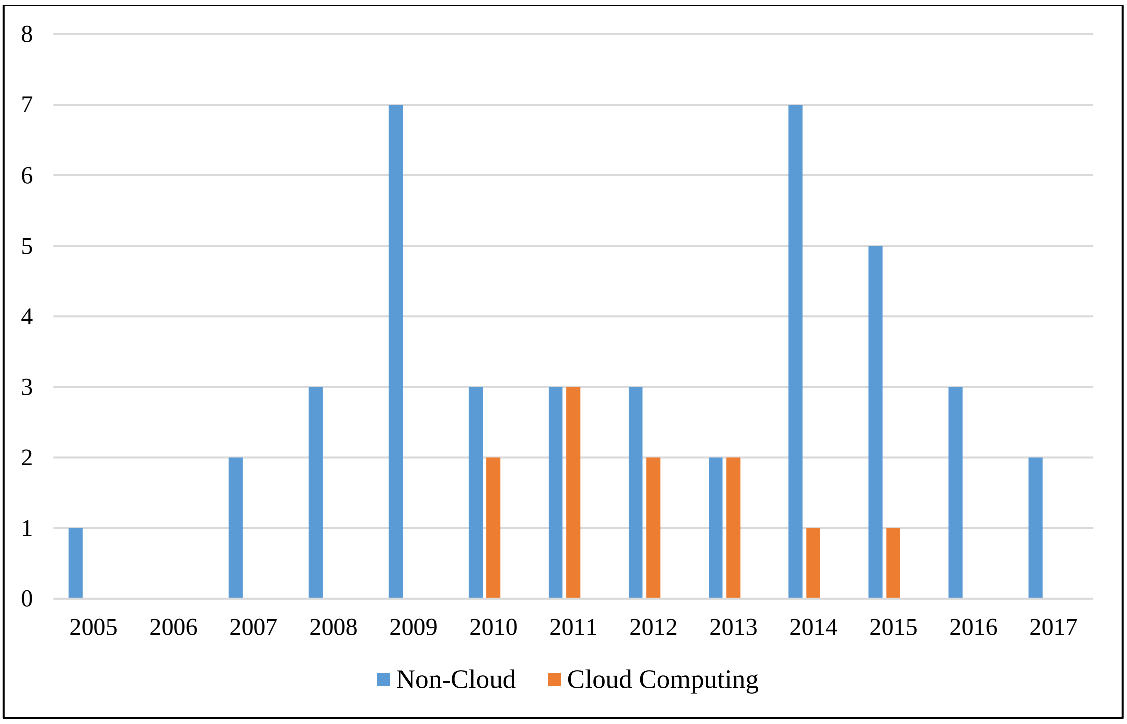

Figure 2.3 Number of studies across the years

2.7.2. Nature of Contribution

Table 2.7 shows the number of articles published on data governance for non-cloud computing in relation to the nature of contribution (academic and practice oriented) during the period 2000-2017. Out of 41 records, the total number of studies on data governance for non-cloud computing published by practice-oriented researchers was 26.83% (n=11), while 73.17% (n=30) were published by academic researchers.

Table 2.7 Number of studies of data governance for non-cloud computing based on nature of contribution

Years	Academic	Practice-Oriented
2005	1	0
2006	0	0
2007	1	1
2008	1	2
2009	6	1
2010	2	1
2011	3	0
2012	3	0
2013	0	2
2014	5	2
2015	3	2
2016	3	0
2017	2	0

Table 2.8 shows the number of articles published on data governance for cloud computing in relation to the nature of contribution (academic and practice oriented) during the period 2007-2017. Out of 11 records, the total number of studies on data governance for cloud computing which were published by practice-oriented researchers was 54.55% (n=6), while 45.45% (n=5) were published by academic researchers.

Table 2.8 Number of studies of data governance for cloud computing based on nature of contribution

Year	2010	2011	2012	2013	2014	2015	2016	2017
Academic	0	2	1	1	1	0	0	0
Practice oriented	2	1	1	1	0	1	0	0

Based on the results above, Figure 2.4 shows the number of studies across the years.

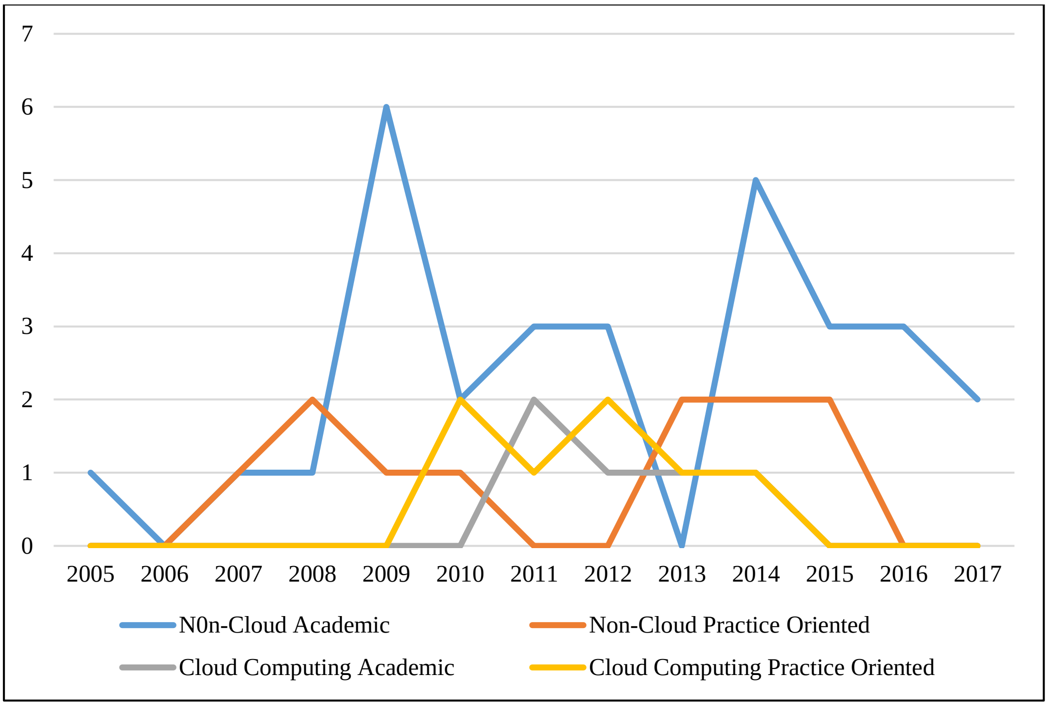

Figure 2.4 Number of study based on nature of contribution.

2.7.3. Analysis of the State of the Art for Data Governance for Non-Cloud Computing

According to the review protocol described in Section 2.6.4, the search results identified 41 records addressing the area of data governance in non-cloud computing, 30 scientific records and 11 practice-oriented records. Table 2.9 gathers together all these records and describes the main finding of each one.

Table 2.9 The main finding of each record

Study Name	Author(s)	Main Conclusion
One size does not fit all – a contingency approach to data governance	Weber et al. (2009)	• A data governance contingency model.
Data governance in predictive toxicology: a review	Fu et al. (2011)	• Reviews seven widely used predictive toxicology data sources and applications. • Focuses on their decision domains for data governance.

Study Name	Author(s)	Main Conclusion
Designing a data governance model based on soft system methodology (SSM) in organisations	Prasetyo & Surendro (2015)	• Designs a data governance model based on soft system methodology in organisations.
Reconciling complex organisations and data management: The Panopticon paradigm	Buffenoir & Bourdon (2012)	• Proposes a new scheme inspired by Foucauldian analysis of governmentality – the panopticon data governance paradigm.
Data governance and data sharing agreements for community-wide health information exchange: lessons from the beacon communities	Allen et al. (2014)	• The paper shares lessons learned based on the experiences of six federally funded communities participating in the beacon community cooperative agreement programme, • Offers guidance for navigating data governance issues and developing DSAs to facilitate community-wide health information exchange.
Driving compliance through data governance	Nunn (2009)	• Presenting brief principles about governance enterprise information and design data governance phase.
Organising data governance: findings from the telecommunications industry and consequences for large service providers	Otto (2011b)	• Presenting a case study on the organisation of data governance based on two of the largest companies from the telecommunications industry, namely BT and Deutsche Telekom.
Drive towards data governance	Badrakhan (2010)	• The article discusses the data governance strategy that companies need to ensure the quality of their corporate

Study Name	Author(s)	Main Conclusion
		data.
Designing data governance structure: an organisational perspective	Imhanwa et al. (2013)	• Focuses on the accountability aspect of data governance: the assignment of decision rights and responsibilities pertaining to data management.
Some practical experiences in data governance	Panian (2010)	• Offering the common business drivers and current market trends behind data governance. • The key data attributes and the components of an effective data governance practice. • Providing the data governance framework components.
A model for data governance organising accountabilities for data quality management	Wende (2007)	• Outlining a data governance model comprised of three components. • Data quality roles, decision areas and responsibilities to build a matrix, comparable to a RACI chart.
A morphology of the organisation of data governance	Otto (2011)	• Developing a morphology of data governance organisation on the basis of a comprehensive analysis of the state of the data governance both in science and in practice. • Six mini case studies are used to evaluate the morphology by means of empirical data.
Explicating performance impacts of IT governance and data governance in multi-	Neff et al. (2013)	• Analyses the performance impact of a combined IT and data governance concept.

Study Name	Author(s)	Main Conclusion
business organisations		• The framework is developed by using nine exploratory case studies in multi-business organisations.
Organising accountabilities for data quality management – a data governance case study	Weber et al. (2008)	• Examining a large organisation that has adopted an ad-hoc data governance model to manage its data. • It was found that DQM efforts were hampered mainly by the lack of clear roles and responsibilities and the lack of a mandate to carry out data quality improvement initiatives. • This research identifies a data governance structure with the emphasis on collaboration between business and IT to support organisations.
Data governance strategy: a key issue in building enterprise data warehouse	Rifaie et al. (2009)	• This paper articulates data governance as one of the key issues in building an Enterprise Data Warehouse.
Data governance (how to design, deploy, and sustain an effective data governance program)	Ladley (2012)	• This book aims to give the reader a brief outline about the deployment, implementation or maintenance of data governance programs.
Non-invasive data governance	Seiner (2014)	• This book aims to put the necessary components of data governance into place to help stockholders to deliver successful and sustainable data governance in their organisation.
Data governance (creating	Bhansali	• The goal of this book is to assist others who are on the journey to drive value

Study Name	Author(s)	Main Conclusion
value from information assets)	(2014)	from informational assets using data governance. • Book chapters present how ideas have been adapted as techniques and policies for practice in organisations on their journey to successful data governance. • The case studies in this book are from the healthcare and financial sectors.
Data governance imperative	Sarsfield (2009)	• This book aims to present a business strategy for corporate data. • This book presents a data governance definition. It defines generic data governance success factors and discusses technologies that support data governance. • Presenting a case study about data governance and data quality improvement focusing on British Telecommunications (BT).
Developing a data governance model in health car	Reeves MG1 (2013)	• Presents some important suggestions when building a data governance model in health care.
Designing a data governance framework	Niemi (2011)	• This paper looks at existing literature and the current state of data governance. • The authors found out that there is only a limited amount of existing scientific literature.
Data governance intelligent way of managing data	Pennanen (2014)	• Data governance issues and advantages from the business point of view.

Study Name	Author(s)	Main Conclusion
The impact of data governance on corporate performance: The case of a Petroleum Company	Ndamase (2014)	• Aiming to identify the factors influencing data governance in a petroleum firm and the significance of these influencing factors collectively. • Determining the extent to which data governance influences corporate performance.
Applying aspects of data governance from the Private sector to Public Higher Education	Poor (2011)	• The goal of this research is to present a collage of selected data governance practices within the private business sector for consideration by individuals in public higher education who promote and support data quality initiatives.
Data governance in small businesses – why small business framework should be different	Nwabude et al. (2014)	• The study looks at data governance in small businesses and investigates why data governance frameworks in small businesses should be different to those in larger organisations.
Using Bolman and Deal's four frames in developing a data governance strategy	Fruehauf et al. (2015)	• The study offers a review of relevant literature to examine how the Bolman and Deal model can be used in existing data governance framework development models to enhance their effectiveness.
Data governance and automated marketing – A case study of expected benefits of organising data governance in an ICT company	Hallikas (2015)	• The study seeks to find out what benefits employees expect the organisation of data governance to bring to an organisation and how it benefits the implementation of automated marketing capabilities.

Study Name	Author(s)	Main Conclusion
Data governance activities: an analysis of the literature	Alhassan et al. (2016)	• An analysis of the literature of data governance activities.
Data governance, data literacy and the management of data quality	Koltay (2016)	• The study aims to review data governance, data literacy and the management of data quality.
Taxonomy of literature to justify data governance as a prerequisite for information governance	(Olaitan et al., 2016)	• The study aims to produce a taxonomy of literature to justify data governance as a prerequisite for information governance.
A Comprehensive Review of Data Governance Literature	Benfeldt (2017)	• The study presents a comprehensive review of data governance literature.
Data governance for platform ecosystems: critical factors and the state of practice	Lee et al. (2017)	• The study identifies data governance factors for platform ecosystems through a literature review. • The study then surveys the data governance state of practice of four platform ecosystems: Facebook, YouTube, EBay and Uber. • Nineteen governance models in industry and academia are compared against the identified data governance factors for platform ecosystems to reveal the gaps and limitations.

Data governance is an emerging trend in enterprise information management (Kamioka et al., 2017). In the literature, a limited number of studies have discussed this important area. The roots of data governance research can be traced back to the early 1980s; however, the first efforts to propose a framework for data governance were published in 2007 (Niemi, 2011). Niemi (2011) also observed that all existing sources for data governance from researchers and practitioners, at the time he published his paper, focused on the placement of decision-making authority for Data Quality Management (DQM) and organisational structuring. Otto (2011) reported that organisations that believe they have a data governance programme in fact have not considered all the aspects required for these programmes to be complete and effective. This work was the only attempt in the literature to review the area of data governance, up until 2010. It aimed to develop a morphology of data governance organisation. Six mini case studies were used in this study to assess the morphology of the organisation of data governance. Other researchers, such as Wende (2007), suggested transferring knowledge to build IT governance into the development of data governance programmes. However,(Imhanwa et al., 2013) argued that organisations should establish a data governance structure to take responsibility for data out of the IT department. According to Prasetyo & Surendro (2015), similar to IT governance, data governance also needs to align with any organisation's business strategy. Wende and Otto (2007) argue that a data governance model helps organisations to structure and document the accountabilities for their data quality. Other authors have also related data governance to accountability, such as Wende (2007) and Imhanwa et al. (2013). In addition, Adelman (2008) stated that organisations must design a data governance model of role responsibilities to identify people who have a level of accountability to define, produce and use the data in the organisation. Wende (2007) also outlined a data governance model, which comprised three components: data quality roles, decision areas and responsibilities. Data governance requires the participation and commitment of all IT staff, management and senior-level executives (Kamioka et al., 2017).

Fu et al. (2011) reported the absence of data governance frameworks. They argued that an effective data governance framework can help organisations to create a clear mission, achieve clarity, increase confidence in using the organisational data, establish accountabilities, maintain scope and focus, and define measurable success criteria. In support of Fu et al.'s argument, other authors added that a good data governance framework supports compliance and legal efforts over the long term by organising data for retrieval and retention as well as building better relationships with customers and partners, which enhance income opportunities (Moseley, 2008; Panian, 2010; Otto, 2011). Rifaie et al. (2009) recommended the implementation of the Enterprise Data Warehouse, in order to achieve an effective data governance framework, which should be based on structure, process and communication. Despite the repeated calls by researchers for data governance frameworks, this study shows only a handful of them, mainly developed by industry associations such as DAMA, DGI and IBM (Adler, 2007; Poor, 2011b; Niemi, 2011; Prasetyo & Surendro, 2015). In 2011, Otto proposed a framework for data governance, which consists of goals and structure. The goals are divided into formal IT, business and functional goals, while the structure is divided into the focus of control, organisational form, and roles and committees. According to DGI, the development of a data governance framework is a complex task. The framework could be formed of various related items, including programmes, stages, decision domain, universal objects and components. DGI divides their framework activities (see Figure 2.5) into three components, namely rules & roles, people & organisations, and processes (Thomas, 2006; Prasetyo & Surendro, 2015). In addition, IBM's approach to data governance was built from the perspective of the vendor's data governance software provider, so establishing a data governance that will require software support (Ibm, 2007; Prasetyo & Surendro, 2015). This model shows that organisations need to ensure that the business and IT problems are clearly defined (Prasetyo & Surendro, 2015). The IBM model includes 14 elements, 10 of which are required and four of which are optional (See Figure 2.6) (Ibm, 2007; Soares, 2012; Prasetyo & Surendro, 2015).

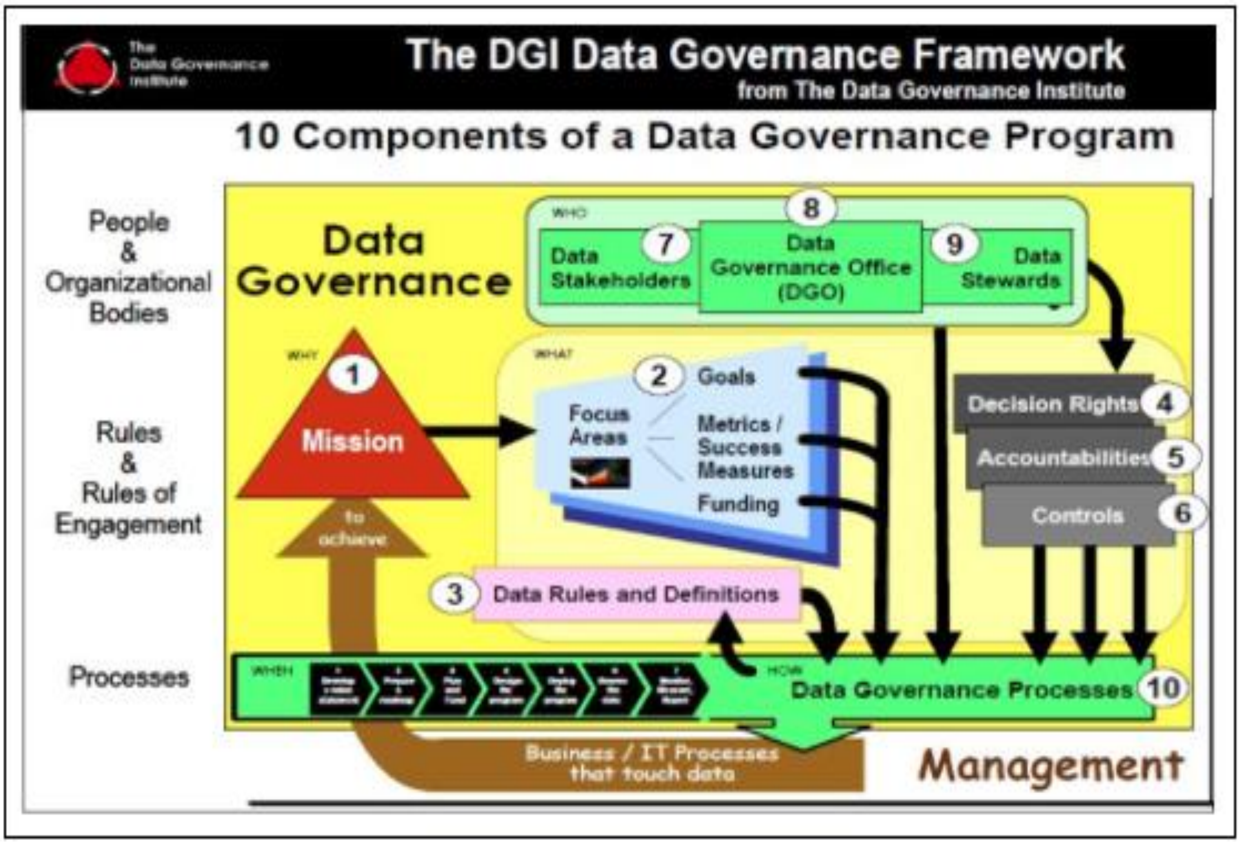

Figure 2.5 DGI Framework of Data Governance. Source: (Thomas, 2006)

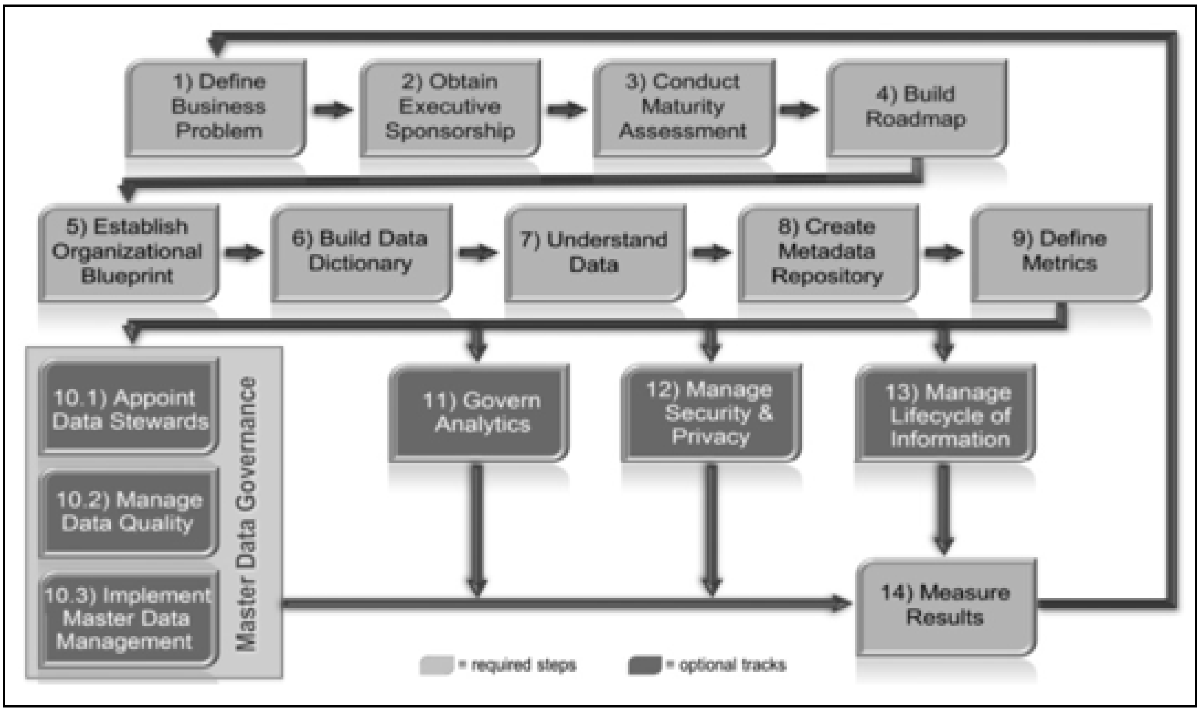

Figure 2.6 IBM data governance unified process. Source: (Soares, 2012)

Begg and Caira (2012) focused on defining CSFs for effective data governance, which they categorised into organisational and technological success factors. The organisational factors include the clear definition of roles and responsibilities, business and IT involvement, executive sponsorship and the integration of a competency centre. The technological factors include the automation of a data integration life cycle to deliver on the goals of data governance. Cheong & Chang, (2007) also identified some critical data governance success factors including strategic accountability, standards, managerial blind spots, embracing data complexities, cross-divisional issue, data quality metrics, partnership with other companies, strategic points of control, training and awareness of data stakeholders, and compliance monitoring.

Successful data governance, therefore, requires bringing together a diverse number of experts from various departments in any one organisation to achieve consistency, transparency and repeatability of processes. This in turn enables the best data-related decision making (Power & Street, 2013), establishes accountabilities, maintains scope and focus, and defines measurable successes (Begg & Caira, 2012). It also supports compliance and legal efforts over the long term by organising data for retrieval and retention (De Hert & Papakonstantinou, 2013), and improves income opportunities and customer and partner relationships (Weber et al., 2009). Table 2.10 summarises the CSFs for implementing effective data governance, as reported in the literature for non-cloud computing, and developed as a result of the aforementioned systematic literature review.

Table 2.10 The most important CSFs to implement data governance as extracted from the literature

N	Factors	Reference	Description
1.	Establish data governance structure	Wende & Otto (2007), Wende (2007a), Rifaie et al. (2009), Otto (2011b), Traulsen & Tröbs (2011), Ladley (2012), Neff et al. (2013)	• Data governance structure should consist of the best people in the organisation who are specialists and are most skilled in the data governance aspects.
2.	Define roles and responsibilities	Wende & Otto (2007), Wende (2007a), Otto (2011b), Traulsen & Tröbs (2011), Ladley (2012)	• Define data governance roles and responsibilities in the data governance team to delegate the correct data governance jobs to the right people in the organisation so that tasks are carried out correctly.
3.	Develop processes, procedures guideline, principles, policies and standards to support data governance	Wende & Otto (2007), Cheong & Chang (2007a), Wende (2007a), Rifaie et al. (2009), Otto (2011b), Ladley (2012), Neff et al. (2013)	• A clearly defined process for identifying and regulating data governance policies and procedures and guidelines to implement data governance in the organisation and to achieve data governance objectives.
4.	Develop communication plan	Rifaie et al. (2009), Ladley (2012)	• Sharing information, activities, tasks, scope and objectives between the data governance members and communication of the results at each data governance

N	Factors	Reference	Description
			implementation stage to the data governance office and to top management in the organisation.
5.	Monitor tool and measure metrics	Wende & Otto (2007), Cheong & Chang (2007), Ladley (2012)	• Establish a tool to monitor data governance performance in the organisation, and create matrices to measure data governance performance in each stage of the data governance programme.
6.	Organisational	Wende & Otto (2007), Wende (2007a), Panian (2010), Otto (2011b), Traulsen & Tröbs (2011), Ladley (2012), Neff et al. (2013)	• Organisational refers to all organisational factors that influence data governance implementation, and that support data governance implementation.
7.	Technological	Traulsen & Tröbs (2011), Panian (2010), Ladley (2012)	• Technological refers to all technical factors and technology sources that influence data governance implementation, and that support data governance implementation.
8.	Accountability	Wende & Otto (2007), Wende (2007a), Traulsen & Tröbs (2011), Cheong & Chang (2007a)	• An accountability approach that focuses on setting data governance goals for organisations based on criteria established in current data governance policy, and allowing organisations discretion to determine how those goals are met.

N	Factors	Reference	Description
9.	Training and education	Cheong & Chang (2007a), Ladley (2012)	• Deliver data governance training, education and awareness events for organisational staff.
10.	Awareness of data stakeholders	Traulsen & Tröbs (2011),(Salido et al., 2010)	• Deliver data governance awareness events for organisational staff about the importance of data and its risks.
11.	Compliance monitoring	Wende (2007), Traulsen & Tröbs (2011), (Salido et al., 2010)	• Continuous process of obtaining information to determine if the parties required by law to control their data governance are doing so.
12.	Environmental	Wende & Otto (2007), Wende (2007), (Salido et al., 2010)	• Environmental refers to external environmental factors such as government legislation and data protection acts. The data governance teams have to consider environmental factors when designing data governance functions. This means the data governance functions have to comply with this factor.
13.	Develop Integration process	Panian (2010), Traulsen & Tröbs (2011), (Salido et al., 2010)	• Good integration process between data governance programmes and other programmes in the organisation, and a good integration process to share and transfer information.
14.	Organisational culture change	Traulsen & Tröbs (2011), (Salido et al., 2010)	• Use organisational culture change to bring the required change to the core culture of the organisation to

N	Factors	Reference	Description
			meet data governance objectives.
15.	Develop change management plan	Wende (2007), Traulsen & Tröbs (2011), (Salido et al., 2010)	• An initial strategy and strong institutional identity are needed to ensure the successful implementation of data governance. Changes in the work process are required to fit with the data governance process in the organisation.
16.	Develop business case for data governance	Wende (2007), Otto (2011), (Salido et al., 2010), Neff et al., (2013)	• The business case can be defined as "a formal document that summarises the costs, benefits and impact of an investment". The main activities in this task are finding and exploring opportunities that return to the organisation from data governance implementation, and definitions of relevant terms such as data governance vision and mission, cost of data governance, and benefits and risk.
17.	Assess data governance situation	Traulsen & Tröbs (2011), Wende (2007), (Loshion, 2007)	• To implement effective data governance in an organisation, the current data governance situation needs to be assessed before the new/revised system is implemented.
18.	Aligning data governance with the overall organisation	Wende & Otto (2007),(Fu et al., 2011), (Salido et al., 2010)	• Alignment means linking of organisational goals with the data governance goals, which requires common understanding of the

N	Factors	Reference	Description
	context		purposes and goals of existing strategies in the organisation. The alignment will consider many strategies and factors that will help the organisation to achieve an effective data governance strategy.
19.	Define the sustaining requirements	(Salido et al., 2010)	• Define the sustaining requirements to ensure data governance continues, and improvement is possible to achieve its objectives.
20.	Data governance tools	Wende (2007), (Salido et al., 2010),	• Develop an automated tool for implementing data governance in the organisation, and for monitoring data governance performance.

2.7.4. Analysis of the State of the Art of Data Governance for Cloud Computing

To recap, one of the main impediments to the wider adoption of the cloud computing model has been linked primarily to aspects related to data governance (Groß & Schill, 2012; Mary et al., 2011). While security has been shown to be the most cited challenge to cloud adoption, Kim & Lee (2015) show that 41% of the security problems in the cloud are related to governance and legal issues. Cloud governance is a new term in the IT field, and it is still under-developed (Woldu, 2013; Saidah & Abdelbaki, 2014). Microsoft defines cloud governance as "*defining policies around managing the factors: availability, security, privacy, location of cloud services and compliance and tracking for enforcing the policies at run time when the applications are running*" (Woldu, 2013, p.13). Data governance is considered to be one of the most important aspects in cloud governance (Groß & Schill, 2012; Saidah & Abdelbaki, 2014). However, a data governance programme built for on-premises IT infrastructures cannot be deployed for a cloud infrastructure and service provisioning, which would require completely new requirements, design and implementation (Olaitan et al., 2016). Undoubtedly, the area of cloud data governance will become an important topic for the coming decades (De Hert & Papakonstantinou, 2013), although it is still under-researched by both academia and industry due to its novelty (Wende 2007; Begg & Caira 2012). As discussed in Chapter One, data governance is still under-developed and under-practised, even for traditional IT infrastructures, let alone for cloud computing environments. This section presents further analysis of the state of the art of data governance for cloud computing. The analysis is based on the results of the presented systematic review conducted for this purpose, which has identified only 11 records discussing data governance for cloud computing. Table 2.11 shows the main existing research contributions on data governance for cloud computing.

Table 2.11 Academic research on data governance for cloud computing

Study Name	Authors	Main Conclusion
Is data governance in cloud computing still a mirage or do we have a vision we can trust?	Yale (2011)	• Provides information about data governance and its issues in cloud computing. • Provides a list of some concerns related to data management and data protection in cloud computing.
Accountability for data governance in cloud ecosystems	Felici et al. (2013)	• Focuses mainly on the accountability aspect of cloud data governance. • In this paper, the authors propose a model that allows them to explain cloud data governance in terms of accountability attributes and cloud-mediated interactions between actors.
Interoperability analysis of accountable data governance in the cloud	Tountopoulos (2014)	• Presenting an accountability-based approach for cloud data governance, as a means of addressing interoperability requirements relating to the protection of personal and confidential data involved in complex service provision chains in the cloud.
Architectural requirements for cloud computing systems: an enterprise cloud	Rimal et al. (2011)	• This paper emphasises the importance of data governance for any enterprise cloud, especially when dealing with sensitive data.
Towards user-centric data governance and control in the cloud	Groß & Schill (2012)	• This paper advocates the users' role in managing their data in cloud environments.

Governance in the cloud requires the understanding, moderating and regulating of the relationships between different cloud actors or stakeholders in terms of roles and responsibilities (Badger et al., 2011). Data governance is meant to classify and assign responsibilities, communication, labelling and policies (Saidah & Abdelbaki, 2014). There are few studies reporting on data governance for cloud services. Almost all existing work on data governance for cloud computing focuses on accountability and interoperability (Catteddu et al., 2013; Tountopoulos et al., 2014). The research presented by Felici et al. (2013) which aim to proposed a model that explains data governance in terms of accountability attributes and cloud-mediated interactions between actors. According to these authors and others, it is accountability that identifies the relationships between cloud actors in terms of data governance; it also enhances trust between cloud actors (F et al., 2013; Toney & Kadam, 2013).

Accountability could be addressed at different levels – technological, regulatory and organisational (Pearson et al., 2012). Felici et al. (2013,p.4) define accountability as consisting of: *"defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly*". As a result, accountability is only one aspect of cloud data governance; therefore, it is not quite enough to achieve cloud data governance goals. Cloud data governance needs more input from academic researchers to design a data governance strategy or programme to cover all its aspects.

Cloud data governance has also been overlooked by industry. According to various authors (Mary et al., 2011; Cloud Security Alliance, 2015; Hunter, 2015), the Cloud Security Alliance, Trustworthy Computing Group, and Microsoft Corporation are regarded as the recognised leaders in this area. The cloud data governance working group in Cloud Security Alliance currently focuses on the data protection aspect, with the aim of proposing a data governance framework for ensuring the availability, integrity, privacy and overall security of data in different cloud models; however, this is far from being realised (Cloud Security Alliance, 2015). The Trustworthy Computing Group and Microsoft Corporation describe the basic elements of a data governance initiative for privacy, confidentiality, and compliance, and provide guides to help organisations get started down this path (Salido et al., 2010).

According to a MeriTalk report in 2014, only 44% of IT professionals in the federal government believe their agencies have mature data governance practices in the cloud. This report also suggests that around 56% of agencies are currently in the process of implementing data stewardship or data governance programmes (Alexandria, 2014). As a result, the work provided by industry regarding cloud data governance is not quite enough to achieve cloud data governance goals, and to provide good solutions for decision makers in the organisations so that they can understand the important processes required to achieve governance for their data in the cloud environment.

2.7.5. Analysis Barriers to Cloud Data Governance Implementation

In the literature, scholars have argued that, in spite of the many benefits that can be accrued through data governance implementation in organisations, there are difficulties in implementing data governance because barriers are deeply embedded in organisations' cultural, technical, economic and political principles and values. Prinzo (2012) classifies the data governance barriers as technological, organisational, legal, financial and relating to policy and knowledge. However, a number of researchers have recognised the need to design a data governance framework for cloud computing(Adelman, 2008; Hoying, 2011; Imhanwa et al., 2013). Designing and implementing data governance for cloud computing is potentially complex, and it will change according to the roles and responsibilities in the internal process of an organisation (Groß & Schill, 2012; Felici et al., 2013). The implementation of cloud data governance will face many issues that will influence the implementation decision in the organisation; thus, the decision maker should address these issues before implementing cloud data governance, thus decreasing the complexity. This section reviews the barriers identified in the data governance literature.

Based on a systematic review of data governance, the results show that few sources have addressed data governance in general and cloud data governance in particular. The results also show that there are currently no empirical studies specifically addressing the barriers to cloud data governance. In addition, most of the empirical studies in the literature investigate the barriers related to IT governance, information security governance and cloud computing individually (Abu Musa, 2009; Ataya, 2013; Alkhater et al., 2014). Based on these resources, this study investigates the barriers influencing the implementation of cloud data governance.

To extract the common barriers faced when implementing cloud data governance, this study analyses the different barriers, challenges and considerations related to data governance in general and cloud data governance in particular that have been discussed in the literature.

Therefore, these have been analysed and then classified into eight main barriers, each of which has similar definitions and barriers. Under each main barrier, there are sub-barriers or different explanations from different resources. In addition, some of the barriers have been mentioned in the same expression but in different meanings or contexts. Consequently, they have been dealt with based on their meanings or contexts.

The main barriers are the following: organisational barrier, technological barrier, environmental barrier, knowledge barrier, cultural barrier, human barrier, functional barrier and financial barrier. Figure 2.7 presents a summary of the most common barriers that can impact the implementation of cloud data governance as reported in the literature.

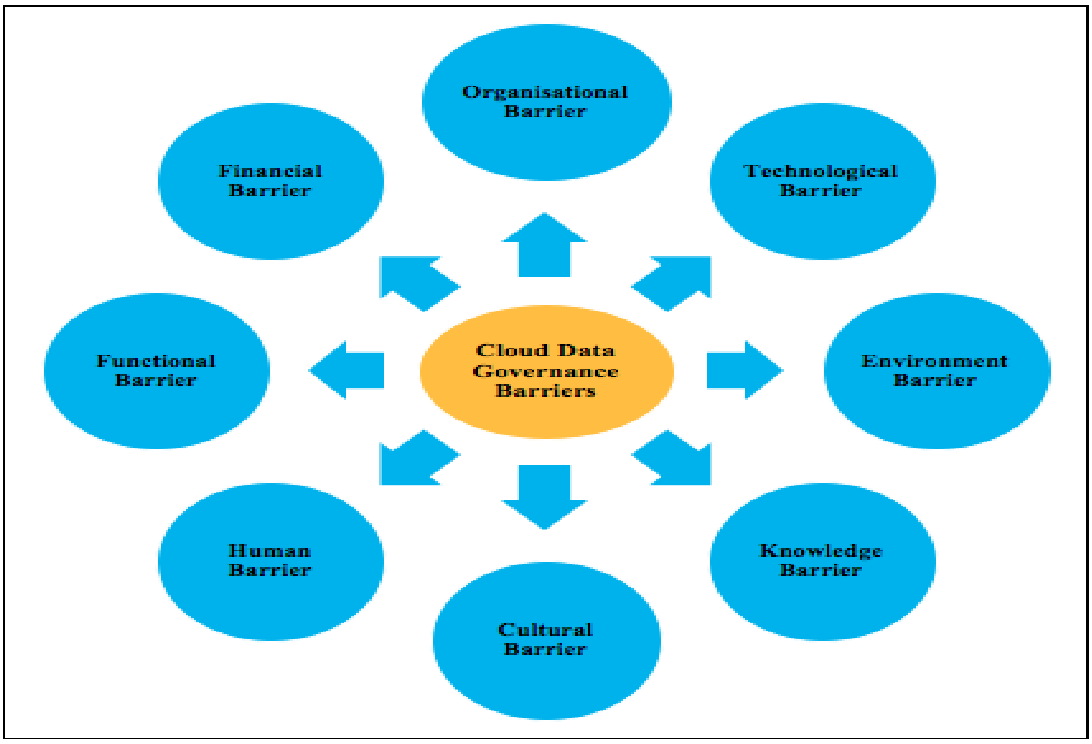

Figure 2.7 Classification of barriers to cloud data governance implementation

The main barriers are the following:

a) Organisational Barrier (OB)

The organisational barrier refers to organisational dimensions of effectiveness that form barriers to cloud data governance implementation in organisations. Based on our finding related to organisational barriers identified in the literature(Abu Musa, 2009; Prinzo, 2012; Alkhater et al., 2014), this study classifies organisational barriers into nine sub-barriers, as follows:

- A low priority given to cloud data governance compared to other projects.
- Inability to communicate the business value of cloud data governance.
- Lack of focus on cloud data governance charter, mission and vision within the organisation.
- Lack of focus on cloud data governance communication plan within the organisation.
- Lack of focus on cloud data governance change management plan within the organisation.
- Lack of a cloud data governance office within the organisation.
- Data is not considered as a strategic asset in cloud computing.
- Lack of time to implement cloud data governance.
- Cloud computing not quite adopted.

b) Technological Barrier (TB)

Technological barrier refers to the technical issues that will affect the decisions made with regard to cloud data governance implementation in organisations. This study classifies technological barrier into six sub-barriers that based on our findings are related to technological barriers identified in the literature(Poor, 2011b; Prinzo, 2012; Almarabeh et al., 2016). These are as follows:

- Cloud data governance is perceived as too complex.
- Lack of technology that is used to implement and monitor cloud data governance in organisations.
- Complexity of storage and processing data in the cloud.
- Complex cloud deployment models.
- Complex cloud service delivery models.
- Lack of simple mechanisms to assess the trustworthiness of potential partners.

c) Environmental Barrier (EB)

Environmental barrier refers to the legal issues that will affect the decisions made with regard to cloud data governance implementation in organisations. This study classifies environmental barriers into four sub-barriers that based on our findings are related to environmental barriers identified in the literature(Prinzo, 2012; Alsanea, 2015), as follows:

- Lack of compliance enforcement.
- Cloud data governance is not build into service level agreement of cloud computing with cloud provider.
- Compliance hazard.
- Lack of cloud regulation.

d) Functional Barrier

Functional barrier refers to the data governance function issues that will affect the decisions made with regard to cloud data governance implementation in organisations. This study classifies the functional barrier into four sub-barriers that based on our findings are related to functional barriers identified in the literature(Silic & Back, 2013; Self, 2014). These are as follows:

- Lack of focus on cloud data governance policies within organisations.
- Lack of focus on cloud data governance procedures within organisations.
- Lack of focus on cloud data governance processes within organisations.
- Lack of focus on defined roles and responsibilities for cloud actors.

e) Financial Barrier

Financial barrier refers to the finance issues that will affect the decisions made with regard to cloud data governance implementation in organisations. This study classifies the financial barrier into two sub-barriers that based on our findings are related to financial barriers identified in the literature(Alkhater et al., 2014; Olaitan, 2016). These are as follows:

- Lack of financial resources.
- Cost.

f) Cultural Barrier

Cultural barrier refers to the organisation's and decision maker's attitudes related to cultural issues that will affect the decisions made with regard to cloud data governance implementation in the organisation. This study classifies the cultural barrier into two sub-barriers that based on our findings are related to the cultural barriers identified in the literature(Silic & Back, 2013; Rebollo et al., 2014). These are as follows:

- Cloud data governance is not part of the organisational culture.
- Resistance to change.

g) Knowledge Barrier

Knowledge barrier refers to the organisation's knowledge issues that influence the successful implementation of cloud data governance in organisations. This study classifies the knowledge barrier into five sub-barriers that based on our findings are related to the knowledge barriers identified in the literature(Rifaie et al., 2009; Weber et al., 2009a; Akin, 2014). These are as follows:

- The organisations do not know where to start when they intend to implement cloud data governance.
- Lack of knowledge and understanding of cloud data governance within the organisation.
- Lack of training on cloud data governance programmes in the organisation.
- Lack of understanding of how to create a communication plan for cloud data governance in the organisation.
- Lack of understanding of how to build cloud data governance matrices and measures in the organisation.

h) Human Barrier

Human barrier refers to the organisation’s Human Resource (HR) issues that influence the successful implementation of cloud data governance in organisations. This study classifies the human barrier into three sub-barriers that based on our findings are related to the human barriers identified in the literature(Alkhater et al., 2014; Rebollo et al., 2014). These are as follows:

- Lack of people to support the implementation of cloud data governance.
- Lack of executives and stakeholders to support the implementation of cloud data governance.
- Lack of people who have skills and experience related to implementing cloud data governance in the organisation.

2.7.6. Analysis of Critical Success Factors for Cloud Data Governance Implementation

The CSF approach has been popularised by Rockart and other researchers and is now being increasingly used by IS departments, and by consultants, as an aid to IS strategic planning (Amberg et al., 2005). This approach has been applied in case studies carried out in UK universities (Forster & Rockart, 1989) to determine the organisational information needs of heads of departments. According to Williams & Ramaprasad (1996, p.252), they state that "*there is a great deal of attention devoted to the concept in the IS literature as many argue that the use of CSF can have a major impact on the design, development, and implementation of I*S".

In the literature, there are several definitions of CSFs; for example, Forster and Rockart (1989) reported that "*the critical success factors are areas of activity that should receive constant and careful attention from management*"(Forster & Rockart, 1989, p.23). Pinto and Slevin (1987) defined CSFs as "*factors which, if addressed, [would] significantly improve project implementation chances*" (Müller & Jugdev, 2012, p.758). The purpose of the CSF approach is "*the determination of the set of factors that the manager considers critical for his or her success, once identified, these factors are stated as his or her objectives and the information required to monitor their performance is then identified*"(Forster & Rockart, 1989, p.25). Therefore, the complexity of a cloud data governance programme means that success in its implementation requires reference to a solid methodical foundation and proven scientific theories. It seems that the concept of CSFs provides a good basis for stating what criteria should be followed during the implementation of a cloud data governance programme (Amberg et al., 2005).

With regard to cloud data governance, the CSFs refer to the important factors that are considered to be critical for the implementation of the cloud data governance programme. The results of the systematic review of data governance show that in the literature many authors have published a list of CSFs in relation to the implementation of data governance programmes in organisations. Table 2.11 above has summarised the most common and most important CSFs that have been identified by various authors. Some authors have also mentioned important requirements that need to be fulfilled in order to achieve successful data governance in the cloud environment (Mary et al., 2011; Smitha et al., 2012; Felici et al., 2013).

Thus, to extract the common CSFs for implementing cloud data governance, the study analyses the different factors and considerations related to data governance in general and cloud data governance in particular that have been discussed in the literature. These have therefore been analysed and classified into eight main factors, each of which has similar definitions and factors. Under each main factor, there are sub-factors or different explanations from different resources. In addition, some of the factors have been mentioned in the same expression but in different meanings or contexts. Consequently, they have been dealt with based on their meanings or contexts. Figure 2.8 presents a summary of the most common CSFs that, as reported in the literature, are important for implementing cloud data governance.

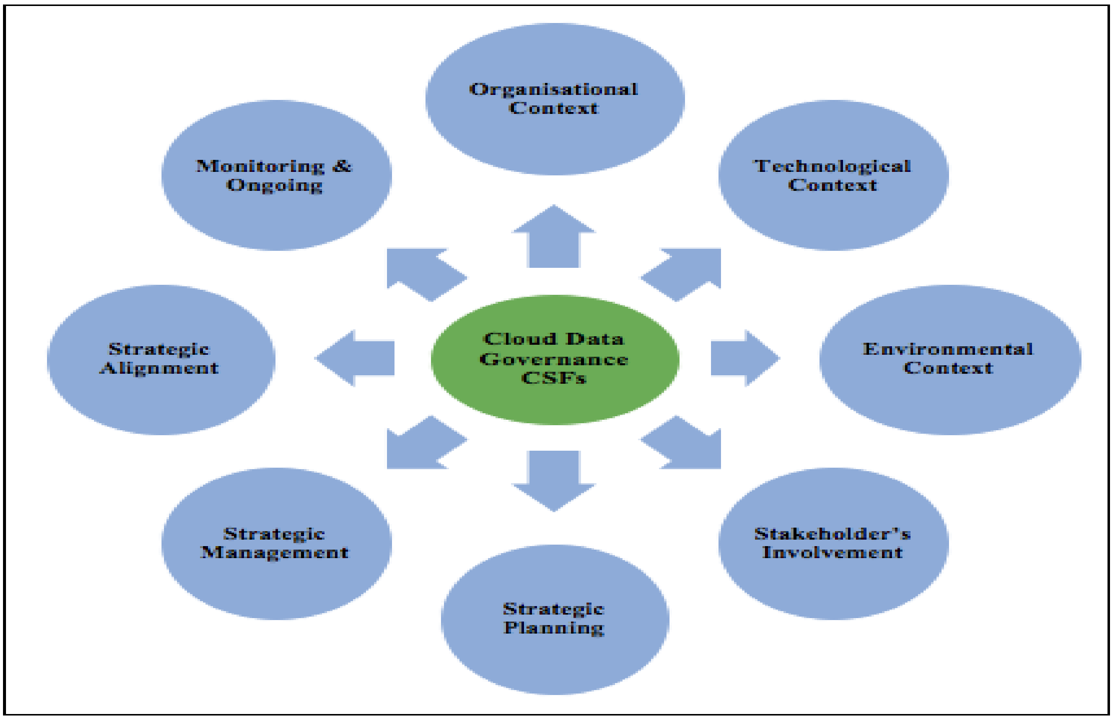

Figure 2.8 Classification of CSFs for cloud data governance implementation

The main factors are the following:

a) Organisational Context

Cloud computing supports organisations to embrace new business opportunities, improve their current business performance, respond to crisis situations and change their current business model (Rajendran, 2013; Alkhater et al., 2014). In addition, the data governance strategy is essential for supporting business functions in any organisation (Begg & Caira, 2012). The literature review has identified a significant gap in the research related to appropriate and effective data governance in the cloud. Organisations need to embrace a data governance programme in the cloud, and organisational factors are important for data governance to be successful. The systematic literature review demonstrates that there are many organisational factors that affect an organisation's implementation of data governance and cloud data governance. This study classifies the organisational factors into six sub-factors:

- Setting up a clear cloud data governance office structure.
- Ongoing funding for cloud data governance requirements.
- Improving staff's skills and experience in relation to cloud data governance.
- Providing top management support for cloud data governance implementation.
- Following the principle of corporate governance.
- Providing leadership and commitment of top management for the adoption of a risk management strategy for the organisation.

b) Technological Context

Technology is also a key element for data governance success (Fleissner et al., 2014). Therefore, a lack of adequate technology is considered to be a common barrier to successful data governance. Technical factors encapsulate data management issues that affect organisations' strategies such as security, privacy, quality and integrity (Traulsen & Tröbs, 2011; Ladley, 2012). As such, it is incumbent upon organisations that anticipate the implementation of data governance to assess all technological characteristics available to them in order to effectively implement data governance. However, a recent development in technology is the emergence of cloud computing. It is suggested that there are many factors acting as barriers to cloud computing, and that a majority of these involve concerns over moving business data to the cloud, where it is handled by a third party (Mary et al., 2011). Central to these concerns is the loss of control of data, data security and privacy, data quality and assurance, data stewardship, etc. The cloud computing model is discussed as a highly disruptive technology, with the adoption of its services requiring extremely rigorous data governance strategies and programmes, which although necessary can be complex. Therefore, it is important to integrate the technological factors in cloud computing with data governance functions for successful cloud data governance implementation. There is little research reported in the literature about the technological factors that affect an organisation's implementation of cloud data governance (Mary et al., 2011; Smitha et al., 2012; Felici et al., 2013). This study classifies the technological factor into four sub-factors:

- Integrating data governance functions with cloud deployment model features.
- Integrating data governance functions with cloud service delivery model features.
- Assessing and managing data risks in cloud computing on time.
- Automating cloud data governance.

c) Environmental Context

Environmental factors refer to external environmental considerations such as government legislation and data protection acts (Alkhater et al., 2014). Legal contracts written between cloud actors are expressed in very complicated statements. Hence, customers find it very difficult to understand the legal and regulatory implications of such agreements (Dogo et al., 2013). The legal framework for cloud computing still remains at an unsatisfactory level in many countries (Maaref, 2012). For example, Middle Eastern countries and Africa lack compulsory regulatory support for data protection, governance and privacy (Dogo et al., 2013; MCIT, 2014). Organisations should be considering all environmental aspects when designing cloud data governance functions; this means that cloud data governance functions have to comply with the environment. In the literature, there are many reported environmental factors that affect an organisation when implementing data governance in the cloud (Mary et al., 2011; Felici et al., 2013; Alkhater et al., 2014). This study classifies the environmental factor into three sub-factors:

- Building cloud data governance into the service level agreement of the cloud computing project.
- Supporting a compliance enforcement to implement cloud data governance.
- Providing a regulatory environment and compliance requirements to support cloud data governance implementation.

d) Stakeholders' Involvement

Organisations are embracing stakeholder management in their strategic operations in order to gain a competitive advantage in business (Edelenbos & Klijn, 2006). Stakeholders have become an integral part of an organisation's strategy in their different capacities as shareholders, customers, staff, government agents, the general public, suppliers and business partners. Therefore, stakeholder involvement raises the chances of the provision of better services and products that are more customer oriented (Edelenbos & Klijn, 2006). In the literature, some research suggests that stakeholders' involvement in the data governance strategy is important for the success of data governance initiatives in organisations (Weber et al., 2009; Begg & Caira, 2012). With regard to cloud data governance, cloud actors are one of the most important stakeholders who have to be considered in the cloud data governance strategy (Bumpus, 2010). The term ‘cloud actors’ refers to a person or an organisation that participates in processes or in a transaction, and/or performs tasks in the cloud computing environment. The NIST cloud computing reference architecture distinguishes five major actors: the cloud consumer, the cloud provider, the cloud auditor, the cloud carrier and the cloud broker (Mell & Grance, 2011). All of the aforementioned have special roles and responsibilities in the cloud, so the data governance teams must clearly define the roles and responsibilities for all cloud actors. Based on the literature, this study classifies the stakeholder involvement factor into three sub-factors:

- Involvement of board of directors and top management support and ownership to support the implementation of cloud data governance.
- Involvement of the cloud provider in cloud data governance.
- Involvement of other cloud actors in cloud data governance (cloud broker, cloud auditor, cloud carrier).

e) Strategic Planning

Strategic planning is considered to be a useful tool to help manage the enterprise, especially if the strategy and strategic plans can be successfully deployed throughout the organisation (Gates, 2010). The strategic planning factor refers to the preparation for the implementation of cloud data governance, which is a critical factor that requires attention before implementation commences. As with any project implementation, there are many strategic planning factors that should be addressed to ensure that the whole organisation is ready for the cloud data governance project. In addition, this factor aims to set up the cloud data governance requirements and plan, which are important for the implementation of cloud data governance in the organisation. The literature reports that strategic planning is important for the success of data governance initiatives in organisations (Wende & Otto, 2007; Otto, 2011; Imhanwa et al., 2013). Based on the findings related to strategic planning factors identified in the literature, this study classifies the strategic planning factor into seven sub-factors:

- Analysing and evaluating current cloud data governance.

- Identifying and articulating priorities to implement cloud data.
- Setting up clear cloud data governance mission and vision.
- Setting up clear communication plan.
- Setting up clear change management plan to implement cloud data governance.
- Defining data values.
- Classifying data in the cloud.

f) Strategic Management

Strategic management is a systems approach to identifying and making necessary changes and measuring the organisation's performance as it moves towards its vision (Macnair, 2010). Strategic management goes beyond the development of a strategic plan, as it includes the pre-planning and strategic planning processes (Gates, 2010). Strategic management is the deployment and implementation of the strategic plan and the measurement and evaluation of the results. Deployment involves completing the plan and communicating it to all employees. Implementation involves resourcing the plan, putting it into action and managing those actions. In the literature, some research suggests that strategic management in a data governance strategy is important for the success of the data governance initiatives in organisations (Kunzinger et al., 2010; Otto, 2011; Begg & Caira, 2012; Felici et al., 2013). Therefore, with a cloud data governance strategy, the strategic management factor should be involved when putting it into action and managing those actions. Based on the literature, this study classifies the strategic management factor into seven sub-factors:

- Setting up clear cloud data governance policies.
- Setting up clear cloud data governance procedures.
- Setting up clear cloud data governance processes.
- Defining clear roles and responsibilities for cloud actors.
- Creating a strong cloud data governance methodology.
- Regularly communicating with all cloud data governance participants.
- Creating a clear risk management strategy.

g) Strategic Alignment

It is important to confirm that the data governance strategy is part of the organisation's strategy and it must follow the organisation strategy and be aligned with the other strategies in the organisation (Wende & Otto, 2007; Chao, 2012). Prioritisation is the core business for any organisation; this consideration will help to align the data governance strategy with the business priorities (Kunzinger et al., 2010). Therefore, the alignment between data governance and other strategies in the organisations is one of most important factors when implementing cloud data governance. This factor will give cloud consumers the ability to measure their success in managing data governance (Ladley, 2012). A sound cloud data governance strategy should be aligned with many contexts to address data issues in the cloud environment. In the literature, many strategic alignment factors are reported as affecting an organisation's implementation of data governance and cloud data governance (Wende & Otto, 2007; Otto, 2011; Ladley, 2012). This study classifies the strategic alignment factor into eight sub-factors:

- Effective alignment with cloud computing regulations.
- Effective alignment with organisation strategy.
- Effective alignment with business strategy.
- Effective alignment with IT strategy.
- Effective alignment with environmental strategy.
- Effective alignment with corporate governance.
- Effective alignment with IT governance.
- Effective alignment with other strategies.

h) Monitoring and Ongoing

As part of the strategy process, the objectives and outcomes of the programme that is being implemented must be clearly defined. Successful monitoring delivers information that allows organisations to track their progress towards outcomes and make amendments to implementation arrangements as necessary (Rutnam, 2013). A data governance programme needs to evolve a means to monitor its own effectiveness; therefore, without monitoring, the data governance programme will certainly fade away (Ladley, 2012). An over-emphasis on technology controls in cloud computing will lead to underlying weaknesses in data governance processes (Cloud Security Alliance, 2015). Therefore, monitoring is important for cloud consumers to ensure control of their data in the cloud provider environment, and to ensure that their data is very well managed. It is also useful to ensure that all the cloud data governance activities are implemented correctly.

Thus, the real cloud data governance programme requires ongoing monitoring and evaluating to promote continuous improvement. A number of scholars have observed that "*you cannot manage what you do not measure*" (Ladley, 2012). Thus, a cloud data governance programme needs tools and metrics to measure and monitor its process. These tools and metrics will help cloud consumers to capture and measure the effectiveness and value generated from cloud data governance, and monitor compliance and exceptions to defined policies and rules. They will also enable transparency and auditability for the data assets of the organisation in the cloud environment. However, in the literature there are many monitoring and ongoing factors that affect an organisation's implementation of data governance and cloud data governance (Mary et al., 2011; Smitha et al., 2012; Felici et al., 2013). This study classifies the organisational factor into three sub-factors:

- Measuring and reporting for continuous improvement of cloud data governance.
- Training and education of the organisation's staff on the cloud data governance programme.
- Executing a cloud data governance change plan.

2.8. Critical Review Findings

The finding above carries testimony to the interest in the specifics of data governance, where multiple challenges remain for its implementation. In addition, much research needs to be carried out in this regard before organisations will formally start implementing data governance for cloud computing services. Thus, while a few studies have been published that provided details of some aspects of data governance, practical work that would unequivocally answer the questions regarding how organisations can effectively implement data governance is perhaps not as widely available. A host of related issues also need to be addressed, including a conceptual model of the data governance for cloud computing and the precise nature of the effect of various factors on the implementation of data governance for cloud computing services in government organisations.

The majority of studies undertaken to date are intended to prove the potential advantages that could accrue to organisations from implementing data governance, although hardly any studies have shown the impact of undertaking this initiative in governmental organisations. This study finds many limitations in these studies in terms of data governance in the non-cloud environment; to the best of the author's knowledge these include:

- Currently there is no single approach to the implementation of data governance programmes in all organisations.
- All existing research ignores the fact that each organisation requires a specific data governance configuration that suits a set of contingencies.
- All existing sources from scholars and practitioners focus on the placement of decision-making authority for data quality management (DQM) and organisational structuring for data governance in a non-cloud environment.
- Decision-making structures within data governance programmes are poorly designed and there is limited information on best practices for the development of governance requirements.
- Lack of effective data governance solutions and policies.
- Lack of clarity over the interaction of roles and responsibilities in data governance programmes.
- There is a gap between practice and theory identified by the absence of a strategy framework for implementing data governance in both the public and private sectors.
- No academic empirical studies show data governance for cloud and non-cloud environments.

Regarding data governance in cloud computing, there is little research focusing on this area in terms of accountability and interoperability. Also, there is little research focusing on the information security governance framework in cloud computing.

Another noticeable issue is how much ground governments in developing countries such as Saudi Arabia need to cover with regard to cloud data governance before implementing cloud computing services (Alkhater et al., 2014; Noor, 2016). The majority of studies undertaken gather data from simple questionnaires and similar tools to collect information on the adoption of cloud computing in Saudi Arabia (Alkhater et al., 2014; Alsanea, 2015). However, there is now an urgent need to undertake significant empirical studies observing the effects and the results of the adoption of cloud computing in current data governance by government organisations. Furthermore, the prerequisites and basic bottom-line requirements for an organisation wishing to implement data governance for cloud computing services are not clearly and expressly defined. In the absence of clearly laid-down frameworks and best practices for data governance in the cloud, government bodies are often unclear about the precise requirements that would enable them to benefit from the functionality of data governance for cloud services. This study finds many limitations in these studies on data governance in non-cloud and cloud computing environments in the KSA; to the best of the author's knowledge these include:

- Only one study has carried out an empirical study on an information security governance (ISG) framework for IT governance in Saudi Arabian organisations.
- There is no research about data governance in cloud and non-cloud environments for organisations in Saudi Arabia.
- There are no empirical studies on data governance for cloud and non-cloud environments in Saudi Arabia.
- There is no strategy framework to design, deploy and sustain data governance for cloud computing in general and in Saudi Arabia in particular.

2.9. Chapter Summary

This chapter aimed to develop knowledge of data governance and cloud computing technology, and to identify the research gaps. The systematic literature review guideline was used in this chapter to investigate the state of the art of the data governance in traditional technology (non-cloud) and in cloud computing. This chapter also aimed to identify the significant gaps in knowledge that are present in the current literature regarding data governance. A systematic review is provided in this chapter of studies in academic and industry fields related to data governance in the cloud and non-cloud environments. The published empirical literature relevant to data governance implementation in cloud and non-cloud environments was reviewed. Critical success factors (CSFs) and barriers to implementation of cloud data governance have been discussed. The research gap has been identified in this chapter and it has been shown that there is an absence of theoretical and empirical studies on the implementation of data governance for cloud computing services in general and more specifically in the KSA. In addition, a critique of the relevant literature is provided followed by a summary that includes the identification of gaps in the literature. The following chapter will present a proposed strategy framework to design, deploy and sustain an effective cloud data governance programme.

Chapter 3. A Strategy Framework for Cloud Data Governance

3.1. Introduction

In the light of the previous discussion, it is clear that there is no effective framework to implement cloud data governance programmes in organisations. Existing frameworks were mostly focused on data governance structure, data quality and the important processes required to implement data governance for non-cloud (traditional IT) environments, and examples of these frameworks were discussed in Chapter Two. As part of the work presented in this thesis, a novel framework to enhance cloud data governance, at this stage for all organisations, is proposed. Therefore, this chapter presents the proposed strategy framework to design, deploy and sustain an effective cloud data governance programme.

The framework is developed based on an analytic theory and critical success factors (CSFs) concept. As part of the framework development in this chapter, the data governance taxonomy is extracted from the literature to understand the key dimensions involved in cloud data governance. Based on this information, the data governance taxonomy and its key dimensions are presented in this chapter before the framework development. Furthermore, the first phase in the proposed framework assists cloud consumers to understand the data governance situation in their organisations. The second phase helps cloud consumers to design data governance activities, while the third phase enables cloud consumers and providers to understand how to implement the cloud data governance programme. The fourth phase helps the cloud consumer and provider to evaluate and monitor the performance of cloud data governance, and the fifth phase helps the cloud consumer and provider with improving and sustaining their cloud data governance.

This chapter also describes the components of each phase of the framework, and the way in which the different phases of the framework interact with each other. The different components' activities used at each phase of the framework are discussed and a justification is given for why these components occur at each phase. Additionally, guidelines on how to manage the framework implementation are also presented in this chapter. This study shows how the secondary research has informed the development of the framework and an overall summary of the framework is presented.

3.2. Theoretical Foundation

This section provides an insight into the theoretical foundation of this research. A theoretical basis provides a guide for the researcher in the interpretations of the results of their study (Simon & Goes 2011). Both academic researchers and practitioners consider that the loss of governance of data in cloud computing has several impacts on cloud users' strategies and on the capacity to meet their mission and goals. Both sides share the consensus view that data governance is not a one-size-fits-all proposition (Weber et al., 2009). However, to the best of the author's knowledge, there are no empirical studies in the academic literature that address data governance for cloud computing.

This research aims to close this gap by developing a strategy framework to understand how to implement a data governance programme for the cloud services on the basis of a comprehensive analysis of the data governance in both science and practice. In the following section, different approaches and concepts found in the literature will be considered as part of the theoretical foundation of this research, enabling afterwards the construction of the conceptual framework of the study. These approaches and concepts are the following:

3.2.1. Analytic Theory

Analytic theory is useful for understanding the data governance topic, and for understanding the existing data governance frameworks (Otto, 2011). Gregor (2002) showed that "*descriptive theories are needed when nothing or very little is known about the phenomenon in question*"(Gregor, 2002, p.7). The analytic theory is the most basic type of theory used to analyse a phenomenon (Gregor, 2006). Gregor (2006) postulated that the analytic theory is useful for describing or classifying specific dimensions or characteristics of individuals, groups, situations or events by summarising the commonalities found in discrete observations. With the popularity of frameworks, classification schema, and taxonomies in IS, the variants of the analytic theory are referred to as classification schema, frameworks or taxonomies (Gregor, 2002). In this study, the analytic theory has been chosen as a concept with which to make a strategy framework for implementing data governance for cloud services. Since this study will be based on the deductive approach, the analytic theory will be suitable for conducting the research. In this context, the deductive approach and analytic theory are used as they allow the researcher to acquire a more complete view and different perspectives of the research problem being studied. The research approach comprises three steps:

Step 1: Analysis of the scientific and practice-oriented literature related to data governance in general and for cloud computing in particular – this was explored in the literature review (see Chapter Two).

***Step* 2:** All data governance frameworks in the sources of literature are analysed and coded according to the dimensions of the cloud data governance.

Step 3: The analysis of both scientific and practice-oriented literature combined with a comparison of existing data governance frameworks. This will allow an insight into the dimensions, concepts and relationships within this area. Once further analysed and generalised, these features will then be developed into a novel strategy framework for cloud data governance. Table 3.1 gives gives a summary of using analytic theory for cloud data governance.

Table 3.1 Use of analytic theory for data governance

<table>
<tr><th colspan="3">Theory Overview</th></tr>
<tr><td colspan="3">This theory is one of the types of theory used in information systems. Gregor (2006) describes this theory by saying that it "provides a description of the phenomena of interest, analysis of relationships among those constructs, the degree of generalizability in constructs and relationships and the boundaries within which relationships, and observations hold".</td></tr>
<tr><th colspan="3">Theory Scope</th></tr>
<tr><td colspan="3">The scope of this theory is the methodologies and procedures that have been proposed in the scholarly literature – these are systematic reviews, taxonomy and process.</td></tr>
<tr><th>Theory Component</th><th>Task</th><th>Means of Representation</th></tr>
<tr><td>Analysis of the literature review</td><td>To understand the state of data governance in both science and practice, and to identify any gaps in research.</td><td>Words, diagrams, tables.</td></tr>
<tr><td>Taxonomy</td><td>To identify and classify specific dimensions or characteristics of data governance for non cloud (traditional IT) and cloud computing.</td><td>Words, diagrams.</td></tr>
<tr><td>Prescriptive Statements</td><td>Identify the important processes for designing, deploying and sustaining cloud data governance programme.</td><td>Words, diagrams, tables.</td></tr>
<tr><td>Framework</td><td>Design a strategy framework for an effective cloud data governance programme.</td><td>Diagrams, process.</td></tr>
</table>

3.2.2. Critical Success Factors (CSFs) Concept

In combination with the steps of analytic theory (as mentioned in section 3.2.1), CSFs are also used in the development of the strategy framework for cloud data governance. They allow a different aspect for the framework development that will not be addressed within the existing frameworks. Therefore, the CSFs for implementing data governance for the cloud will be considered in this chapter. The CSF concept is a good theoretical basis to support this objective. The concept of CSFs has been established over the last 30 years by a number of researchers, particularly by Rockart in 1979 (Forster & Rockart, 1989). Currently, this approach is increasingly used to support IS strategic planning by consultants and IS departments (Amberg et al., 2005). Pinto & Prescott, (1988, p.8) argued that "*the majority of the studies in the critical success factor research stream have been theoretical and have assumed a static view of the importance of various factors over the life of a project*". The literature also showed that the CSF concept is important for overall organisational objectives, missions and strategies. The CSF concept is appropriate to each unit of business and the overall organisational aim in the fulfilment of the organisation's objectives (Amberg et al., 2005). Establishing clear CSFs would be a significant element of risk management and of eventual data governance programme success (Ladley, 2012). This requires a repetitive process for CSF identification, validation and analysis of the constraints underlying each CSF, and a determination of the measures needed for each identified CSF (Amberg et al., 2005). Thus, a successful data governance programme requires a number of CSFs.

3.3. Cloud Data Governance vs. Non-Cloud Data Governance

Although the majority of organisations have been interacting with technology (traditional IT) to carry out their work in recent years, there is no disputing the fact that cloud computing differs greatly from traditional IT (Joint & Baker, 2011). The risk of moving data outside organisations is what fundamentally distinguishes cloud computing from traditional IT (in-house) (Matthews & Muntés-Mulero, 2013). Data stored in a cloud environment is more likely to be exposed to risks than in traditional IT, so organisations have to adopt many solutions to avoid these risks. However, many organisations lack the resources, time, technology or expertise to research and develop cloud computing initiatives and innovations (Mukherjee & Sahoo, 2010). Also, decision making relating to the cloud differs from that of traditional IT, because the cloud provider will be involved in these decisions. Many organisations in different countries are adopting cloud computing at an increasing rate, according to a report published by RightScale in 2016. The report was based on a survey of

1060 organisation in different countries at various stages of their business life cycles. The report states that 80% of organisations have already adopted cloud computing, dividing this into 26% cloud beginners (first project), 25% cloud explorers (running apps), and 29% cloud focused (heavy use). The report also shows that 9% of the organisations surveyed said that they were still planning to adopt cloud computing solutions, and 11% planned to adopt cloud computing in the next few years. In addition, 18% of the respondents were using a public cloud, 6% were using a private cloud and 71% were using a hybrid cloud (public cloud= 89%, private cloud=77%). Along with this increase in adopting cloud computing in organisations come the associated risks, privacy and security issues, as well as the mismanagement and misuse of data.

The main goals of data governance for cloud services are to ensure that the data meets the needs of the business and that the cloud consumers have control of their data in order to ensure the integrity, security and confidentiality of that data. Also, it is important to develop data as a valued organisational asset, to manage and resolve data-related issues, and to lower the cost of managing data in the cloud environment. Data governance sets the procedures, policies and standards required to manage data in the cloud (Cloud Security Alliance, 2015). A few data governance frameworks exist, as presented in the literature review chapter, but these frameworks focus on non-cloud (traditional IT) computing. However, there are some differences between data governance for non-cloud (traditional IT) and cloud computing with regard to implementing some dimensions. Table 3.2 is an attempt to show some of these differences.

Table 3.2 The differences in the five common defined dimensions between the cloud and non-cloud (traditional IT) paradigm

Dimensions	Non-Cloud (Traditional IT)	Cloud Computing
Data governance function	• All data governance policies are handled in-house.	• Data policies are implemented but then it is up to the third party to ensure the guidelines are followed.
Data governance office structure	• The infrastructure is on-site, and all aspects of data governance are left to the local administrators.	• The infrastructure is multi-site, thus new members are involved in the data governance structure, such as cloud managers, cloud providers and cloud brokers.

Dimensions	Non-Cloud (Traditional IT)	Cloud Computing
Organisational	• No extra cost. • Internal training. • Local employees involved in data governance structure.	• Extra cost and training. • Change management. • New skills and experience are needed for cloud computing. • New roles and responsibilities. • External members are involved in the data governance structure.
Technical	• The infrastructure is set up and maintained by local administrators in the IT department. • Runs programs and services on servers by local administrators. • Data governance policies are implemented by local administrators. • No loss of control and governance. • Local administrators have responsibilities to protect data.	• The infrastructure is set up and maintained by a third party. • Runs programs and services on servers by a third party. • Data governance policies are implemented by a third party. • Loss of control and governance. • A third party has responsibilities to protect data.
Environmental	• Less complex regulation.	• Cloud regulation alignment will be considered in data governance policies.

3.4. Data Governance Taxonomy

As mentioned above in Table 3.2, there are differences between the implementation of data governance for non-cloud (traditional IT) and cloud computing based on five common dimensions. Based on these differences, this section contributes by showing the taxonomy of data governance extracted from the literature review. Moreover, this taxonomy will be beneficial for this study, as knowing the key dimensions of data governance for traditional IT and cloud computing is important for the generation of the proposed framework.

The taxonomy approach also helps to understand the data governance aspects in cloud and non-cloud environments. Thus, this study presents the data governance taxonomy, which is considered to be one of the contributions of this research, before developing the proposed framework. This study classifies the taxonomy of data governance into two parts: traditional data governance and cloud data governance. This study also presents the sub-taxonomy related to a high-level taxonomy of data governance. Figure 3.1 shows the high level of data governance taxonomy.

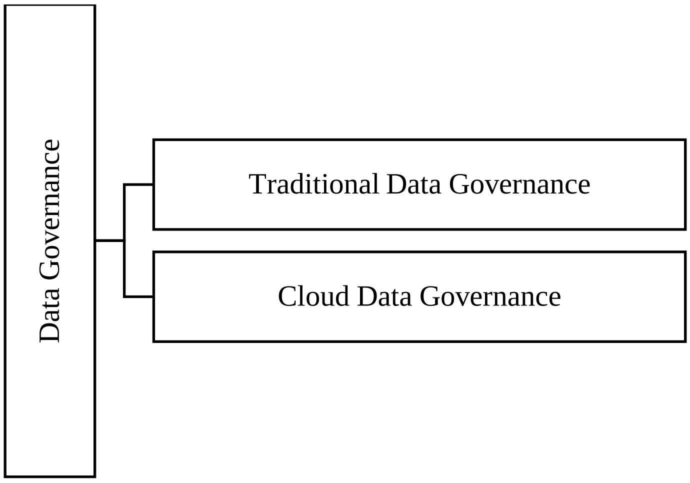

Figure 3.1 High level of data governance taxonomy

3.4.1. Traditional Data Governance

Several studies published by academia and industry are interested in data governance. Some of these studies present the aspects of data governance from their own point of view, because they agree that there is no single approach to the implementation of data governance in all organisations (Begg & Caira, 2012). This means that each organisation's approach to data governance will be unique and should be aligned with cultural tendencies in the organisation. In short, there are common traditional aspects for all organisations' structures on which the data governance approach depends.

In the taxonomy in this study, traditional data governance is understood as data governance structures for traditional IT. This structure will follow the organisation's structure, which determines how to manage data and to ensure a high level of data quality across the organisation's internal departments. This study classifies traditional data governance into three categories: people and organisational bodies, policy and technology. Figure 3.2 shows the traditional data governance taxonomy.

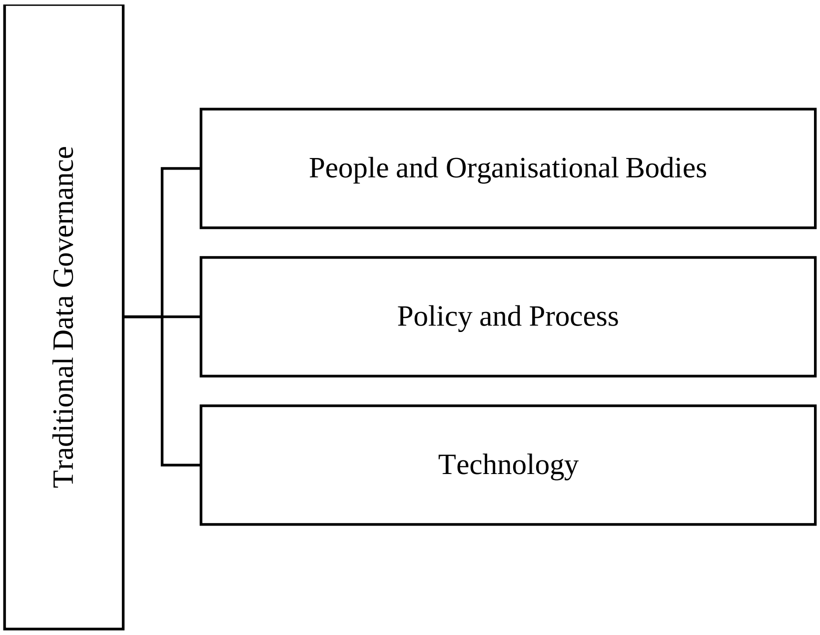

Figure 3.2 Traditional data governance taxonomy

- **People and Organisational Bodies**

Data governance will influence the mix of data stakeholders involved in data-related decisions and actions in an organisation, as well as the amount of effort required of the stakeholders. Therefore, in traditional data governance, the people and organisational bodies play an important part when organisations implement data governance for their business (Jansen & Grance, 2011). The people and organisational bodies element in data governance can be defined as: any individual or group that could affect or be affected by the data under discussion.

In traditional data governance, this comprises the following: data governance office, data governance council, executive sponsorship, chief information officer (CIO), data management committee, compliance committee and data stewards. All of them have specific roles and responsibilities within the organisation. The people in traditional governance have many tasks: authority, data stewardship, business rules, collaboration, accountability and culture attitude (Pokharel, 2013). Figure 3.3 shows the people and organisational bodies factors for traditional data governance.

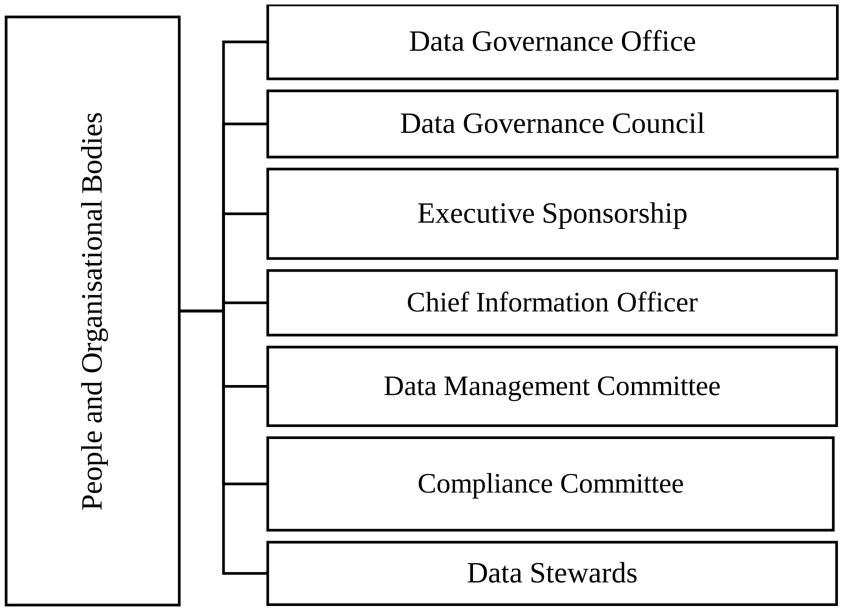

Figure 3.3 People and organisational bodies taxonomy in traditional data governance

- **Policy and Process**

The aim of a data governance policy is a set of measurable rules for a series of data management functions, in the context of organisational scope and policy, for ensuring the benefit of a business process (Thomas, 2006). The data governance processes also aim to describe the methods used to govern data, and these processes should be standardised, documented and repeatable (Thomas, 2006; Soares, 2012). Data governance policies and processes should be crafted to support regulatory and compliance requirements for data management functions. The policy and process aspects in traditional data governance comprise the following: principles, policies, standards and processes. All of these aspects consist of defining the statement, rationale, implications and key actions. Figure 3.4 shows the policy and process factor for traditional data governance.

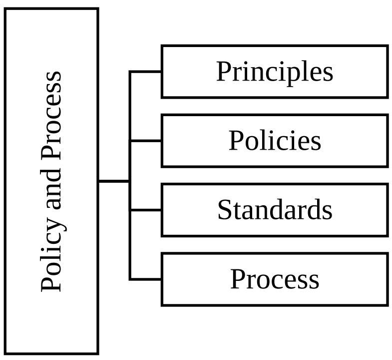

Figure 3.4 Policy and process factor in traditional data governance

- **Technology**

Technology is the most important factor to achieve data governance benefits for organisations, and it aims to automate, enforce and control data governance policies. Therefore, the role of technology is important after the data governance policy and process have been approved by the data governance committee. Technology in data governance refers to the engineering methods responsible for implementing and measuring the data governance policy. The data governance teams must develop a plan for using the technical tools to support the data governance polices within the context of the roles, responsibilities and accountabilities (Thomas, 2006; Begg & Caira, 2012). The technology factors in traditional data governance are hardware, software and monitoring tools. Figure 3.5 shows the technology factors for traditional data governance.

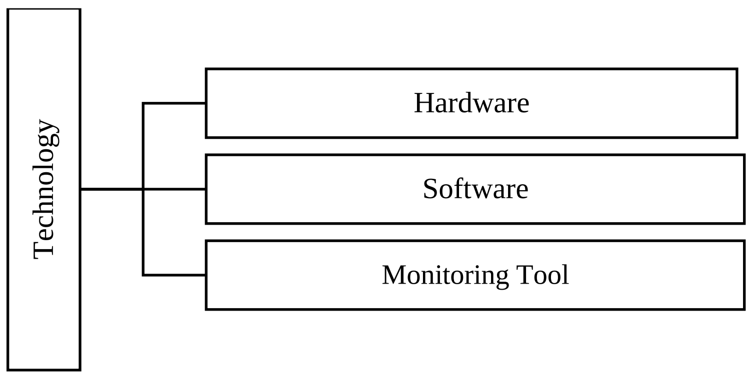

Figure 3.5 The technology factors in traditional data governance

3.4.2. Cloud Data Governance

Cloud data governance is the second part of the data governance taxonomy in this study, and it is the main focus area in this research. Data governance is one of the most important issues in the cloud; also, it is an important aspect that contributes to cloud consumers maintaining control over and trust in their data when they move to the cloud provider's environment (Catteddu & Hogben, 2009; Tweneboah-koduah, 2014). The research on data governance in general and in cloud computing in particular is still limited and in its infancy (Wende, 2007; Nwabude et al., 2014). Cloud data governance is an often neglected but necessary component of successful cloud computing adoption in organisations. There is a strong consensus that cloud computing will lead to changes in the strategy of traditional data governance in organisations (Trivedi, 2013). Cloud data governance is a term for applying specific functions (e.g., policies and principles) to gain data control in cloud computing services. The goal of cloud data governance is to gain control of cloud consumer data when it is located in the cloud provider's environment. Ideally, cloud data governance complements or is integrated into existing data governance processes and it is viewed as an ongoing process. Therefore, this study aggregates all the aspects that data governance needs to implement in the context of cloud computing in one taxonomy. The taxonomy of cloud data governance consists of 10 key elements: data governance office structure, data governance policy and process, cloud deployment model, service delivery model, cloud actors, service level agreement (SLA), organisational context, technological context, legal context and monitor matrix (see Figure 3.6).

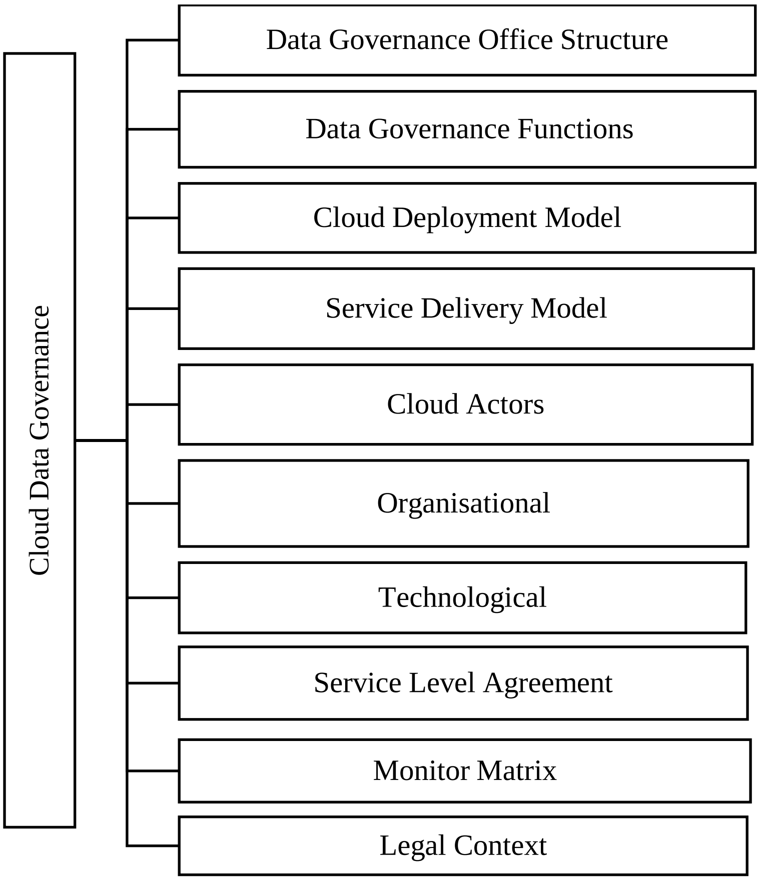

Figure 3.6 Cloud data governance taxonomy

- **Data Governance Office Structure**

A data governance office structure is a key resource for organisations that need to be deliberate about how they use data resources and control their data when it moves to the cloud computing environment. The data governance office partners with various business units to set data governance standards and policies for cloud computing services. This includes how data is formatted, stored and accessed in the cloud. It also monitors all data types in the cloud to ensure compliance with data governance standards and policies, and drives the continuous improvement of data quality for organisation. This means that the data governance structure includes many work groups. They have to continue working closely with the business unit to make significant changes to how data is managed in cloud computing. The office is also responsible for building the data governance process and policy for cloud computing services, and the distribution of the roles and responsibilities among cloud actors. The data governance office structure for cloud computing involves many individual members and working groups: executive sponsorship, data management committee, compliance committee, data stewardship team, cloud manager, cloud provider members, IT members and legal members. Figure 3.7 shows the data governance office structure for cloud data governance. In addition, each part of this taxonomy has sub-taxonomies, all of which will be discussed by this study.

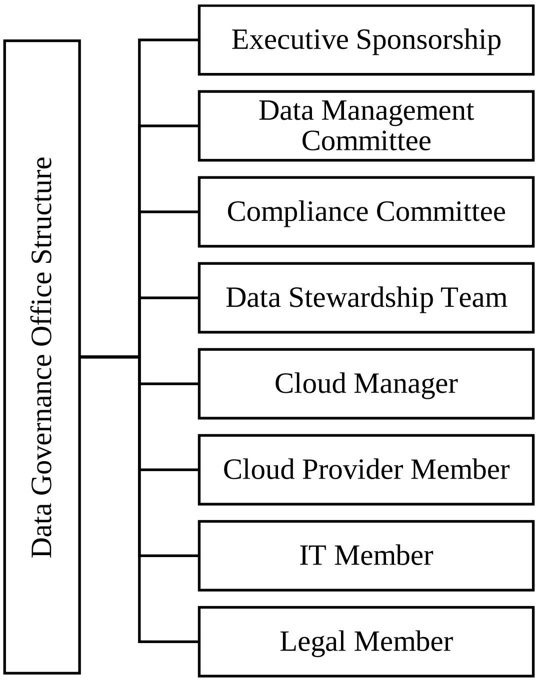

Figure 3.7 Data governance structure for cloud data governance

- **Data Governance Functions**

Establishing consistent policies, standards and operating processes to ensure the accuracy, availability and security of data should be part of the data governance strategy as well as defining the organisation's data assets (Ladley, 2012). Therefore, the data governance team has to define all data governance polices that support the cloud consumers' concerns when moving their data to a cloud environment. The data governance policy must comply with business policy. The data governance functions (policy and process) can help the organisation to make cloud service decisions such as the geographic distribution of data stored, processed and in transit, regulatory requirements, data management requirements and audit policies (Mary et al., 2011). Good data governance in cloud computing requires transparency and accountability, which lead to appropriate decisions that foster trust and assurance for cloud consumers (Groß & Schill, 2012; Tountopoulos, 2014). All of these factors should be considered when establishing data governance rules for cloud computing services. Thus, the cloud provider must follow these rules, which will be written in the SLA. The data governance functions for cloud data governance include process, standard, principles and procedure. Additionally, the data governance set should include compliance, transformation, integration, management, auditability and transparency. Figure 3.8 shows the data governance function and its concerns for cloud data governance.

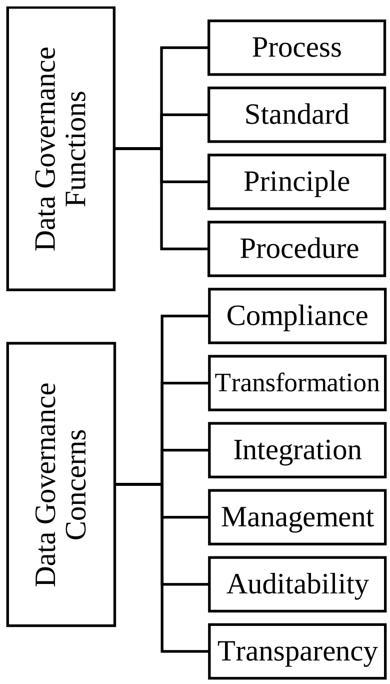

Figure 3.8 Data governance functions and its concerns for cloud data governance

- **Cloud Deployment Model**

The deployment model is the basis of cloud computing, and it means that an organisation should consider how clouds can be deployed (Mell & Grance, 2011). Cloud computing may be deployed privately or hosted on the premises of the cloud customer, shared among a limited number of trusted partners, hosted by a third party, or be a publicly accessible service

(Eugene, 2013). Therefore, the roadmap of data governance varies greatly based on the cloud deployment models supported (public, private, hybrid, community)(Weber, 2011). The data governance teams should consider the different characteristics of these deployment models when implementing data governance for cloud computing services. Therefore, the data governance approach for the cloud can help organisations to keep control of their data at different stages of deployment. This consideration will assist an organisation to achieve strong data governance for cloud computing services. The cloud deployment models that are considered to be part of cloud data governance are private, public, hybrid and community. Figure 3.9 shows the cloud deployment model types for cloud data governance.

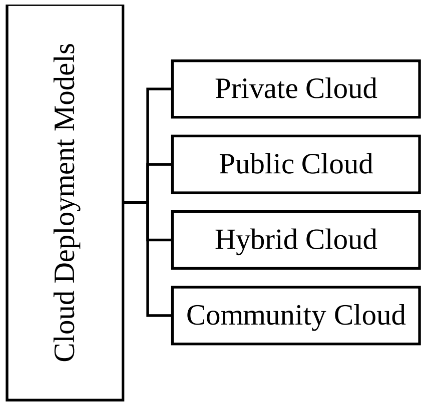

Figure 3.9 Cloud deployment model types for cloud data governance

- **Service Delivery Models**

Cloud computing technology provides on-demand and pay-per-use access in different ways to elastic virtualised computing resource pools(Mell & Grance, 2011). These resources are abstracted to services so that cloud computing resources can be retrieved as infrastructure (IaaS), platform (PaaS) and software (SaaS) services respectively (Groß & Schill, 2012). As the cloud computing environment is very different from traditional IT outsourcing in the service delivery model, it requires a new approach to data governance and management(Becker et al., 2014). Moving to the cloud environment forces the cloud consumer to accept the control of the service provider on a number of important issues and areas of the business process(Arturo & Alvarez, 2011). To avoid the potential pitfalls of extending data governance to the cloud paradigm, organisations should put in place and sustain a practical data governance framework to ensure that the cloud computing infrastructure and operations are as secure, if not more so, than traditional IT governance approaches (Becker et al., 2014). Also, the cloud consumers lose control over their data in these models. Therefore, the data governance approach for the cloud services should involve all cloud service models. The cloud service delivery models that are considered to be part of cloud data governance are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Figure 3.10 shows the cloud service delivery model type for cloud data governance.

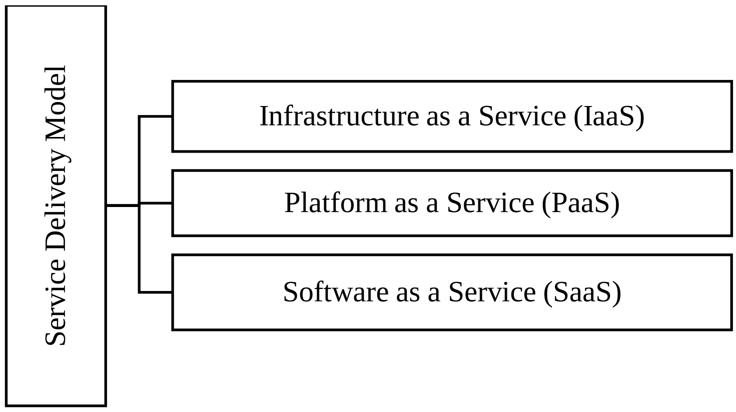

Figure 3.10 Cloud service delivery model for cloud data governance

- **Cloud Actors**

The term 'cloud actors' refers to a person or an organisation that participates in a process or a transaction and/or performs tasks in the cloud computing environment. According to the NIST, cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud auditor, cloud carrier and cloud broker (Lui, 2011). As increasingly large amounts of data (e.g., personal and confidential) are transferred to the cloud, stakeholders' interactions change and responsibilities are allocated across the entire cloud among the cloud actors (Felici et al., 2013). Data governance in the cloud therefore requires understanding, moderating and regulating the relationships among cloud actors, and identifying the roles and responsibilities between them (Badger et al., 2011).

The data governance team in an organisation must identify all the responsibilities and accountability that support the cloud actors' roles in data governance for the cloud services. The cloud actors that are considered to be part of cloud data governance are the cloud consumer, cloud provider, cloud auditor, cloud carrier and cloud broker. Figure 3.11 shows the cloud actors for cloud data governance.

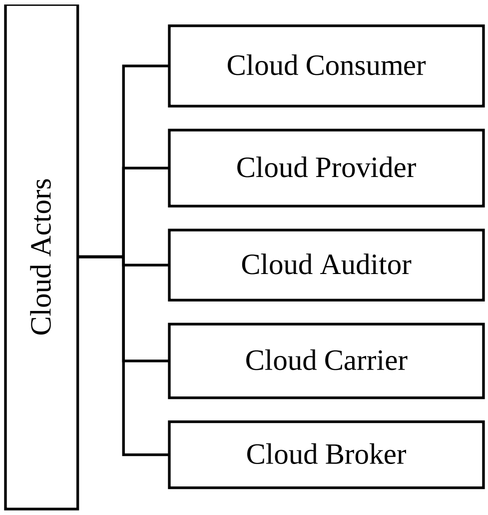

Figure 3.11 Cloud actors for cloud data governance

- **Service Level Agreement (SLA)**

One key issue for cloud computing consumers is to provide governance for data that they no longer directly control (Cochran & Witman, 2011). One of the best solutions for this issue is service level agreements (SLAs) between cloud actors. Cloud SLAs are important to clearly set expectations for services between cloud consumers and providers and to provide guidance to decision makers on what to expect and what to be aware of with regard to cloud computing requirements(Chawngsangpuii & Das, 2014). Before evaluating any cloud SLA, cloud consumers must first develop a strong business case for the cloud services, with data governance-level policies and requirements, and a strategy for their cloud computing environment. The SLA should contain a set of guidelines and policies to assist client organisations with defining governance plans for data they may choose to move to a cloud provider (Cochran & Witman, 2011).

These have to comply with legal and regulatory requirements. All of these policies can be negotiable between the cloud consumer and cloud provider to identify the target level of data governance before the contract is drawn up. The SLA for cloud data governance includes data governance functions, data governance requirements, roles and responsibilities, and data governance metrics and tools. Figure 3.12 shows the SLA elements for cloud data governance.

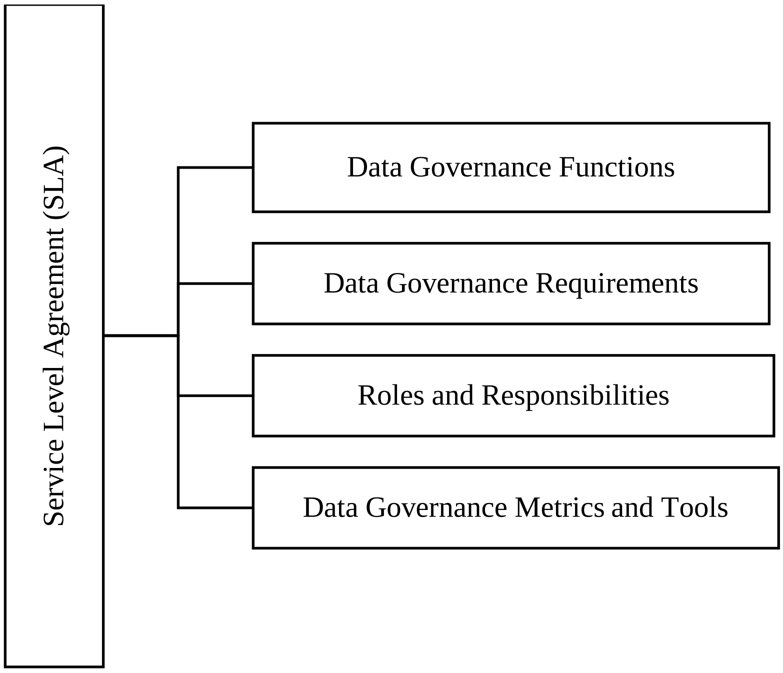

Figure 3.12 SLA elements for cloud data governance

- **Organisational**

Data governance is a major mechanism for establishing control of an organisation’s data assets and enhancing its business value (Ladley, 2012). It is also a critical element in implementing a sustainable data management capability that addresses enterprise information needs and reporting requirements. The data governance team should work closely with the business representatives in an organisation; this will help them to define the data governance roadmap, and to establish priorities and realistic time frames that are aligned with the organisational circumstances and goals (Otto, 2011). Therefore, the data governance functions have to comply with the organisational requirements. The organisational context is an important factor in the data governance strategy for cloud computing, because it encourages top management to support the implementation of data governance (Groß & Schill, 2012). The organisational context means defining all the internal factors that the organisation must consider when it manages risks. There are three perspectives for the organisational context: strategic, tactical and operational. The data governance for cloud computing services should comply with these perspectives. The organisational context for cloud data governance includes organisation charts, organisation vision and mission, organisation strategy, business model, decision-making processes, training plan, communication plan and change management plan. Figure 3.13 shows the organisational context elements for cloud data governance.

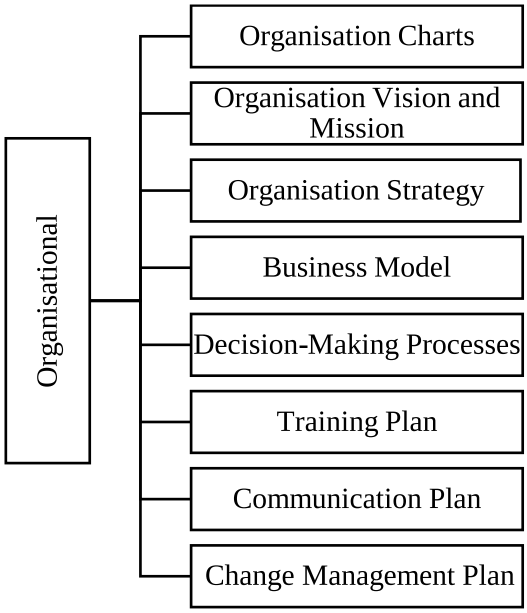

Figure 3.13 Organisational context in cloud data governance

- **Technical**

The technical context represents the issues related to data that will affect the decisions about cloud computing adoption (Alkhater et al., 2014) and the data governance implementation for cloud computing services. The data governance team intending to implement data governance for cloud computing services needs to align all the technological characteristics available at the organisation with the data governance strategy. Thus, the technological context should be considered when implementing a data governance solution for cloud computing services in an organisation.

The technical issues that affect the implementation of data governance for the cloud services include availability, reliability, security, privacy, quality, compatibility, ownership, auditing, integrity, data lock-in and performance (Khajeh-Hosseini et al., 2010; Alkhater et al., 2014). This context is expected to be an important, positive and significant factor for decisions about data governance implementation. Figure 3.14 shows the technological context for cloud data governance.

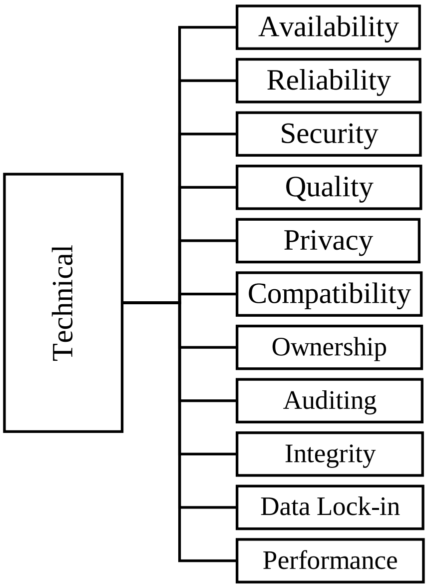

Figure 3.14 Technical context for cloud data governance

- **Legal**

The legal context determines the external and internal law and regulatory elements related to data that might affect an organisation's intent to adopt cloud technology (Alkhater et al., 2014), and these elements might affect the implementation of data governance for cloud computing services. In addition to these elements, the great legal concern is ensuring that data acquired under some form of contract is managed in compliance with such contracts. Therefore, the data governance team must understand what is implied about data in the contracts that exist before implementing a data governance strategy for the cloud services. Also, they must understand the legal/compliance/regulatory issues impacting data(Olaitan, 2016). Failure to comply with the law when dealing with confidential data erodes trust, which can seriously damage the view of the top management in an organisation about the trustworthiness of the cloud provider's services (Mell & Grance, 2011).

This context is expected to be an important and positive significant factor for the decision about data governance implementation. The legal context for cloud data governance includes data protection acts, change of control acts and cloud regulations. Figure 3.15 shows the legal context for cloud data governance.

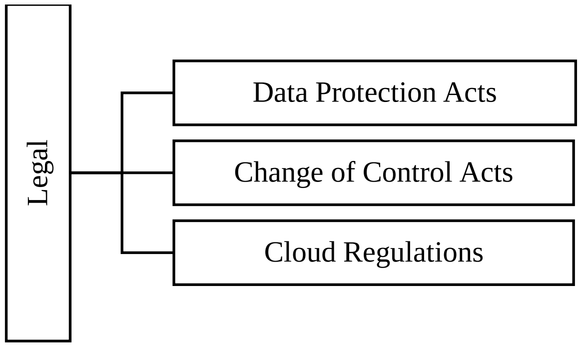

Figure 3.15 Legal context in cloud data governance

- **Monitor Matrix**

The monitor matrix in data governance is the exercise of authority, control and shared decision making over the management of data assets (Salido & Cavit, 2010). The monitor should be applied to all phases of the data governance framework to ensure the enforcement of data governance functions (principles, policy, process, role and responsibility) and the monitoring of risk management between the cloud actors (Mosley, 2008). Moreover, the monitor should be applied to ensure that all points of data governance in the SLA are applied by the cloud provider. It is important to ensure that the data governance complies with organisational, technical and legal contexts and to include this in the monitor matrix. The cloud control matrix is one of the most important factors that should be included in the monitor matrix (Cloud Security Alliance, 2015) as it will assist with minimising the impact of confidential data loss when data is moved to the cloud environment. The data governance monitor matrix for cloud computing services includes a cloud control matrix, key performance indicators (KPIs) and monitoring tool. Figure 3.16 shows the monitor matrix for cloud data governance.

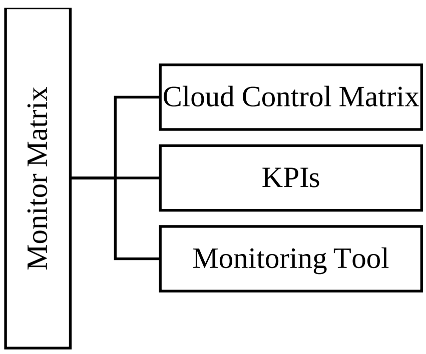

Figure 3.16 Monitor matrix for cloud data governance

Figure 3.17 shows the data governance taxonomies that include details for each taxonomy.

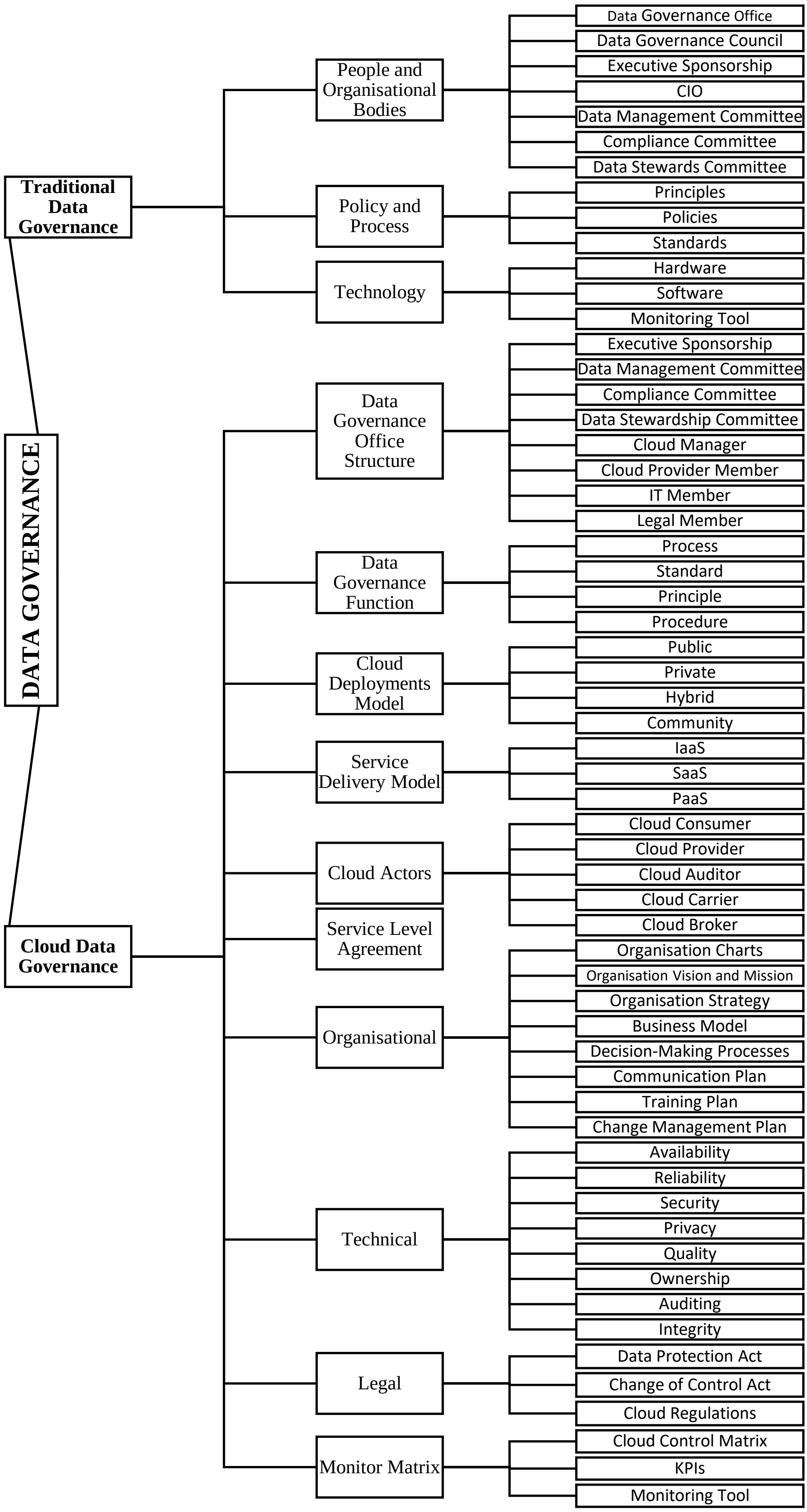

Figure 3.17 the data governance taxonomies that include details for each taxonomy

3.5. Key Dimensions of Data Governance

Many researchers have recognised a need to implement data governance for cloud computing (Wendy, 2011; Rimal et al., 2011; Felici et al., 2013). In order to do this, the key dimensions must be identified. Identifying the specific data governance dimensions for cloud services is potentially a complex process and consequently it needs considerable investigative efforts and to involve different stakeholders. To the best of the researcher's knowledge and following the aforementioned systematic review, there is no published research that defines the key dimensions of data governance for cloud computing.

In contrast, for traditional IT (non-cloud) computing, although scarce, there is some reported research. Therefore, the key dimensions for non-cloud and cloud computing are identified and extracted in this section based on the results of the data governance taxonomy in section 3.4 above.

As illustrated earlier in this chapter, although the data governance for non-cloud and cloud computing has some similarities at a higher level, it differs significantly in the details, in addition to the fact that some new factors are related only to cloud technology. Therefore, it is useful to discuss these similarities and differences. In this section, the key data governance dimensions for cloud computing are developed based on the results of the systematic review presented in chapter two, and on the results of the data governance taxonomy presented in this chapter.

Figure 3.18 is the author's view of the key dimensions that could drive data governance for non-cloud environments, according to the compiled literature. Data governance for traditional IT could be built upon six dimensions, which are described below:

1. Data governance function.
2. Data governance office structure.
3. Organisational.
4. Technical.
5. Environmental.
6. Measuring & monitoring tools.

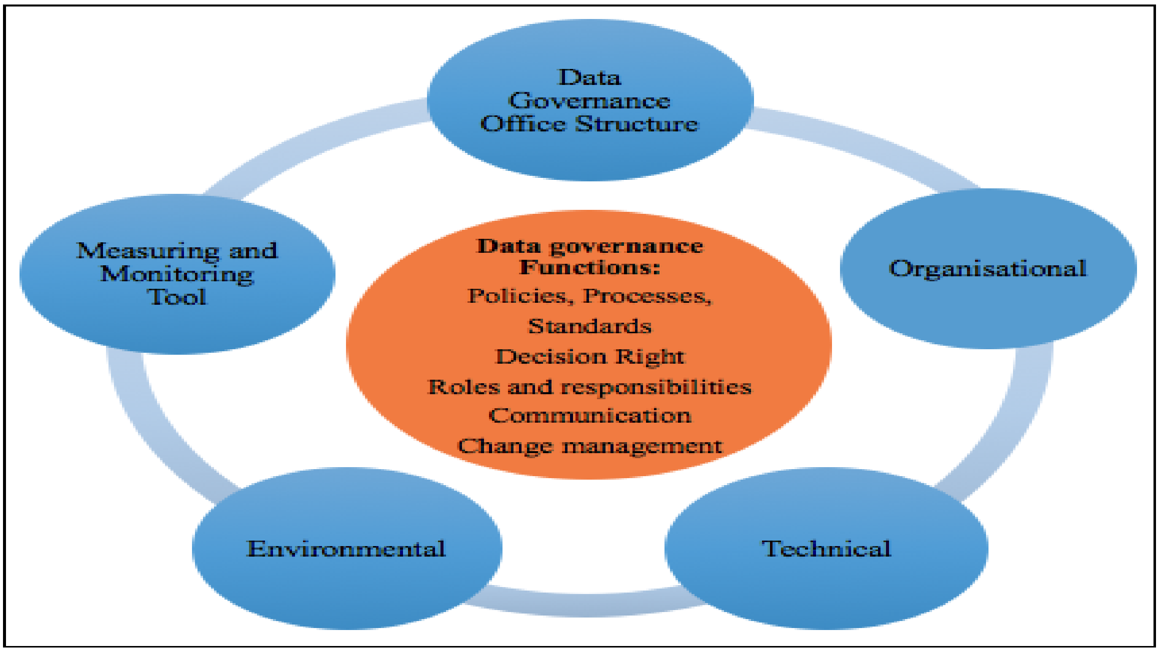

Figure 3.18 Key dimensions for data governance for non-cloud computing

The cloud paradigm, however, introduces new factors that need to be taken into consideration when designing and implementing any cloud data governance programme. These new factors are described below. By considering these new factors, the key dimensions for implementing data governance for cloud computing are derived, as depicted in Figure 3.19.

- **Cloud Deployment Models:** This is an important factor to consider in data governance. There are primarily four cloud deployment models that differ in terms of their level of risk and concerns about control and security, and contractual barriers. They are public, private, hybrid and community. To address data governance, the level of risk and complexity of each cloud deployment model must be taken into consideration (Mell & Grance, 2011).
- **Service Delivery Models:** The cloud service can be categorised into three delivery models: SaaS, PaaS and IaaS (Bulla et al., 2013). In some of these models, the cloud consumer loses control over their data, because the cloud provider has responsibility for managing some components in these models (Kshetri, 2012). Therefore, the data governance teams should consider all the characteristics of the service delivery model and define the policy to enforce control roles and responsibilities.
- **Cloud Actors:** They are also a critical factor in data governance for cloud services. The term ‘cloud actors’ refers to a person or an organisation that participates in a process or a transaction and/or performs tasks in the cloud computing environment. According to the NIST, cloud computing reference architecture defines five major

actors: cloud consumer, cloud provider, cloud auditor, cloud carrier and cloud broker (Kshetri, 2012). All of them have special roles and responsibilities in the cloud, so the data governance teams must define the roles and responsibilities for all cloud actors.

- **Service Level Agreement (SLA):** One key issue for the cloud consumer is to provide governance for data that it no longer directly controls (Cochran & Witman, 2011). Contractual barriers between cloud actors are increased. The SLA is an agreement that serves as the foundation of expectation for service(s) between the cloud consumer and the provider. The agreement states what services will be provided, how they will be provided and what happens if the expectations are not met. Therefore, the SLA is an important factor for data governance; thus, the cloud consumer and provider have to negotiate all aspects of data governance before developing the SLA. As a result, these agreements are in place to protect both parties.
- **Data Governance Function:** This factor includes important activities for data governance which the data governance teams have to take into account when implementing a data governance programme (Power & Street, 2013). The outcomes from this activity are the policies, principles, processes, decision right, roles and responsibilities, communication plans and change management. Therefore, this factor is considered the master dimension for data governance and it must comply with the other dimensions to produce effective data governance.
- **Data Governance Office Structure:** Designing the data governance office structure is an important factor to ensure that requisite roles and responsibilities are addressed throughout the enterprise at the right organisational levels (Panian, 2010). Several common data governance roles have been identified in existing studies on data governance; they are Executive Sponsor, Data Governance Council, Data Governance Office, Chief Steward, and Business and Technical Data Steward (Wende, 2007; Weber et al., 2009). Therefore, they have to collaborate to formulate data governance bodies.
- **Organisational:** Organisational factors are important for the success of data governance (Power & Street, 2013). Data governance requires change management in the organisation. It also requires the participation and commitment of IT staff and business management, and senior-level executive sponsorship in the organisation (Weber et al., 2009b). Moreover, top management support is considered to be the CSF for the implementation of data governance (Panian, 2010). The organisation’s staff

need to learn about the data governance function, therefore the top management's support will help to improve the staff's skills.

- **Technical:** Technology is the key element for data governance success (Fleissner et al., 2014). Therefore, a lack of technology is considered to be a common barrier to successful data governance. The technical dimension represents the data management issues that will affect an organisation's strategy such as security, privacy, quality and integrity. Thus, organisations that are intending to implement data governance need to assess all the technological characteristics that are available to them to achieve effective data governance.
- **Environmental:** Environmental refers to external environmental factors such as government legislation and data protection acts (Power & Street, 2013). The data governance teams should consider all aspects of environmental factors when designing data governance functions. This means that the data governance functions have to comply with this factor. This will contribute to building strong data governance in the organisation.
- **Measuring & Monitoring Tool:** Measuring and monitoring supports ongoing data governance efforts to ensure that all incoming and existing data meets business rules (Thomas, 2009). Adding a monitoring component to the data governance programme will enhance data quality efforts and make data much more reliable (ISACA 2016).

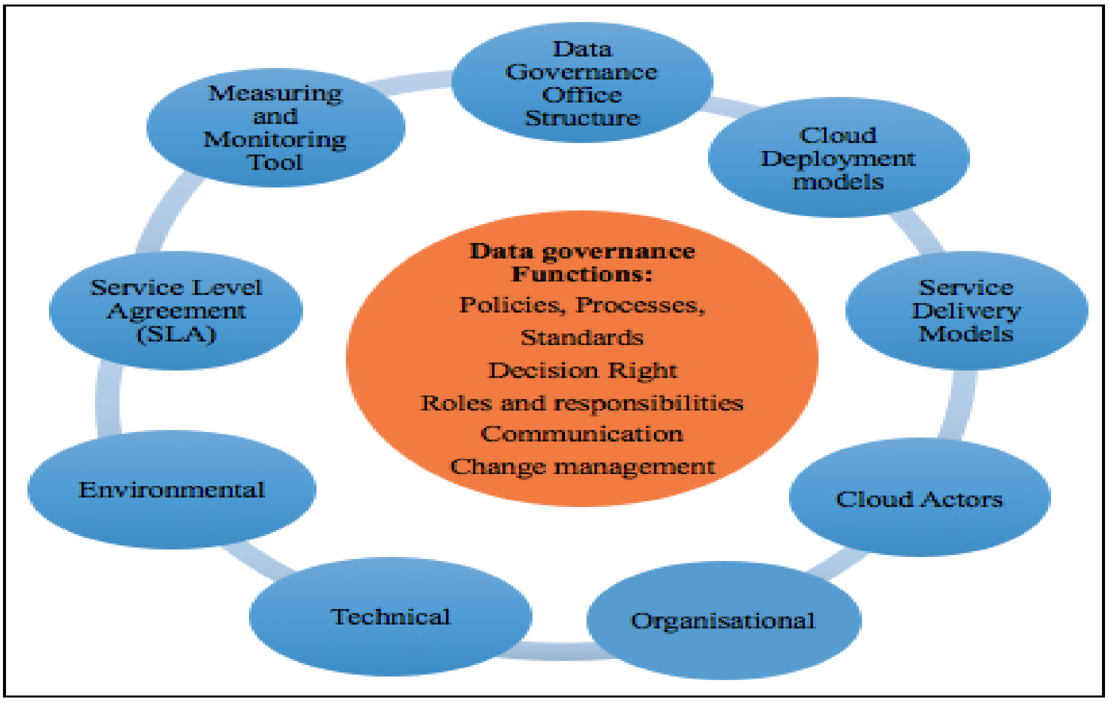

Figure 3.19 Proposed key dimensions for cloud data governance

As mentioned above, the six dimensions are common when implementing data governance for cloud or non-cloud (traditional IT) computing; however, they differ in their implementation.

3.6. Definitions of a Strategy Framework for Cloud Data Governance

As illustrated earlier in chapter One, there is currently no agreed-upon definition for a data governance framework within the literature. In order to determine what data governance is, chapter One in this study referred to some different definitions offered in the literature. However, a strategy framework to implement a cloud data governance programme is even harder to define because the area is both novel and constantly evolving. Therefore, to ensure consistency within this work it is necessary to provide a definition for a strategy framework for cloud data governance.

This novel definition is as follows: a strategy framework for cloud data governance is one that operates within the unique features of cloud environments and allows the development of a strategy to understand how to design, deploy and sustain an effective data governance programme for decisions rights and accountabilities. It encourages desirable behaviour in the use of data within the cloud environment by developing policies, guidelines and standards that are consistent with the organisation's strategy and integrating these within the cloud computing context. Throughout the rest of this study this definition will be the basis of the meaning of a strategy framework for cloud data governance.

3.6.1. Aim of the Framework

The aim of this framework is to provide a strategy that will help organisations to understand the processes involved in designing, deploying and sustaining an effective cloud data governance programme.

3.6.2. Analysis of Existing Data Governance Frameworks

Given the diverse nature of the existing data governance frameworks and the key dimensions of cloud data governance described in this chapter, this research examined existing frameworks for their use to support the development of a new framework. Table 3.3 shows the data governance frameworks comparison chart.

Table 3.3 The data governance frameworks comparison chart

Frameworks	Key Dimensions of Cloud Data Governance									
	Data Governance function	Data Governance structure	Organisational	Technical	Environmental	Measuring and Monitoring Tool	Cloud Deployment Model	Service Delivery Models	Cloud Actors	Service Level Agreement (SLA)
UW-Madison Framework	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
NCI Metadata Governance Framework	Yes	Yes	Yes	Yes	No	No	No	No	No	No
DGI-Data Governance Institute	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No
IBM Data Governance Unified Process	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No
Morphology of Data Governance Organisation	Yes	Yes	Yes	Yes	No	No	No	No	No	No
Building Blocks of the Data Governance Framework (Panian, 2010)	Yes	No	Yes	Yes	No	Yes	No	No	No	No

As can be seen, none of the existing frameworks are completely suitable for the cloud paradigm in three important ways. First, they are all targeted towards organisations that have adopted traditional IT (in-house) infrastructures. This study recognises that, although important for successful implementation, cloud computing characteristics were not considered in these frameworks. Second, whereas the existing frameworks can meet the needs of traditional IT (in-house), they do not provide a comprehensive framework within which organisations can implement data governance for cloud services in a coordinated way involving all cloud computing actors; thus, the cloud consumers might not be able to identify their roles and responsibilities. Finally, the important phases in designing a strategy for understanding how to implement cloud data governance in organisations were not considered in the existing frameworks.

3.7. The Proposed Cloud Data Governance Framework

The gap analysis exposed several gaps in all of the previous studies and proposed frameworks. The gap was presented in section 3.6.2 – that is, cloud computing characteristics were not considered in the existing data governance frameworks in the literature. It was therefore realised that in order to mitigate the gaps identified within the literature, it is necessary to develop a novel data governance framework for cloud computing. The proposed cloud data governance framework addresses the identified gaps and seeks to satisfy the data governance requirements for organisations. It facilitates an understanding of preserving governance from different stakeholders' perspectives and builds a communal agreement on the data governance requirements of cloud computing services. The proposed framework in this study contains five key phases; the main tasks in each phase in the framework are based on the interdependencies among its components, and these components should be performed when developing data governance. These phases are the following: initial, design, deploy, monitor, and sustain phases.

All the phases of the framework are involved in the process of data governance implementation for cloud computing services and each phase has a specific task. Furthermore, each phase in the framework builds upon the previous one. The initial phase covers the understanding of data governance, the data governance situation in the organisation and the data governance requirements in order to implement it for cloud services. The design phase covers all the tasks that the cloud consumers should complete to design data governance strategy requirements. The deployment phase covers the tasks and activities required to complete and implement data governance for cloud services. The monitoring phase covers all the monitoring tools required to support ongoing data governance efforts to ensure that the data governance is implemented correctly, and that it meets the cloud consumer's requirements. The sustain phase covers the important factors that promote the sustainability of the data governance strategy, and help the cloud consumers to improve their data governance. Figure 3.20 shows the cloud data governance framework architecture.

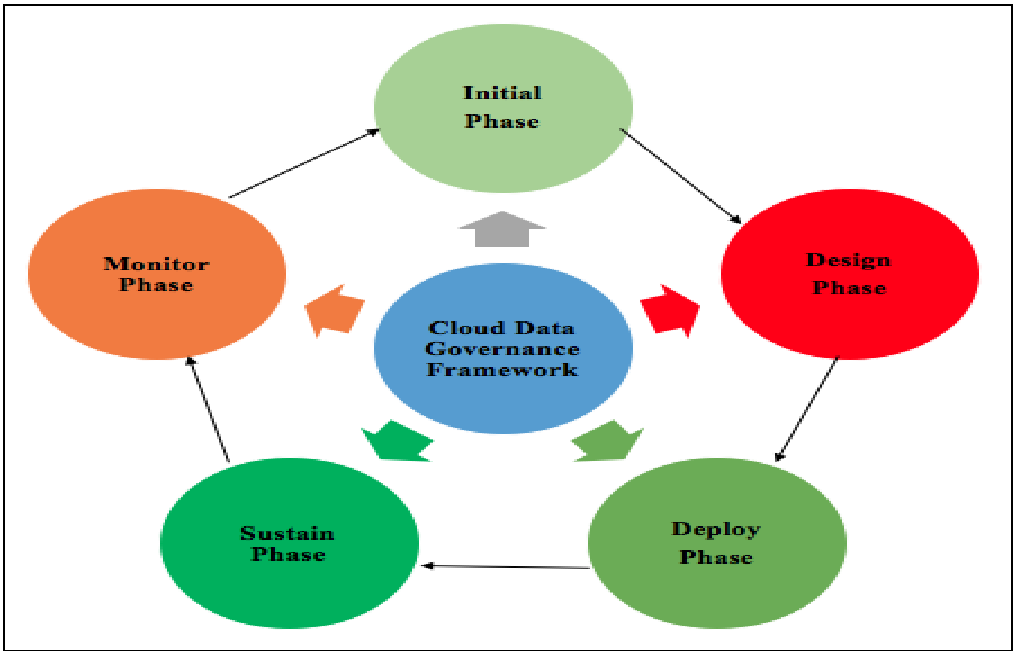

Figure 3.20 Cloud data governance framework phases

3.7.1. Detailed Phases of the Proposed Framework

In this section, the phases of the framework are described in detail, including the processes and procedures that are important to perform to achieve the goals of each phase. The framework phase details have emerged as a result of the literature review, which included CSFs and cloud data governance dimensions. In addition, each component in these phases depends on having an understanding of cloud computing characteristics, which have been neglected in the literature.

a) Initial Phase

This phase covers the understanding of data governance, the data governance situation in the organisation and the data governance requirements to implement it for cloud services. This phase includes four components: cloud data governance office, business case, assessing cloud data governance, and cloud data governance requirements. These are the general components most frequently mentioned in the literature on data governance (Wende & Otto, 2007; Wende, 2007; IBM, 2007; Rifaie et al., 2009) and adopted in this proposed framework. Other sources of information do not explicitly refer to the phase components, but suggest similar concepts equivalent to the components of the initial phase of the proposed cloud data governance strategy (Ibm, 2007). Each component in this phase needs to take into account the cloud computing characteristics, which have been ignored so far in the existing literature. Figure 3.21 shows the proposed components of the initial phase.

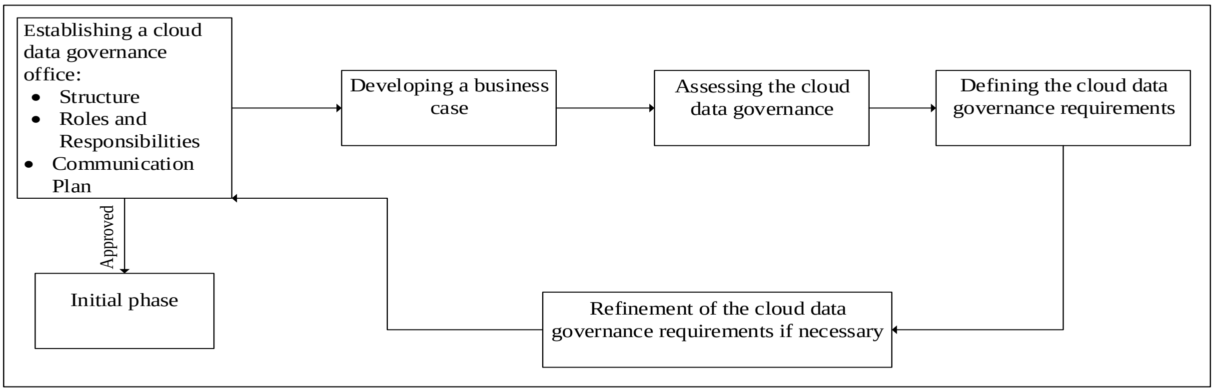

Figure 3.21 The proposed components of the initial phase

- **Cloud Data Governance Office**

Establishing the structure of the data governance office is a critical step to ensure that representative groups at all levels are involved (Niemi, 2011). In the literature, data governance practitioners and researchers have made a number of recommendations for establishing data governance structures in organisations (Wende & Otto, 2007; Wende, 2007; IBM, 2007; Rifaie et al., 2009). The data governance structure is important as a clear structure ensures that individuals within the organisation understand their role and responsibilities within the broader data governance effort for cloud computing services (Felici et al., 2013). In the present study, the cloud data governance office is structured according to the representative groups who are involved in data governance for the cloud. To establish a cloud data governance office, the organisation needs to consider three elements: cloud data governance structure including all stakeholders, communication plan, and roles and responsibilities, as shown in Figure 3.22.

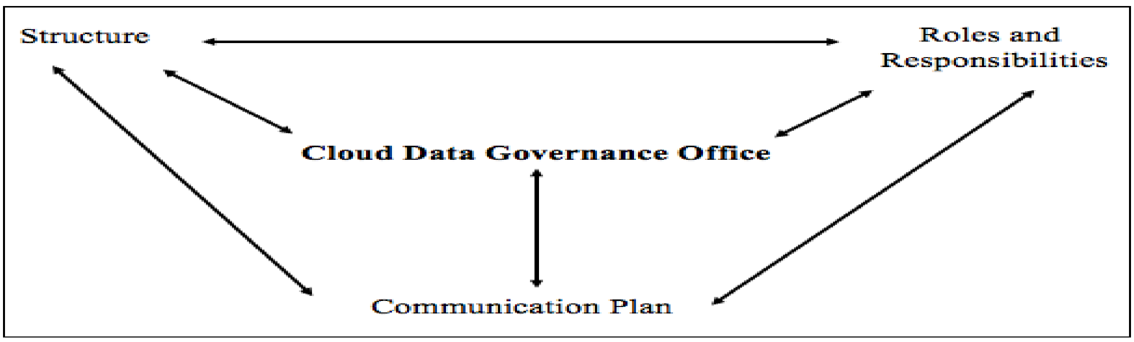

Figure 3.22 Main elements of the cloud data governance office

- **Business Case**

The business case can be defined as "*a formal document that summarises the costs, benefits* *and impact of an investment*" (Maes et al., 2014, p.47). Some researchers and practitioners refer to the importance of the business case for data governance (Wende, 2007; Otto, 2011). In addition, they show how an established business case for data governance is the CSF when implementing effective data governance. The main activities in this component involve finding and exploring opportunities to bring profits to the organisation that can be derived from effective cloud data governance, defining the data governance vision and mission, the cost of data governance, and its benefits and risks. It also involves determining the organisation's expectations and the needs with respect to data governance for cloud computing and resolving possible conflicts that may arise while considering possible changes necessary for implementing it (Ladley, 2012).

- **Assess**

Assessment can be defined as "*a process by which information is obtained relative to some known objective or goal*"(Kizlik, 2012, p.1). In data governance contexts, assessment refers to the ability of the organisation to govern and to be governed (Weber et al., 2009). In the literature, researchers have considered the assessment of data governance in organisations, concluding that the prior implementation of an assessment strategy is important to achieve effective data governance (Wende, 2007; Traulsen & Tröbs, 2011). Furthermore, once the cloud data governance business case is understood and approved by top management in the organisation, the data governance team can establish and set the criteria for assessing data governance in their organisation. The main activities of the data governance assessment process involve determining the current state of data governance, the mechanisms and the capability of an organisation (Ladley, 2012) to change some of its processes when implementing data governance for cloud computing services. It is necessary to identify the risk and any issues that may emerge when data moves to cloud computing environments. Therefore, the assessment process helps an organisation to measure how well equipped it is in a particular area of data governance or to prepare it for a new effort.

- **Cloud Data Governance Requirements**

Identifying the cloud data governance requirements is an important task in the initial phase, therefore the policies, rules, process and principles of engagement must be outlined in advance (ISACA 2016). Data governance should also be flexible so that it can be expanded or contracted depending on an organisation's needs. The literature does not explicitly refer to this task, but suggests similar concepts within the initial phase of data governance development (IBM, 2007). Designing data governance means tailoring it to an organisation's specific culture, organisational structure and current decision-making processes (Russom, 2008). However, organisations that have strong data governance for on-premises applications cannot depend on its effectiveness in cloud environments. Furthermore, the cloud data governance framework should consider the requirements of data governance for traditional IT computing as well as those specific to cloud computing. In addition, data governance for cloud computing services must include solid rules, because the features offered by the cloud providers vary (Eugene 2013). Therefore, organisations may need to rewrite rules that are no longer adequate when they need to move their data and services to cloud computing environments (Eckerson, 2011; Alkhater et al., 2014). As a result, the rules of data governance are very important for cloud consumers, who must identify their data governance requirements before implementing the transfer.

As a result, the main deliverables of this phase involve the setup of many initial activities to launch the cloud data governance strategy. They involve establishing the structures of a cloud data governance office, building a data governance business case, assessing the current data governance in the organisation, and identifying the data governance requirements for cloud computing services. These activities enable cloud consumers to know their requirements, to take control of their data in the cloud, and to define their target level when they implement data governance for the cloud.

b) Design Phase

This is an important phase in the framework, which aims to design cloud data governance activities. The design phase includes four components: cloud data governance functions (covering issues related to data), integration with cloud computing characteristics, alignment with other strategy efforts in the organisation, and understanding the contractual context. Most of the current research on data governance is focused on some of the components in this phase such as data governance functions and alignment with other strategy efforts in the organisation (Wende & Otto, 2007; Cheong & Chang, 2007; Rifaie et al., 2009). However, the previous studies did not take into account the integration with cloud computing characteristics and the contractual context because they were concerned with internal data governance design. However, the advent of cloud technology means that cloud computing characteristics and the contractual context should be considered in data governance design. Figure 3.23 shows the proposed components of the design phase.

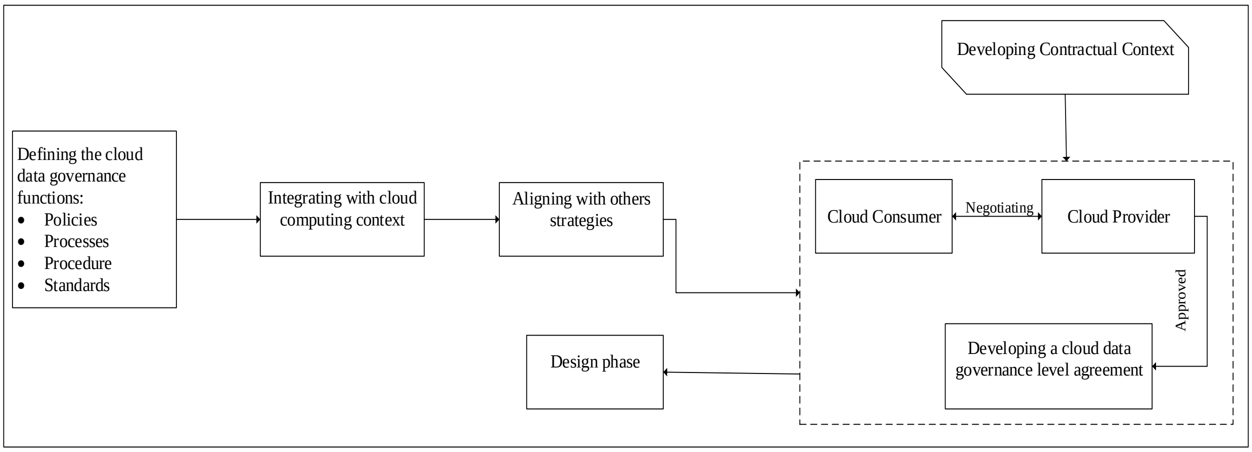

Figure 3.23 The proposed components of the design phase

- **Cloud Data Governance Functions**

Data governance functions relate to the functional areas that the data governance team have to understand and undertake when implementing a data governance programme (Wende & Otto, 2007). Most previous studies show that the data governance functions are the backbone of data governance (Cheong & Chang, 2007; Wende, 2007; Rifaie et al., 2009; Otto, 2011). Thus, the data governance functions play an important role in implementing effective data governance. In cloud data governance, the cloud data governance office will establish the data governance functions based on an assessment report, covering issues related to data in the cloud, such as compliance, transformation, integration, management, accountability, auditability and transparency, and avoidance of conflicts of interest. Therefore, this component involves identifying the data governance functions in order to establish levels of control in the cloud environments, taking account of an organisation's capabilities. The main functions that have been reported in the literature are policy, process, procedure and standards.

- **Integrating with the Cloud Computing Context**

Moving data to cloud computing environments has become a growing trend for many organisations in the last few years (Sengupta et al., 2011). There is, as a consequence, a growing worry about the security, integrity and confidentiality of data stored in cloud computing environments (Sengupta et al., 2011). Existing studies on data governance do not take into account issues concerned with integrating older systems with cloud computing characteristics because they focus on traditional IT and data governance designs internal to organisations. Since the advent of cloud technology, it is important to consider cloud computing characteristics in the cloud data governance design. The main process in this component involves integrating the cloud data governance functions with those relating to the cloud computing context, which includes integration with cloud deployment models (public, private, hybrid, community) and service delivery models (SaaS, PaaS, IaaS) (Bumpus, 2010). The different characteristics of each model will be considered in this component. Thus, this is an important component for implementing data governance in cloud computing environments.

- **Align with Other Strategies**

The main activity is to align data governance functions with other strategy efforts in the organisations that own data (Niemi, 2011). Most previous studies show that the alignment of data governance functions with other strategies in an organisation is important in order to implement effective data governance, and to avoid process errors caused by conflicts with other strategies (Wende & Otto, 2007; Rifaie et al., 2009; Otto, 2011). Previous studies in the literature have considered the importance of alignment with data governance functions such as business strategy, organisational context, technical context, corporate governance and IT governance (Wende & Otto, 2007; Cheong & Chang, 2007; Otto, 2011). On the other hand, other strategies have been ignored in previous studies, which do not consider the design of data governance for the cloud computing environment, including its environmental context (e.g., cloud regulation) and cloud governance. In addition, in this study’s framework, this component aims to align all the strategies in the organisation with cloud data governance functions.

- **Contractual Context**

Developing the contractual context is important for the successful implementation of any project (Joint & Baker, 2011), and it is important to draft an SLA between the cloud consumer and cloud provider (Cochran & Witman, 2011). Previous studies ignore this because they focus on data governance in traditional IT environments and internal operations. In the present framework, the contractual context will be considered as part of the design for data governance for cloud services. The main activity in this component involves developing data governance level agreements between the cloud consumer and cloud provider. It begins with negotiation between the cloud consumer and provider to verify the ability of the latter to achieve the required level of cloud data governance. Thus, this contractual arrangement constitutes an agreement in which the cloud consumer and provider will make their best effort to achieve the cloud data governance objectives. At the end of the process, the cloud data governance level agreements will form part of the SLA.

c) Deploy Phase

This phase involves implementing all the processes of cloud data governance in the real world (Felici et al., 2013). Thus, this phase represents the execution of activities related to the cloud data governance programme. The main aim of this phase is to manage the transformation of data assets that are non-governed so that they become governed. In this phase, many components that are important for completing the implementation of the cloud data governance programme need to be considered. The phase consists of two components: the configuration of the cloud data governance programme and its implementation. In the literature, a few studies refer to the components in this phase, while others do not explicitly refer to them but suggest similar concepts within the initial phase of implementing data governance (Ibm, 2007; Otto, 2011; Groß & Schill, 2012). Figure 3.24 shows the proposed components of the deploy phase.

Figure 3.24 The proposed components of the deploy phase

- **Configuring the Cloud Data Governance Programme**

This component is the first step towards executing cloud data governance in the real world. The main activity in this task involves configuring the cloud data governance activities that are defined in the design phase. Another outcome is the configuring of specific responsibilities for each cloud data governance committee and team.

- **Implementing the Cloud Data Governance Programme**

This component is the final step towards launching the cloud data governance programme in the real world. The main activity involves executing the cloud data governance activities in order to achieve the programme's objective. Therefore, this component helps cloud consumers to manage the transformation of their data assets to the cloud provider's environment, from non-governed to governed (Poor, 2011).

d) Sustain Phase

This phase is crucial for the proposed framework because it aims to enable the sustainability of cloud data governance in the organisation over time. The literature shows that establishing sustainable data governance is a critical factor for the implementation of an effective data governance, and to ensure that data governance continues, improves and remains able to achieve its objectives (Truong & Dustdar, 2012). Some researchers show that this phase never ends, and that it is not really a phase with distinct start and stop dates (Ladley, 2012). There will always be a need to manage the transformation of non-governed data assets in the cloud so that they become governed. In the literature, many tasks have been presented as a means to achieve sustainability in data governance (Rifaie et al., 2009; Traulsen & Tröbs, 2011). The most frequently discussed tasks will be considered in the present framework. In this study's framework, the sustain phase includes four components: identify CSFs, education and training plan, execute the change management plan, and execute the cloud data governance change plan. Figure 3.25 illustrates the proposed components of the sustain phase.

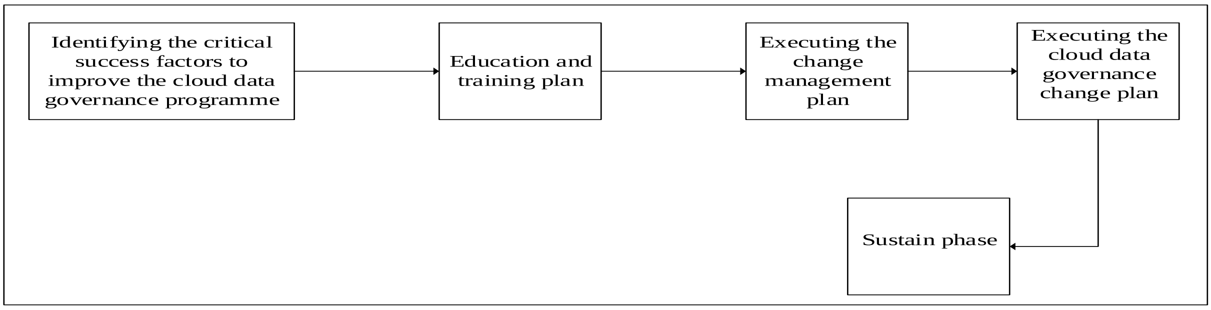

Figure 3.25 The proposed components of the sustain phase

- **Identify Critical Success Factors**

Critical success factors (CSFs) can be defined as "the *factors which if addressed, significantly improve project implementation chances*"(Amberg et al., 2005, p.2). Their identification is the first step in the sustain phase of cloud data governance. Several studies have indicated that the identification of CSFs is very important for effective data governance (Wende & Otto, 2007; Wende, 2007; Traulsen & Tröbs, 2011). The main activities in this component involve identifying the CSFs that need to be addressed to achieve an effective cloud data governance programme, and to help the cloud data governance programme to continue for a long time. The CSFs will need to consider new mechanisms and technology that relate to data governance and cloud computing. Having identified the CSFs, cloud consumers should be prepared to change some processes in their organisation to sustain cloud data governance.

- **Education and Training Plan**

The provision of an education and training plan is an important task to enable data governance to continue and to improve the process (Cheong & Chang, 2007). In the literature, most researchers refer to the training plan as an important task for the education of data governance members and data users on implementation (Cheong & Chang, 2007). In addition, setting up a training plan contributes to sustaining the cloud data governance programme. Education and training plans have to consider distinct levels of training, including setting the stage as well as educating those with a high-level view of data governance. They also need to cover awareness and ability to use cloud data governance policies and procedures, as well as actual hands-on development for use of new procedures and tools (Traulsen & Tröbs, 2011). Over time, educational and training material will require updating; this updating will be based on changes to the cloud data governance programme and cloud computing characteristics (Ladley, 2012).

- **Execute the Change Management Plan**

The change management plan is important when implementing data governance in an organisation, since it will help to align the data governance strategy with other strategies in the organisation (Ladley, 2012). In the literature, many researchers and practitioners suggest implementing a change management plan when applying data governance in organisations (Wende, 2007; Traulsen & Tröbs, 2011). Both sides agree that the execution of a change management plan is important to ensure that data governance continues (Ladley, 2012). The main activity in this component involves developing a formal change management plan for cloud data governance. This will require establishing metrics to measure change and identifying requirements for change (Ladley, 2012). Therefore, the change management plan should be fairly detailed, and should encompass the development of the cloud data governance structures so that the cloud consumer has well-managed data assets in the cloud computing environment.

- **Execute the Cloud Data Governance Change Plan**

The implementation of a change plan for data governance is important in order to improve and sustain current data governance in an organisation. In the literature, some studies recommend that the data governance team should implement plans to ensure that data governance is achieved in the right way and that it achieves its objectives (Truong & Dustdar, 2012). Therefore, the main activity in this component involves defining the change plan for cloud data governance. This change plan will be based on the requirements and elements that need to be addressed in order to ensure that cloud data governance is sustainable. In cloud data governance, many elements will need to be addressed, such as updating the cloud data governance functions based on an assessment of data risks in the cloud environment, improving and changing the cloud data governance level agreement between the cloud consumer and provider, training, monitoring, and ensuring a positive culture.

In sum, the main deliverables of this phase involve activities that help cloud consumers to sustain and improve cloud data governance. These are identifying the CSFs, developing an education and training plan, executing a change management plan, and executing a data governance change plan.

e) Monitor Phase

This phase is a significant phase in the proposed framework; it aims to support the monitoring of cloud data governance efforts, to ensure that all incoming and existing data in the cloud environment meet the cloud data governance rules. It also aims to ensure that the cloud provider considers and enforces the cloud data governance rules and requirements, and that cloud data governance is heading in the right direction. In the literature, most studies show that the monitoring of data governance activities will greatly enhance data quality and improve data management (Wende & Otto, 2007; Cheong & Chang, 2007; Wende, 2007; Fernandes et al., 2014). The outputs of the monitor phase (e.g. reports, alerts etc.) will allow the cloud consumers greater insight into the areas and processes that reduce the quality of data. This then highlights areas of focus in order to improve the processes. The monitor phase in the proposed framework will consider all the procedures that are in the other framework phases. Therefore, cloud consumers have to establish monitoring mechanisms and tools to ensure that they can maintain high levels of cloud data governance on an ongoing basis. There are two components that are considered in the monitor phase: metrics & KPIs, and tools. Figure 3.26 shows the proposed components of the monitor phase.

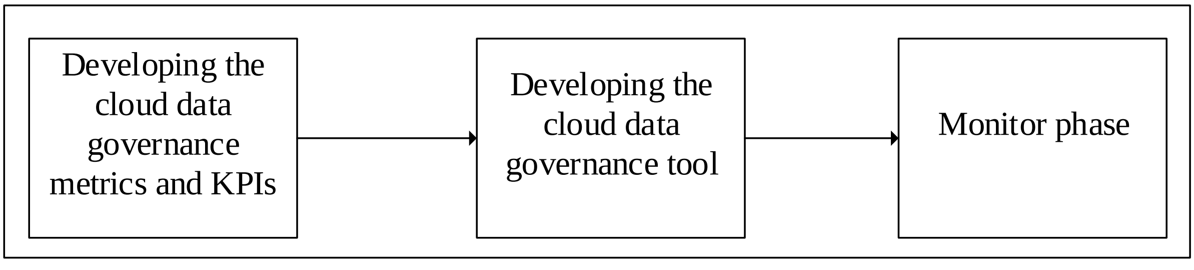

Figure 3.26 The proposed components of the monitor phase

- **Metrics and KPIs**

Data governance cannot be managed without reliable metrics (Rifaie et al., 2009). Therefore, those involved in cloud data governance will need to develop a means to monitor their own effectiveness. The main activities in this component involve developing the metrics and KPIs for cloud data governance. The metrics and KPIs will evolve from simple surveys and the assembling of simple statistics for true monitoring of data governance activity in the cloud environment. The focus should be on the assessment of the various elements of data governance, and a range of data issues in cloud computing.

- **Cloud Data Governance Tool**

The selection of technologies used for monitoring cloud data governance is important. In the literature, most studies suggest that not only is designing a monitor tool important, but that these tools should be based on modern technology (Wende, 2007; Fernandes et al., 2014). Some work even suggests that monitoring cloud data governance in the organisation requires the latest technology (Shimba, 2010). However, the literature does not consider technology devoted to monitoring cloud data governance. Therefore, the main activity in this component involves developing an automated tool to monitor the activities of the cloud data governance programme. This tool should be based on modern technology compatible with cloud computing technology. The cloud data governance tool should consider the many activities of cloud data governance such as administration of the cloud data governance functions, administration of rules and responsibilities, and workflow for addressing cloud data governance issues and audits. Therefore, this tool will help cloud consumers to achieve an effective cloud data governance programme and make the correct decisions.

3.7.2. Holistic Framework to Design, Deploy and Sustain Cloud Data Governance Programme

The framework phases and their components were already discussed and described in detail in section 3.7.1. The organisations require a holistic framework to understand the important processes that help their decision makers to develop an effective cloud data governance programme. Therefore, this research therefore adopts a holistic view to develop a strategy framework for cloud data governance that covers all phases and their components. Figure 3.27 presents the proposed strategy framework for cloud data governance, which includes the main phases of the framework and their components.

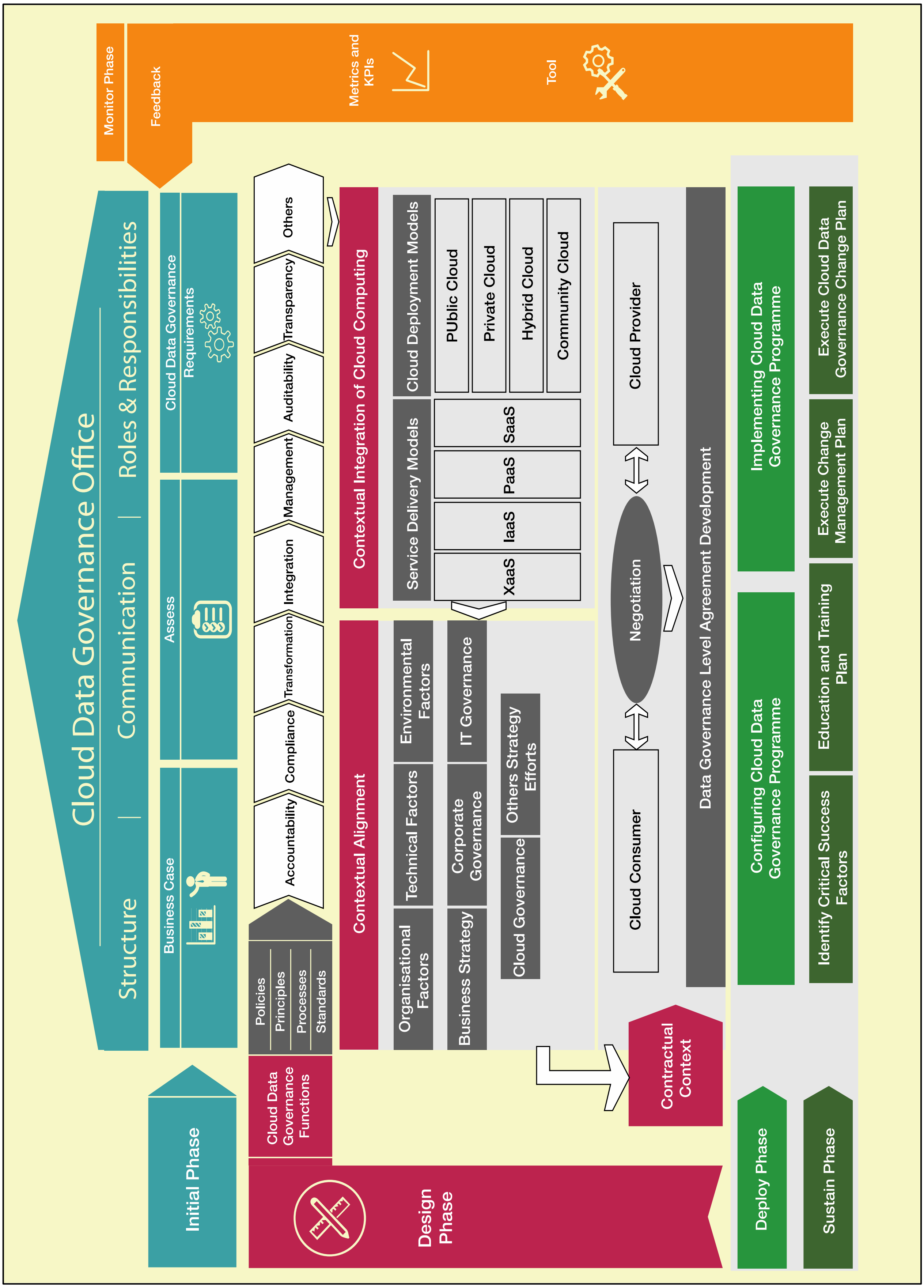

Figure 3.27 The proposed strategy framework for cloud data governance

3.8. Managing the Proposed Framework Implementation

The proposed framework was developed based on five major phases, and each phase has important components. The proposed process is illustrated in Figure 3.28.

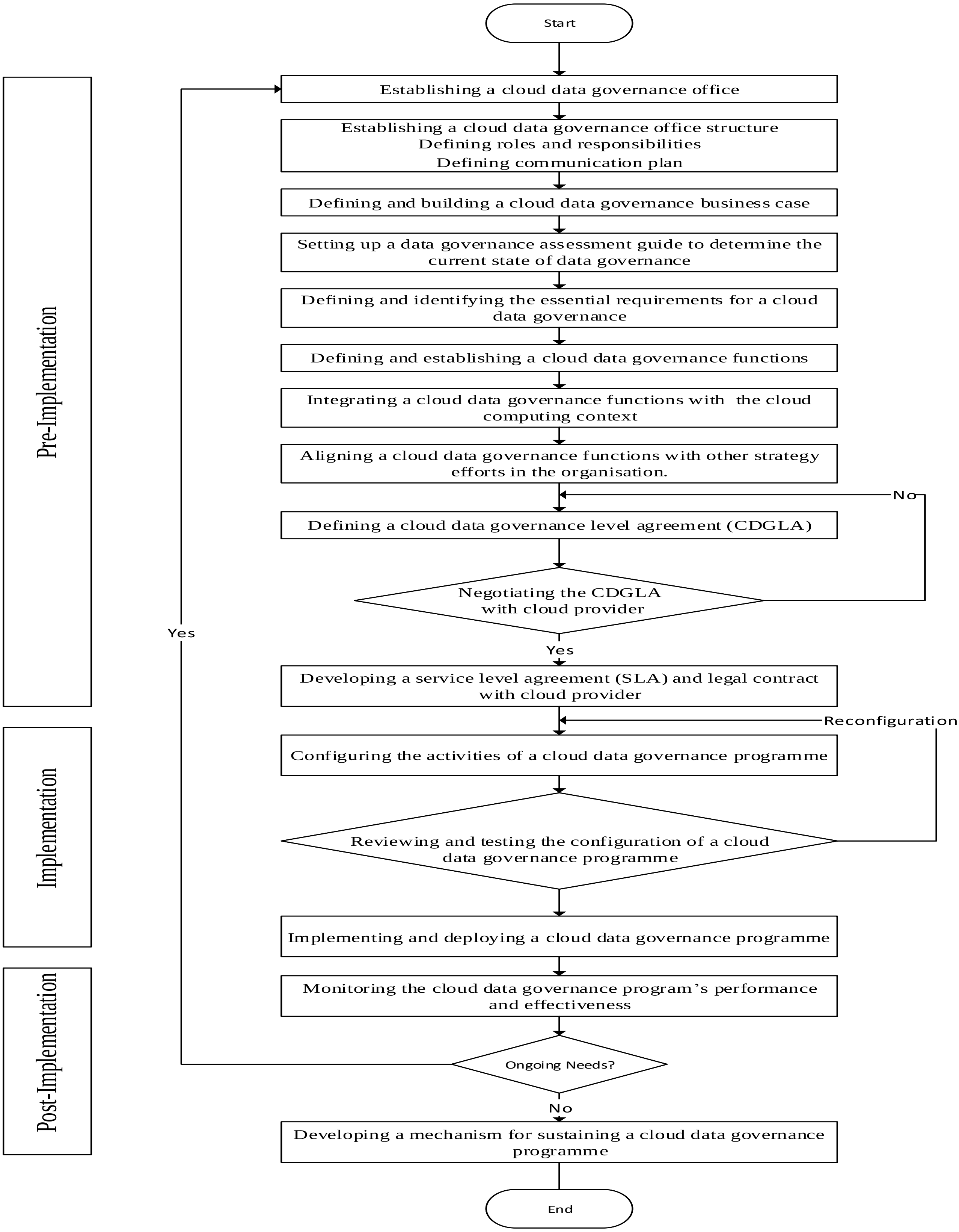

Figure 3.28 Stages to implement the cloud data governance framework

The management and implementation of this framework is a very important factor in securing the desired results. In this study, we propose a process for the successful implementation of the proposed framework. This process will be based on three stages: pre-implementation, implementation and post-implementation, and these are discussed below:

a) Pre-Implementation Stage

This stage refers to the preparation for the implementation of the proposed cloud data governance framework. Many factors should be addressed in this stage to ensure that the cloud data governance project is ready for implementation in the organisation. This stage covers the initial and design phases of the proposed framework, and its steps are described below:

Step 1**:** Establishing a cloud data governance office responsible for defining cloud data governance requirements in organisations and monitoring cloud data governance implementation.

Step 2: Establishing the structure for the cloud data governance office and identifying roles and responsibilities for the cloud data governance office teams or members. Additionally, in this step, the communication plan between the cloud data governance office teams or members should be addressed to create an effective office in the organisation. Thus, cloud data governance needs members that are involved in its structures; they may be cloud managers, cloud provider members and cloud brokers. In addition, in order to build the best cloud data governance office structure, the organisation should have classified representative groups involved in cloud data governance operating at three levels, namely strategic, tactical and operational.

Step 3: Defining and building the cloud data governance business case to understand the value that cloud data governance can bring to the organisation (Eugene, 2013). The business case for cloud data governance will be concerned with the organisation's ability to alter age-old perceptions, to show the holistic impact of cloud data governance. It will try to persuade top management that this will lead to change outcomes through an improved business process. There are many steps that should be considered in the cloud data governance business case, such as the data governance vision and mission, the cost of data governance, and its benefits and risks.

Step 4: Setting up a data governance assessment guide to determine the current state of data governance, mechanisms and the capability of an organisation to change some of its processes when implementing cloud data governance (Huang & Nicol, 2013). Evaluating and identifying the risks and issues relating to data when it moves to a cloud computing environment form part of the assessment procedure (Catteddu & Hogben, 2009). In this step, the organisation (cloud consumer) also should assess its cloud data governance based on a cloud data governance maturity model to determine its current level and its target level for the cloud data governance programme.

Step 5: Defining and identifying the essential requirements for cloud data governance. Identifying all requirements before implementing the cloud data governance programme is very important (Mell & Grance, 2011), and the cloud data governance requirements should be tailored to the organisation's culture, organisational structure, requirements, budget and current decision-making processes.

Step 6: Defining and establishing the cloud data governance functions. The data governance functions refer to master activities for data governance (Loshion, 2007), which data governance committees have to take into account when implementing the cloud data governance programme. The cloud data governance functions consist of many activities, namely the devising of policies, principles, process and standards, and determining who has the rights to make key decisions (The Data Governance Institute, 2015). Setting up the cloud data governance functions (good standards and practices) will help cloud consumers to gain control of their data in the cloud environment. Cloud business objectives and risks related to their data in the cloud environment should be considered when setting up the cloud data governance functions. Therefore, it is important that the organisation (cloud consumer) establishes the cloud data governance functions at the very first stage before choosing a cloud provider as this will lead to an effective cloud data governance programme.

Step 7: Integrating the cloud data governance functions that have been defined in the previous step within the cloud computing context. The integration should be focused on integrating the characteristics of the cloud deployment models (public, private, hybrid, community) and service delivery models (SaaS, PaaS, IaaS) (Mell & Grance, 2011). This step is important to ensure that the consumer's data is well governed in the different cloud deployment and delivery models.

Step 8: Aligning the cloud data governance functions with other factors in other strategy efforts in the organisation. This alignment will help cloud consumers to achieve an effective cloud data governance strategy and programme (Lui, 2011). Thus, the cloud data governance strategy becomes one of several important strategies in the organisation (Cloud Security Alliance, 2015b). Any new strategy adopted in the organisation at a later point should align with the cloud data governance strategy.

Step 9: Defining the cloud data governance level agreement, which includes the cloud data governance requirements, before negotiating and developing a legal contract with the cloud provider.

Step 10: Negotiating a cloud data governance level agreement with the cloud provider. In this step, the cloud consumer informs the cloud provider of its requirements for the cloud in general and, more specifically, for data governance, before moving its data to the cloud provider's environment (Cochran & Witman, 2011). The cloud consumer should understand all the factors that may influence the negotiation before starting it. For example, they should understand the complex infrastructure of negotiations, and be aware of the context of the negotiation and negotiation culture. It is important that legal teams on both sides (consumer/provider) are fully involved in the negotiation. In sum, all data governance policies will need to be negotiated between the cloud consumer and provider in order to identify the target level of data governance before the contract is written.

Step 11: Developing an SLA and legal contract with the cloud provider; the cloud data governance requirements should be included in the SLA.

b) Implementation Stage

This stage refers to the cloud provider implementing and deploying the cloud data governance programme in real time. It involves executing the activities related to cloud data governance and managing the transformation of non-governed data assets so that they become governed data assets. Many factors should be addressed in this stage to implement the cloud data governance programme. This stage covers the deploy phase in the framework. The implementation steps are highlighted below:

Step 1: Configuring the activities of the cloud data governance programme so that they are consistent. The cloud provider should configure the cloud data governance functions that have been defined in the SLA.

Step 2: Reviewing and testing the configuration of the cloud data governance activities before implementing the cloud data governance programme in real time.

Step 3: Implementing and deploying the cloud data governance programme in real time, and managing the transformation of the cloud consumer's non-governed data assets into governed data assets.

c) Post-Implementation Stage

This stage refers to monitoring and following up, in order to make continuous improvements towards the success of the cloud data governance programme. This stage involves monitoring the performance and effectiveness of the cloud data governance programme and ensuring that it can be sustained in the long term. There are many factors that should be addressed in this stage to implement the cloud data governance programme. This stage covers the monitor and sustain phases in the framework. The post-implementation steps are highlighted below:

Step 1: Setting up activities for monitoring the cloud data governance programme's performance and effectiveness. This step aims to ensure that the cloud data governance functions and requirements are enforced by the cloud provider as set out in the data governance level agreement; it also ensures that the cloud data governance is heading in the right direction (Pearson et al., 2012). In this step, the cloud consumer should develop a tool, matrices and KPIs to present the monitoring results.

Step 2: Setting up activities and developing a mechanism for sustaining the cloud data governance programme. This step aims to ensure the continuity of the cloud data governance programme, and to see that improvements are made in order to achieve its objectives.

3.9. Chapter Summary

This chapter presents one of the core contributions of this thesis, i.e. a strategy framework to design, deploy and sustain an effective cloud data governance programme. This chapter starts by defining the theoretical foundations, which were the analytic theory and CSF concept, and the proposed framework aim was also outlined in this chapter. The data governance taxonomy and key dimensions for data governance in cloud and non-cloud environments were considered and presented in this chapter before developing the framework. Then, the existing data governance frameworks were analysed based on the key dimensions of cloud data governance and the results were described in this chapter. Five phases of the framework, which were the initial phase, design phase, deploy phase, monitor phase and sustain phase and their components were presented and discussed in detail based on the literature review. Then, the proposed framework was developed in this chapter based on these phases and their components. Finally, the steps for implementing the proposed framework were also presented in this chapter. The following chapter will discuss and present the cloud data governance maturity model and its assessment matrix development.

Chapter 4. Cloud Data Governance Maturity Model & Assessment Matrix

4.1. Introduction

To recall, loss of data governance is cited as one of the main concerns for organisations when considering moving their data to cloud computing (Tountopoulos et al., 2014; Jones et al., 2017). In Chapter Three, a strategy framework to understand how to design, deploy and sustain an effective cloud data governance programme was developed. It is important, however, to develop tools to assess the utility of the strategy framework. Therefore, this chapter aims to develop a maturity model and an assessment matrix as an approach.

The results of the systematic literature review in Chapter Two show that there seems to be a lack of research in the field of data governance in general and cloud data governance in particular, linked to maturity models and assessment matrices. While there are a few data governance maturity models in the literature, these models do not cover the important features in cloud computing and some changes are required to assess the data governance for cloud services. Thus, this chapter aims to enrich the research area and to develop a new approach for organisations that will enable them to achieve their cloud data governance effectively and efficiently. In addition, this research aims to provide a contribution for developing managers, professionals and any person interested in the study of cloud data governance by providing a roadmap and models of best practice in order to improve their cloud data governance programmes. Therefore, this research aims to develop a new maturity model and assessment matrix for cloud data governance. It also provides a methodology and new concept for an organisation to develop an improved roadmap for its cloud data governance by reaching a specified maturity level.

The concept of a maturity model has been applied within the field of Information Systems for several decades (Frick, 2012). Maturity approaches came from the field of quality management and were extended to the IT field in order to manage software development (Crowston & Qin, 2010). The maturity model can be considered as a measurement model that allows organisations to evaluate their capabilities with regard to a certain problem area (Blommerde & Lynch, 2016). In the literature there are a few data governance maturity models (Adler, 2007; Nascio, 2009) and the literature shows the great interest shown by industry in data governance maturity models. There is also an absence of maturity models for data governance in academic research, as developing the data governance maturity model for cloud computing required incorporating some important features related to cloud computing. However, the existing data governance maturity models ignore these features. Therefore, the existing maturity models do not solve this study's research problem since they are focused on data governance for non-cloud environments. It is clear from the above that there is a need for a maturity model that includes all the best practices and all the aspects of data governance for cloud computing, which are not included in the current maturity models. This chapter presents, for the first time, a cloud data governance maturity model; it takes account of the range of dimensions in the cloud data governance framework that support an organisation to implement a cloud data governance programme. These dimensions will also be described based on the levels of the maturity model. In addition, based on the cloud data governance maturity model concept, a cloud data governance assessment matrix will be developed as a tool to measure the current state of the cloud data governance in organisations.

4.2. Study Findings of the Systematic Literature Review

Maturity models are widely used by information system domains. In order to achieve the aim of this chapter, which is to develop a cloud data governance maturity model, the state of maturity models in information systems (IS) research is investigated. The systematic literature review guidelines as proposed by Kitchenham and Charters (2007) were used to identify the maturity models. Five research questions were developed, and they aimed to generate a comprehensive overview of maturity model research, especially with regard to research designs, research methods and the theoretical foundations of the existing maturity models. The maturity model domains and methods for validating maturity models were considered in these questions (see Appendix B for more details). Based on the systematic literature review process, 89 articles published in leading Information Systems (IS) journals and conference proceedings during the past six years were collected and analysed. The majority of the articles (58) have been published in journals, and 31 were presented at conferences. The results show that the research on maturity models generally increased during the period 2011-2014: there were 19 articles in 2011, 18 articles in 2012, 26 articles in 2013, 17 articles in 2014, and only nine articles in the whole of the last three years, from 2015 to 2017 (see Figure 4.1).

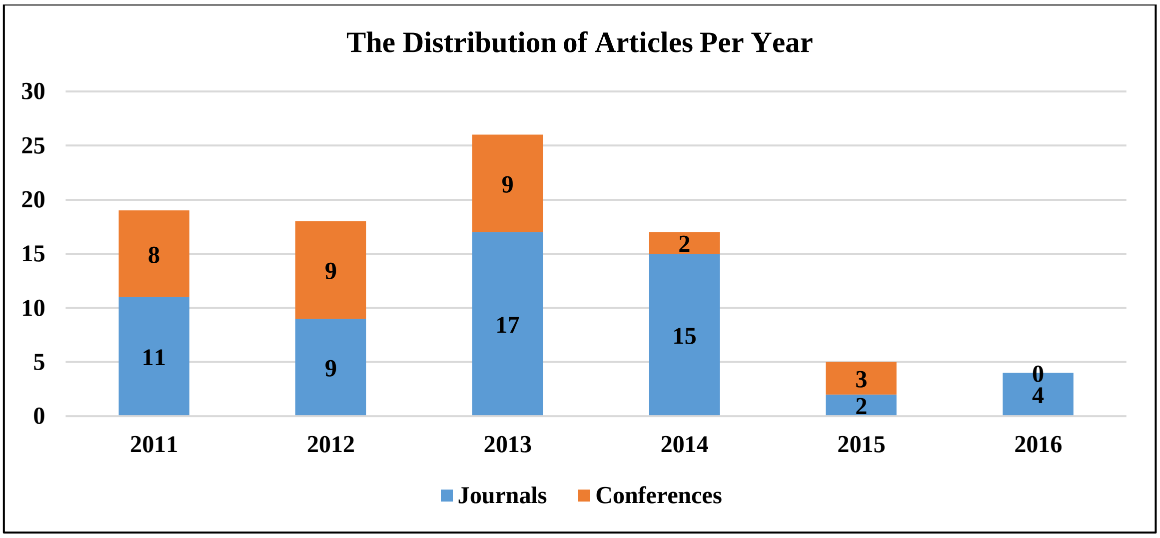

Figure 4.1 The distribution of articles across journals and conferences per year for maturity models development in IS research

Looking at research question 1 (RQ1), which focuses on the research designs applied to develop the existing maturity models, the study shows that most of the maturity models were developed based on an empirical research design (40 articles). A design-oriented approach was also used to develop maturity models: 18 articles were based on a design science research approach. In addition, a conceptual research design was considered in the development of maturity models in many (29) articles (see Figure 4.2).

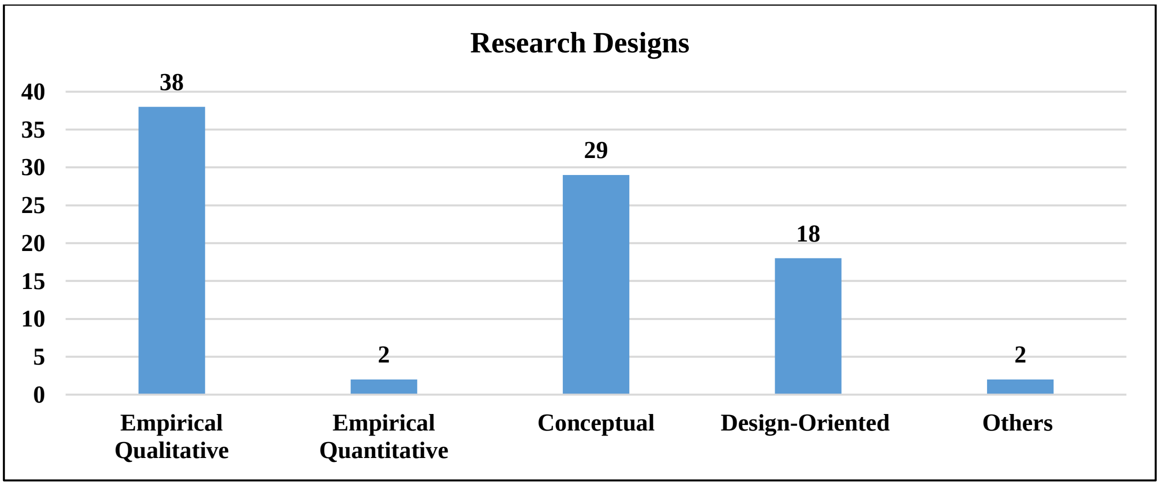

Figure 4.2 Number of articles per research design for developing maturity models in IS research

As for RQ2, which focuses on the research methods applied by the researcher to develop the existing maturity model, the results in Figure 4.3 show that nine methods were applied in the literature to develop the existing maturity models. The literature review method was the main method considered to develop the existing maturity models; it was used in 49 articles. Thirty-eight articles were based on other methods: concept development, workshop, focus group, action research and the Delphi method. Finally, the other 12 articles were based on mixed methods.

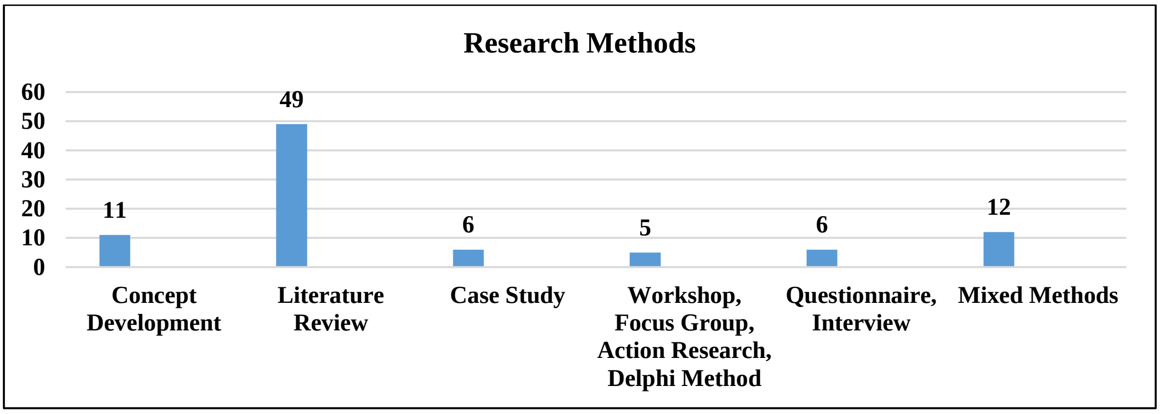

Figure 4.3 Number of articles per research method for developing maturity models in IS research

Furthermore, the theoretical foundations that were used by the existing studies in the literature for developing the maturity models were looked at in RQ3. The literature analysis results show that most of the articles (54 articles, 61%) used existing maturity models as the theoretical foundation, and the other 35 articles (39%) were based on concept construction as the theoretical foundation (see Figure 4.4).

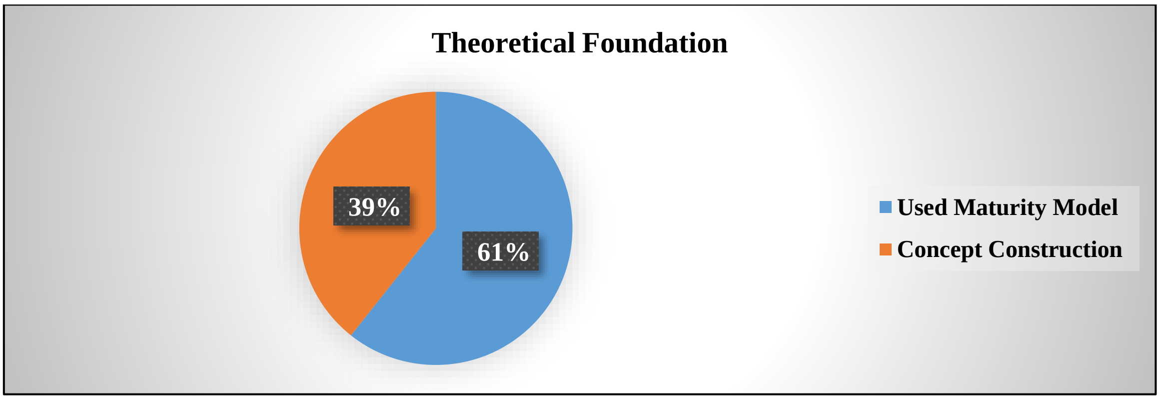

Figure 4.4 The number of articles based on the theoretical foundation classification for developing maturity models in IS research

The literature suggests that the Capability Maturity Model (CMM) and it successor the Capability Maturity Model Integration (CMMI) are the main domain foundations of existing maturity models in information systems (25 articles). However, 10 articles developed maturity models based on other maturity models: ISO, CobiT, SOA, SSE-CMM, OPM3 and NIMM (see Figure 4.5).

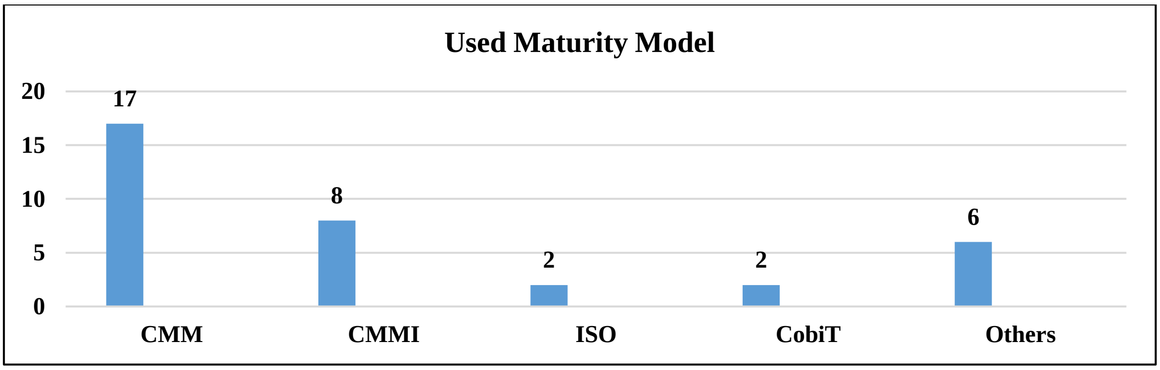

Figure 4.5 The numbers of articles that used existing maturity models for developing maturity models in IS research

In addition, maturity models' validation has been considered in this study in RQ4. This question aims to discover whether the existing maturity models have been validated and how they are validated to fit their purpose. The percentages quoted show that 51% of the maturity models were not validated whilst 49% were validated (see Figure 4.6).

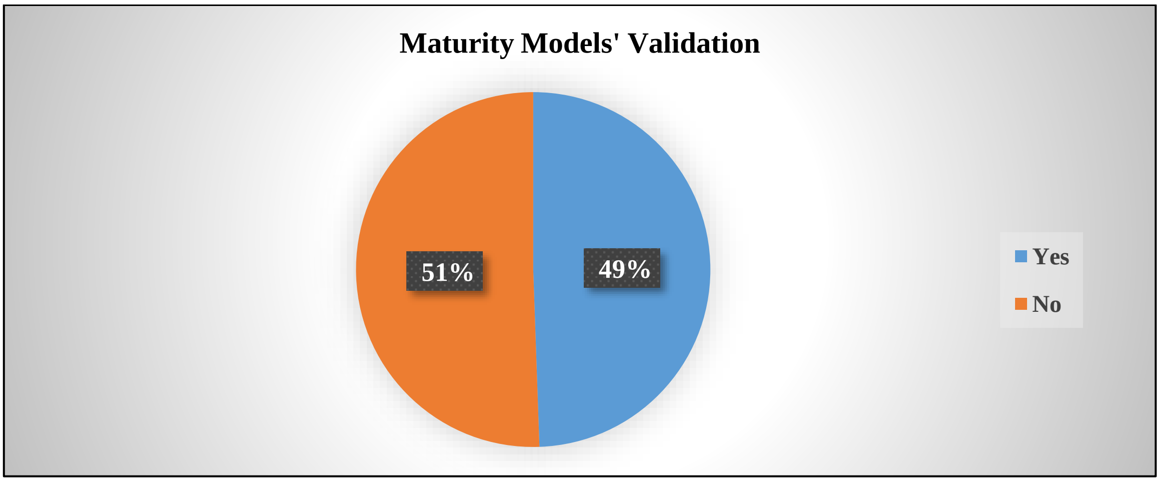

Figure 4.6 The number of articles that validated or did not validate the maturity models in IS research

Regarding the methods that were used to validate the existing maturity models, the literature shows that the case study and interview were the main methods used: 11 articles validated the maturity models by case study, and 11 articles by interview. The other articles validated their maturity models based on surveys, questionnaires, focus groups, workshops and others (see Figure 4.7).

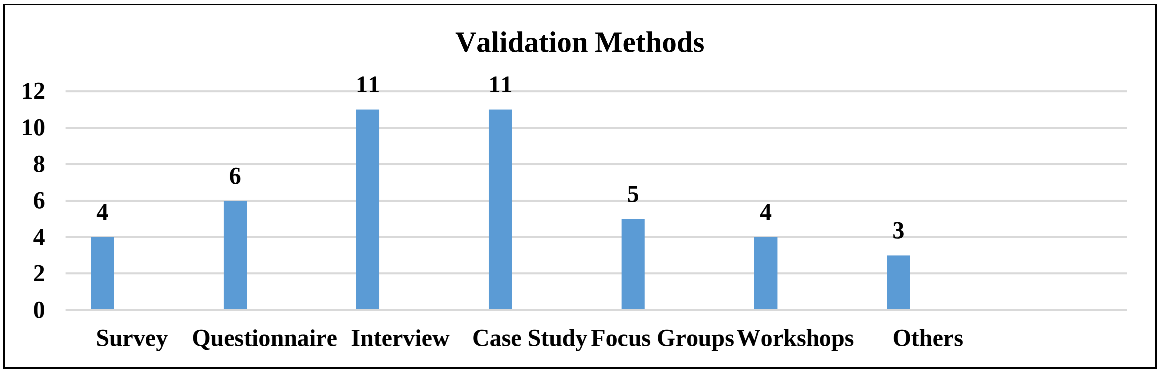

Figure 4.7 The validation methods for maturity models in IS research

Regarding the question about maturity model domains (RQ5), the study discovered a variety of approaches to maturity model research in the information systems domain. The most common domains in these articles were: e-government, software development, project management, mobile learning, cloud computing, governance, risk management, compliance, information security, IT governance, interoperability, collaboration, business intelligence, telemedicine and knowledge management (see Figure 4.8).

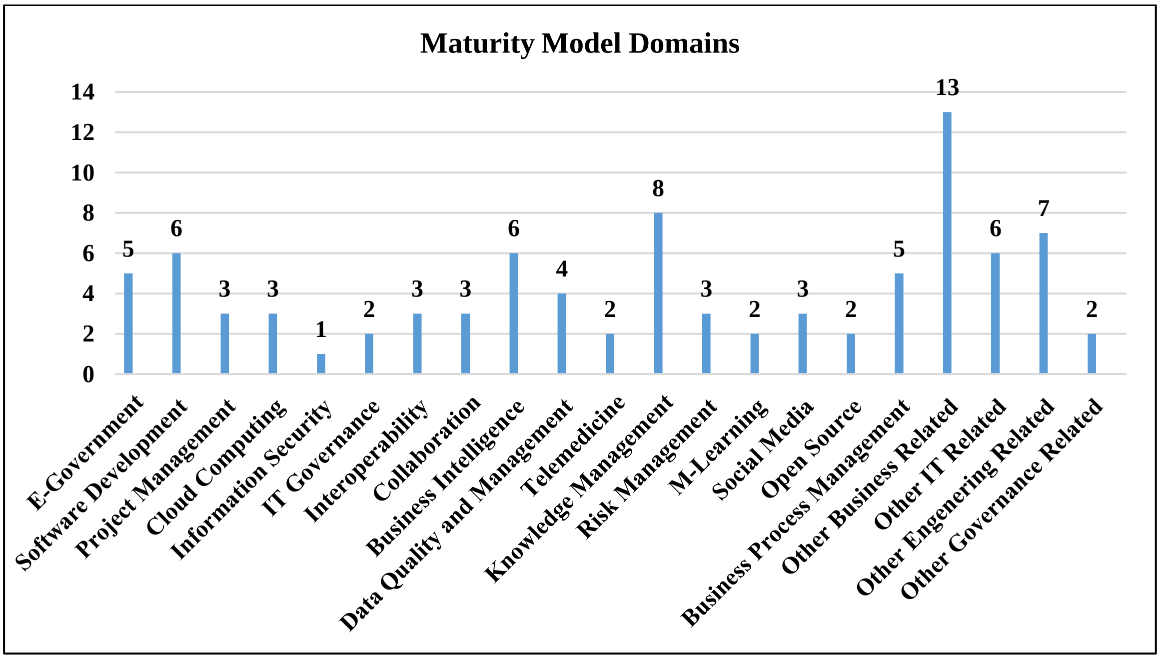

Figure 4.8 Number of articles based on maturity model domains in IS research

4.3. Cloud Data Governance Maturity Model

The concept of a maturity model is an approach used for organisational assessment and development (Saleh, 2011). The maturity model defines a pathway of improvement for the processes of organisational aspects (Frick, 2012). It is classified by a number of maturity levels; these levels often range from one to five, where one is a lack of maturity and five is fully mature (Debreceny & Gray, 2013). This path will assist in enabling the organisation to become mature. According to Wibowo & Waluyo (2015, p.90), maturity generally can be defined as "*the state of being complete, perfect or ready".* Therefore, maturity models allow an organisation to evaluate its capabilities with regard to a certain problem area (Hamel & Herz, 2013). In this research, the maturity model aims to define a pathway to improve the cloud data governance processes in organisations. The cloud data governance Maturity Model is intended as a tool to evaluate the organisation's ability to implement data governance for cloud computing services. This model defines important processes to manage, measure and control all aspects of cloud data governance in organisations, based on the construction of a framework for cloud data governance that was developed in Chapter Three. It also considers a tool for assessing the current state of cloud data governance awareness and effectiveness in the organisation. Through this model, organisations can evaluate current gaps in their cloud data governance practices and define new opportunities for implementing cloud data governance, based upon observable behaviours. In addition, this model enables organisations to:

- Assess where they currently are, where they want to be and the steps they need to take to get there in terms of cloud data governance.
- Gain an informed, objective, documented assessment of the maturity of their organisation with regard to cloud data governance.
- Objectively identify, uncover, highlight and detail the strengths and weaknesses of their cloud data governance capabilities.
- Gain knowledge of existing capabilities and levels of understanding around processes relating to cloud data governance dimensions.
- Challenge internal assumptions and normalise methods for persistently examining cloud data governance processes and practices.
- Define future levels for improving cloud data governance and develop a roadmap to govern more effectively across the organisation.

The cloud data governance maturity model will contribute to organisations' understanding of their current position with regard to cloud data governance implementation and it will enable them to identify their future path. This contribution will be achieved by classifying the activities of the cloud data governance framework components or dimensions based on the five maturity levels. These levels range from one to five, where one is a lack of maturity and five is fully mature.

4.4. Cloud Data Governance Maturity Model Development

To recall, the results of the systematic literature review in section 4.2 show that some of the existing maturity models in the literature were developed based on the concept construction of their area as the theoretical foundation. Therefore, the conceptual construction of cloud data governance has been chosen as the theoretical foundation to develop the cloud data governance maturity model in this chapter.

This study follows three phases to develop the proposed maturity model construction, namely: pre-design, design and post-design. Each phase of the maturity model development will achieve its goals by following a process. Figure 4.9 shows the roadmap to develop a cloud data governance Maturity Model.

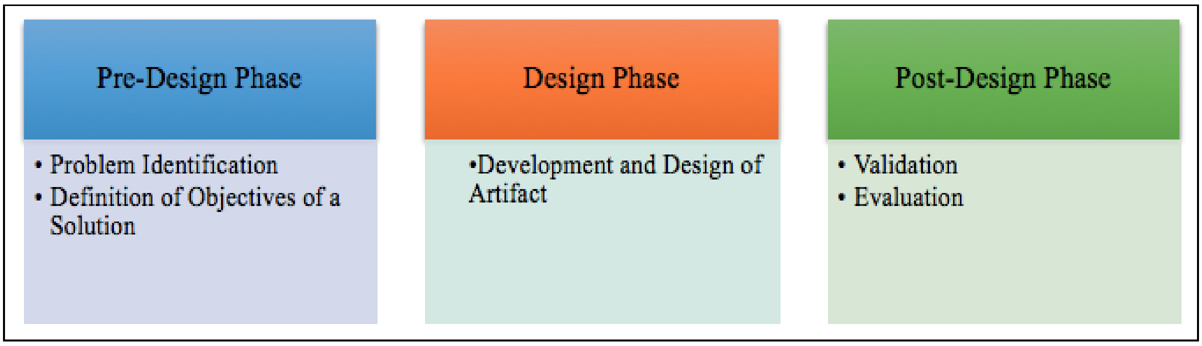

Figure 4.9 Roadmap for constructing the cloud data governance Maturity Model

4.4.1. Pre-Design Phase

The pre-design phase is the initial phase in building the cloud data governance Maturity Model. This phase helps to gain an understanding of the research problem and objectives, and it has two steps: problem identification and definition of objectives for a solution.

- **Problem Identification**

This step specifies the research problem and gaps; this study uses a literature review technique to identify the research problem and research gaps related to cloud data governance. To identify the research gaps, this study reviewed the existing studies related to maturity models to understand the maturity model concept, the state of the problem and the available solutions. Therefore, based on the systematic literature review results in Chapter

Two and in this chapter, there seems to be a lack of research in the field of data governance in general, and cloud data governance in particular, linked to the maturity models and assessment matrices. The results show industry has developed three maturity models related to data governance, and that there are no maturity models for cloud data governance. Victor, (2016, p.23) stated that an "*organization also experiences lack of awareness on the governance mechanism with only a few of the individuals within an organization being aware of the data governance mechanisms*". Therefore, cloud data governance maturity models are useful to measure and assess the current state of cloud data governance implementation in organisations.

- **Definition of Objectives for a Solution**

This step provides a definition of the research goal and objectives of the cloud data governance Maturity Model, which in this study is developed to fill the existing research gap. This model is a solution in this study, which aims to measure cloud data governance in organisations. The maturity model will consider the framework presented in Chapter Three as a theoretical foundation. The maturity model design will be discussed in the next section.

4.4.2. Design Phase

This phase aims to design the maturity model for cloud data governance. In the literature, the majority of the existing maturity models were developed based on two components in order to achieve their goals: dimensions and maturity levels (Ryu et al., 2006; Saleh, 2011; Fath-allah et al., 2014). In this research, the proposed cloud data governance Maturity Model was developed based on three components: outcomes, dimensions and maturity levels.

- **Development and Design of Artefact**

This step aims to describe the proposed maturity model of cloud data governance and its components. The development of the maturity model is built upon three steps. Firstly, the maturity model outcomes need to be identified. Secondly, the maturity levels used to measure the dimensions need to be defined and named in order to fit with the data governance concept. Finally, the maturity model will be built upon the framework dimensions that were presented in Chapter Three. The architecture of the cloud data governance Maturity Model is illustrated in Figure 4.10. The components of the cloud data governance Maturity Model are explained below.

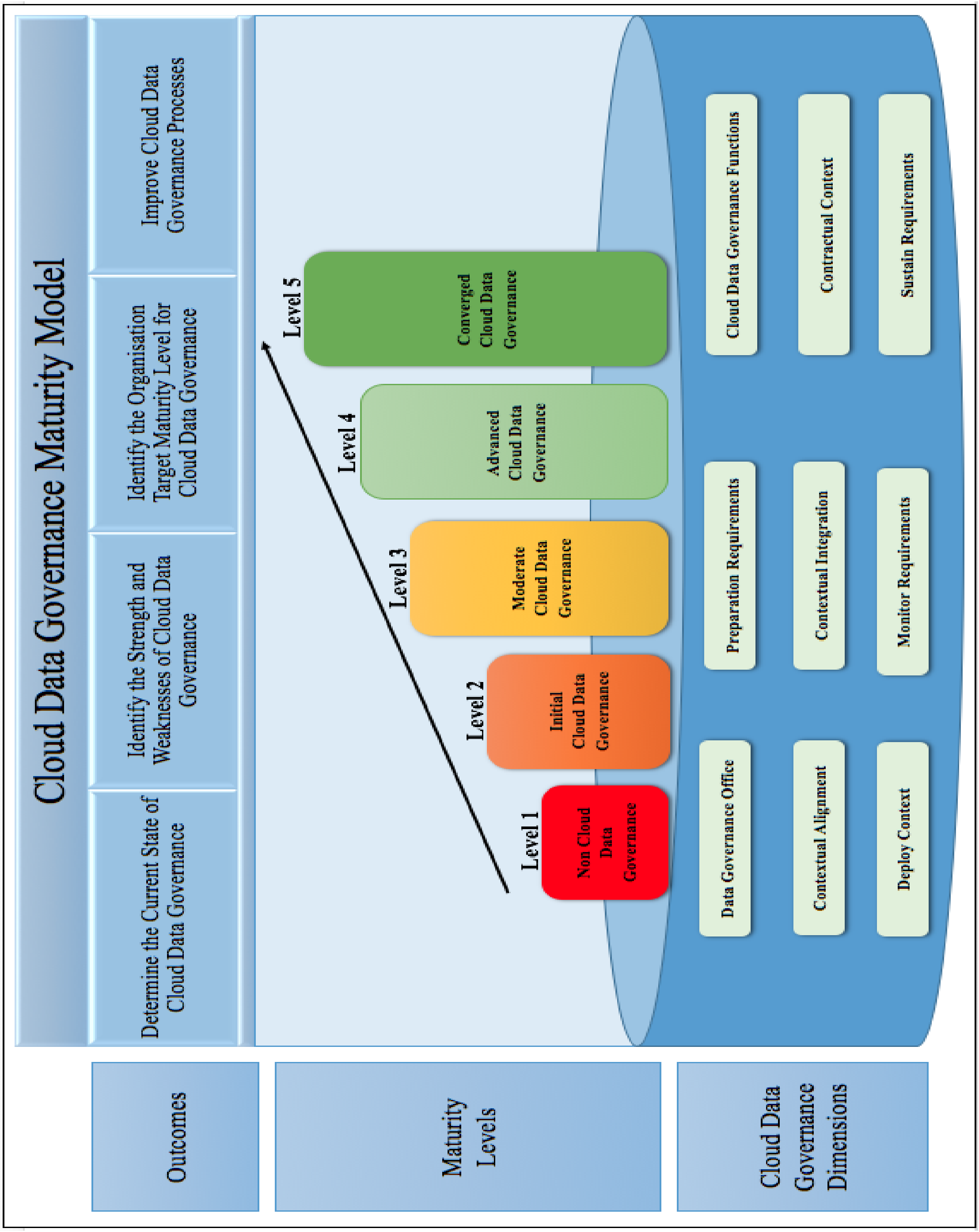

Figure 4.10 Cloud data governance Maturity Model architecture

a) Outcomes

This component refers to expected outcomes; which will be achieving by implementing the cloud data governance maturity model. In the literature, there are some common expected outcomes among existing maturity models. Therefore, the cloud data governance Maturity Model was developed in this research to enable organisations to achieve important outcomes that help them to achieve maturity for their cloud data governance programme. The expected outcomes are highlighted in Figure 4.11 and are outlined below.

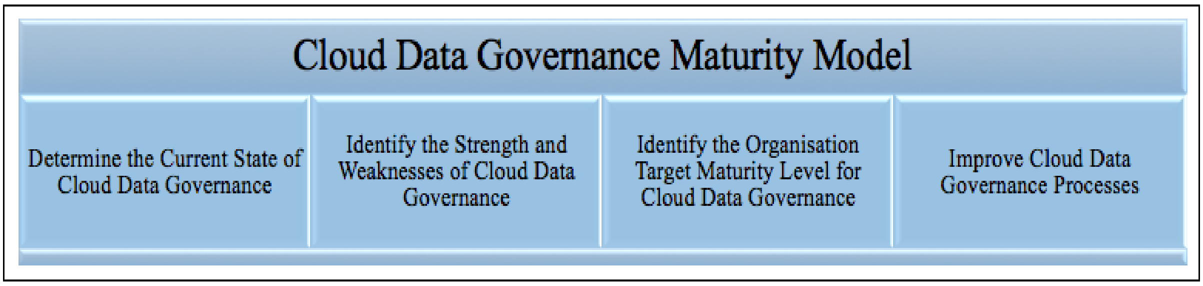

Figure 4.11 Cloud data governance Maturity Model outcomes

- **Determine the Current State of Cloud Data Governance**

Data governance is one of the most important components of the cloud computing strategy for any organisation; thus, an organisation should determine the current state of its cloud data governance and identify any gaps (Hoying, 2011). One of the most important outcomes in this model is allowing organisations to determine and assess the current state of their cloud data governance. Therefore, the expected outcome of this component will help organisations to update and improve their cloud data governance programme in the future to achieve their targets.

- **Identify the Strengths and Weaknesses of Cloud Data Governance**

One of the cloud data governance maturity model's outcomes is that it allows an organisation to identify the strengths and weaknesses of its cloud data governance programme. Strengths and weaknesses are concerned with the positive and negative aspects of the cloud data governance that are under direct control of the organisation or a decision maker. Therefore, to achieve an effective cloud data governance programme, the organisation must determine the strength and weakness factors as well as the opportunity and threat factors that affect its cloud data governance(Rivera et al., 2017). After determining the current state of its cloud data governance, the organisation can identify the strengths and weaknesses of its cloud data governance.

- **Identify the Organisation's Target Maturity Level for Cloud Data Governance**

The cloud data governance Maturity Model will describe the overall maturity levels and the maturity level for each cloud data governance dimension. Based on the organisation's requirements and the current state of the cloud data governance, the target cloud data governance maturity level will be selected. Once the level and dimensions are defined and assessed, the next step is to determine the organisation's target maturity level for each dimension (Saleh, 2011; Rivera et al., 2017). Therefore, not all dimensions of the cloud data governance should operate at the highest level of maturity. The organisation may not want to expend the resources to move those dimensions to a high level of maturity and will accept the risk that the cloud data governance objectives have a higher probability of failure as a result.

- **Improve Cloud Data Governance Processes**

Loss of data governance is still considered the top risk associated with moving to the cloud (Hsu, 2012). In using cloud computing infrastructures, the client necessarily cedes control to the cloud provider on a number of issues that may affect security (Rebollo et al., 2014). At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences (Catteddu & Hogben, 2009). With an effective data governance programme, organisations can take control of their data in the cloud environment. The data governance programme requires the alignment of the cloud data governance dimensions to improve its process and ensure its efficiencies. Therefore, when organisations implement the cloud data governance maturity model, it will help them to improve their cloud data governance processes by understanding their position and discovering new opportunities.

b) Cloud Data Governance Maturity Levels

In the proposed cloud data governance Maturity Model, the maturity levels define a scale for measuring the maturity of an organisation's cloud data governance and for evaluating the capability of its cloud data governance process. It is difficult for cloud computing practitioners and decision makers to know what level of data governance they are achieving with their investments in cloud data governance (Owuonda & Orwa, 2016). It is even harder to estimate how well these investments can be expected to protect their data in the future, as data protection policies, regulations and the threat environment are constantly changing (Saleh, 2011). Therefore, this leads an organisation to develop a cloud data governance Maturity Model that allows it to have its practices, processes and methods evaluated against a clear set of artefacts that establish a benchmark (Caralli et al., 2012). These artefacts typically represent best practice and may incorporate standards or other codes of practice that are important in a particular domain or discipline (Caralli et al., 2012).

The proposed cloud data governance Maturity Model consists of five levels: level 1: non-cloud data governance; level 2: initial cloud data governance; level 3: moderate cloud data governance; level 4: advanced cloud data governance; and level 5: converged cloud data governance. Each level in this maturity model comprises a set of process goals that, when satisfied, stabilise an important component of the cloud data governance process. Achieving each level of the cloud data governance Maturity Model establishes a different component in the cloud data governance process, resulting in an increase in the capability of the organisation to achieve an effective cloud data governance programme. Cloud data governance is believed to improve as the organisation moves up these five levels. Furthermore, section 4.5.1 in below will presents cell text formulation to determine the characteristics of these levels to assess the maturity of the cloud data governance programme based on the dimensions of the strategy framework in this research. The cloud data governance maturity levels are as illustrated in Figure 4.12.

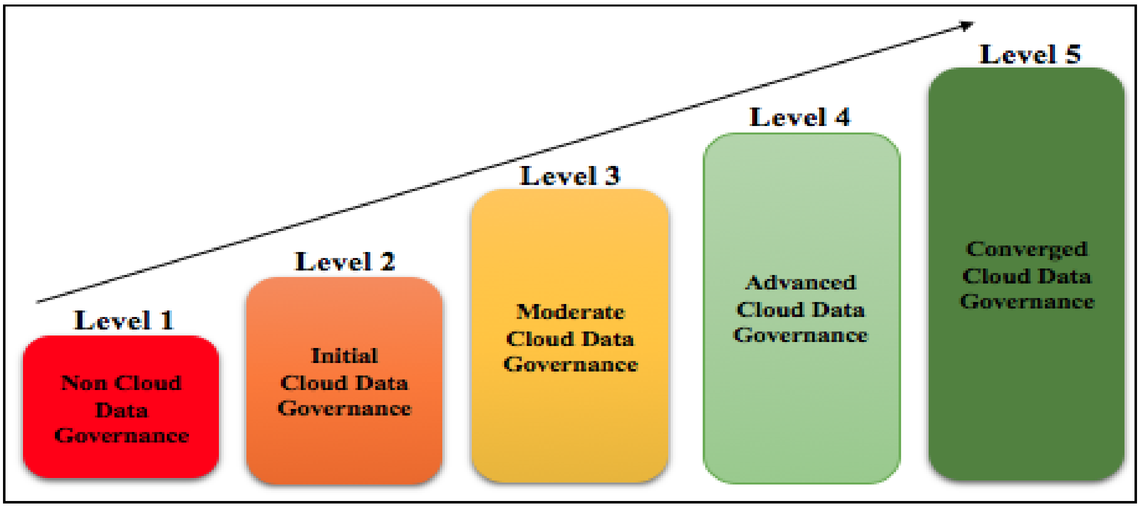

Figure 4.12 The cloud data governance maturity levels

c) Cloud Data Governance Maturity Dimensions

The maturity model dimensions refer to the crucial domains that are used by the maturity model to measure the field of study (Adler, 2007). When determining the maturity model, components or attributes should first be defined to achieve the maturity model's objective (Rose & Guide, 2013). In this study, the dimensions aim to cover the area of cloud data governance that help organisations implement data governance for cloud computing in their business. The components of the proposed framework presented in Chapter Three were chosen as the dimensions for the maturity model in this research. These components were: cloud data governance office, preparation requirements, cloud data governance functions, contextual alignment, contextual integration, contractual context, deploy context, monitor requirements and sustain requirements. The cloud data governance dimensions are illustrated in Figure 4.13.

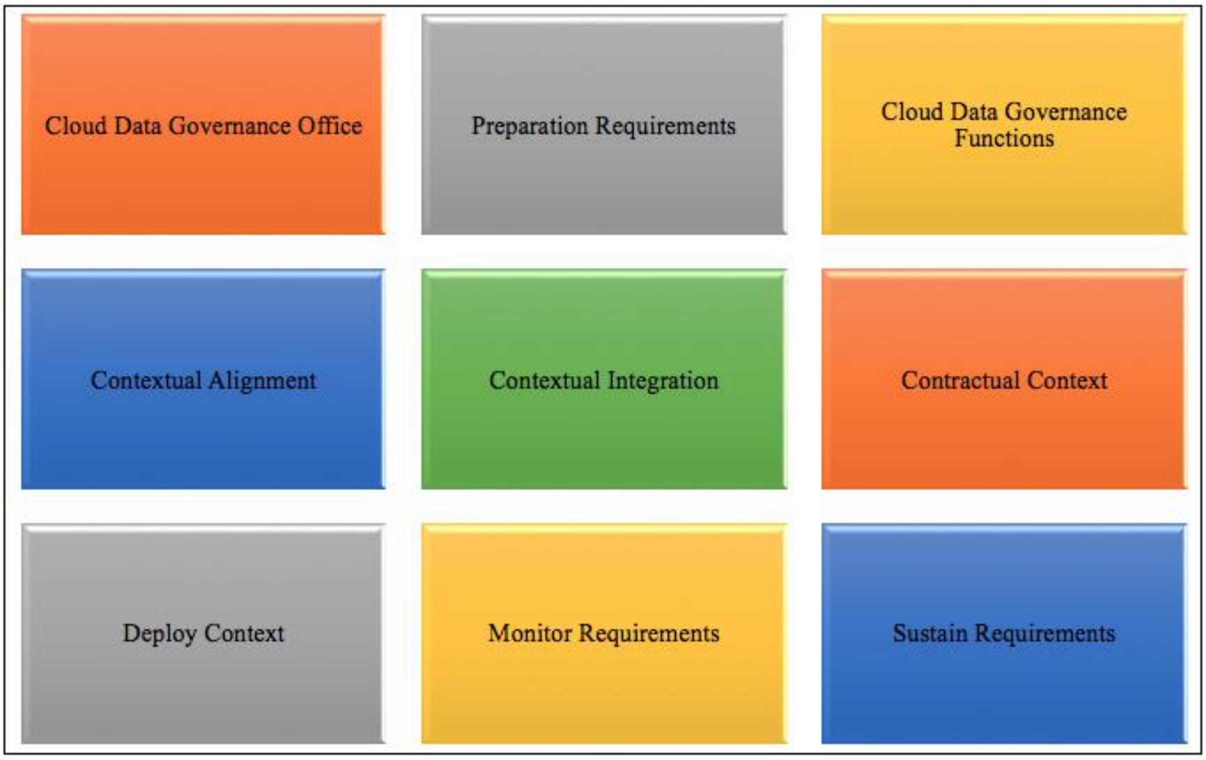

Figure 4.13 The cloud data governance dimensions

These dimensions have been discussed in detail in Chapter Three, and the proposed maturity model will measure cloud data governance in organisations based on these dimensions. Each dimension in this maturity model will be measured and assessed by its sub-dimensions, based on the maturity levels. The sub-dimensions are as illustrated in Table 4.2.

Table 4.1 The cloud data governance sub-dimensions used to assess the core dimensions

Dimension	Assessment by
Cloud Data Governance Office	Structure, communication plan, roles and responsibilities.
Preparation Requirements	Business case, assess cloud data governance requirements, data classification.
Cloud Data Governance Functions	Policies, principles, processes, standards.
Contextual Alignment	Environmental strategy, technical strategy, organisational strategy, IT governance strategy, corporate governance strategy, business strategy, cloud governance strategy, e-government strategy.

Dimension	Assessment by
Contextual Integration	Cloud deployment models, cloud service delivery models.
Contractual Context	Negotiation with cloud provider, cloud data governance level agreement.
Deploy Context	Configuration of cloud data governance programme, review and test cloud data governance programme, implement cloud data governance programme.
Monitor Requirements	Dashboard, metrics and KPIs, cloud data governance tool.
Sustain Requirements	Identify CSFs, evaluate the effectiveness of the cloud data governance programme, education and training plan, execute change management plan, execute cloud data governance change plan.

4.4.3. Post-Design Phase

This phase aims to validate and evaluate the proposed cloud data governance maturity model to make sure that it achieves its objective. The results of the systematic literature review presented above in this chapter showed that the most common validation and evaluation methods used in the literature were: surveys, case studies, questionnaires, focus groups, interviews and workshops (Poeppelbuss et al., 2011; Helgesson et al., 2012). Therefore, a case study in Saudi Arabia has been chosen in this research to validate the maturity model based on a number of criteria through a focus group. The results of this validation will be considered and used to improve the maturity model, to make sure that it is effective. The validation process and results will be presented in Chapter Seven.

4.5. Assessment Matrix

Managing and improving organisational capabilities is a significant and complex challenge (Maier et al., 2012). Performance assessments are commonly used to support management and enable improvement. One way of assessing organisational capabilities is by means of an assessment matrix; while assessment matrices may share a common structure, their content differs and very often they are developed anew (Maier et al., 2012; Blommerde & Lynch, 2016). An assessment matrix can be defined as "*a term given to what is essentially a "checklist" whose purpose is to evaluate how well developed a particular process or programme is*" (Barnes et al., 2012, p.585). According to another definition of the maturity or assessment matrix: a "*maturity matrix is a management assessment tool developed for evaluating an organization's level of progress towards a goal*" (Galán, 2017, p.410). Based on this study's systematic literature review, there are many assessment matrices in the literature that have been developed by researchers and practitioners to assess organisations in different fields (Pohlman, 2010; Maier et al., 2012; Barnes et al., 2012; Blommerde & Lynch, 2016). Most of these matrices have been developed based on process areas related to specific fields and maturity levels. In the case of the data governance assessment matrix, it is designed to be an interactive data governance diagnostic tool for assessing both the current state of data governance readiness and the its maturity within an organisation (Adler, 2007; Rivera et al., 2017). The literature review shows that a few assessment matrices for data governance were developed such as those by IBM, SaS and the University of Stanford(Adler, 2007; Nascio, 2009). These assessment matrices have been developed to assess data governance in general based on their framework dimensions, for non-cloud services.

In order to develop an assessment matrix, Maier et al. (2012) suggested a roadmap consisting of four phases – planning, development, evaluation and maintenance, where each phase has a number of decision points. The first phase, which is the planning phase, includes: specify audience, define aim, clarify scope and define success criteria. The development phase includes; select process areas (content), select maturity levels (rating scale), formulate cell text (intersection of process areas and maturity levels) and define administration mechanism. The evaluation phase includes. validation and verification. The last phase is the maintenance phase and it includes; check benchmark, maintain results database, and document and communicate development process and results. Figure 4.14 shows the phases and decision points of the roadmap to develop an assessment matrix.

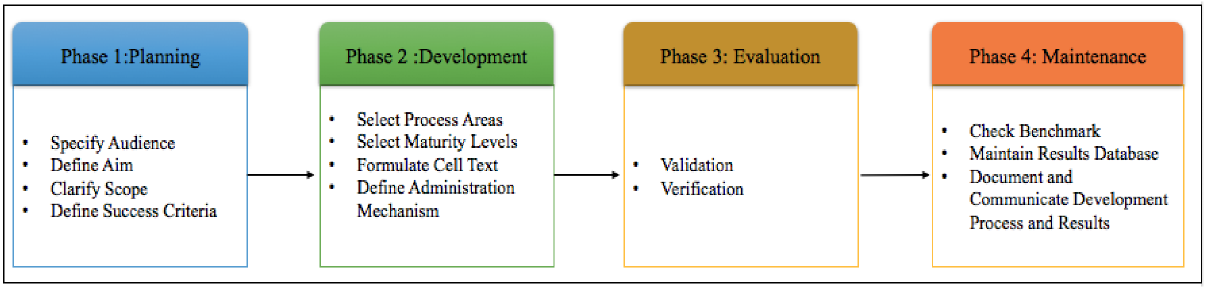

Figure 4.14 Phases and decision points of roadmap to develop an assessment matrix. Source: (Maier et al., 2012)

In the case of the cloud data governance assessment matrix, it is the application of the focus area's maturity model in the field of cloud data governance. In this study, the assessment matrix has been developed as a tool to identify the current state of cloud data governance in an organisation and it helps the organisation to achieve its target of achieving effective cloud data governance outcomes. The cloud data governance assessment matrix also aims to identify the strengths and weaknesses of cloud data governance, and it provides guidelines to improve cloud data governance in the organisation.

With regard to the assessment matrix development, most of the assessment matrices in the literature use two key components to analyse the state of maturity, which are process areas and maturity levels, with statements that describe each process area in each level (Schipper, 2002; Barnes et al., 2012; Blommerde & Lynch, 2016). In the literature, there are differences between maturity models and assessment matrices (Schipper, 2002; Maier et al., 2012). The maturity model highlights the scope of the assessment based on process areas and maturity level, whereas the maturity matrix has a more detailed approach (Schipper, 2002). The next section will present and discuss the assessment matrix development for cloud data governance, based on the findings of this research.

4.5.1. Cloud Data Governance Assessment Matrix Development

In this study, the cloud data governance assessment matrix is developed to support the cloud data governance maturity model developed as part of this thesis. The proposed cloud data governance maturity model was developed to define an organisation's maturity level based cloud data governance Framework, developed in Chapter Three. The cloud data governance maturity model uses two key components to analyse the state and improve the processes of cloud data governance in the organisation: cloud data governance dimensions and maturity level.

This study adopts the development and evaluation phases suggested by Maier et al. (2012). While this section presents the development process, the validation and evaluation processes will be presented in Chapter Seven. The development phase aims to define the architecture of the assessment matrix; and it includes three decision points; select process areas (content), select maturity levels (rating scale) and formulate cell text (intersection of process areas and maturity levels). Thus, the cloud data governance assessment matrix was developed based on three components; cloud data governance dimensions, maturity level and formulated cell text (intersection of dimensions and maturity levels). In terms of the cloud data governance dimensions and maturity level, these have been discussed in the maturity model section above. Additionally, the selection of process areas and maturity levels will influence the formulation of the cell text and ultimately form the basis for assessment (Maier et al., 2012; Moultrie et al., 2016).

With regard to formulating the cell text, once the process and levels of maturity assigned to each dimension are identified, in the literature some authors reported that one of the most important steps in developing an assessment matrix is the identification and formulation of behavioural characteristics for processes (Barnes et al., 2012; Maier et al., 2012; Blommerde & Lynch, 2016; Moultrie et al., 2016). Furthermore, the process characteristics need to be described at each level of maturity, and each level should build on the level before, meaning that to achieve level 3 it is expected that requirements of levels 1-2 have also been demonstrated; thus, the descriptions should be clear, concise and precise (Maier et al., 2012; Rose & Guide, 2013).

In terms of differentiating between the maturity levels, Maier et al. (2012) and Moultrie et al. (2016) suggested that it requires: a) some decision points on whether the cell text is “prescriptive” or “descriptive”; b) a justification of the information source; and c) a decision on the mechanism to be used to formulate the text descriptions (Maier et al., 2012; Moultrie et al., 2016). These decision points are considered in this study to differentiate between maturity levels in the cloud data governance assessment matrix. The descriptive approach was used to formulate the cell text; this means that the focus is on a detailed account of the individual case and there are a number of aspects that should be considered, such as the underlying rationale, characteristics and knowledge of the subject area (Maier et al., 2012).

Regarding the information source, there are a number of options available in the literature to formulate the text descriptions in each cell (Maier et al., 2012; Moultrie et al., 2016). The first option is synthesising viewpoints from a sample representing the future recipients of the assessment. The second option is reviewing and comparing practices of a number of organisations, for example, through empirical studies, reviewing written case studies in literature, and best practice guides.

Therefore, this study follows the options of reviewing written case studies and best practice guides in the literature, and these will be validated and evaluated by experts in many organisations through a focus group. With regard to the mechanism of formulating the text descriptions, identifying extreme ends of the scale is one of the main mechanisms that has been used in the literature (Maier et al., 2012; Barnes et al., 2012; Moultrie et al., 2016; Blommerde & Lynch, 2016). Therefore, this study adopts this mechanism, which is used to determine the best and worst practices, and then to determine the characteristics of all the levels in between.

To formulate the text descriptions for each level in the assessment matrix, it is important avoid any confusion, by creating a clear distinction between the levels, which allows for more accurate diagnosis of the situation. For this these terms are used as differentiators: Does not exist, Informal, Semi-formal (complete and incomplete), and Formal. As for the 'does not exist' it means that the organisation does not have or support or even recognise that cloud data governance sub-dimension. The formality in this context refers to the degree at which any one sub/dimension is adopted and embedded into the organisation's structure, officially, which can range between informal, semi-formal and formal. The completeness, ok the other hand, refers to the state of implementation of any one sub-dimension, which can be fully implemented (complete) or partially implemented (incomplete). Figure 4.15 shows the adopted roadmap to differentiate between the maturity levels in the assessment matrix.

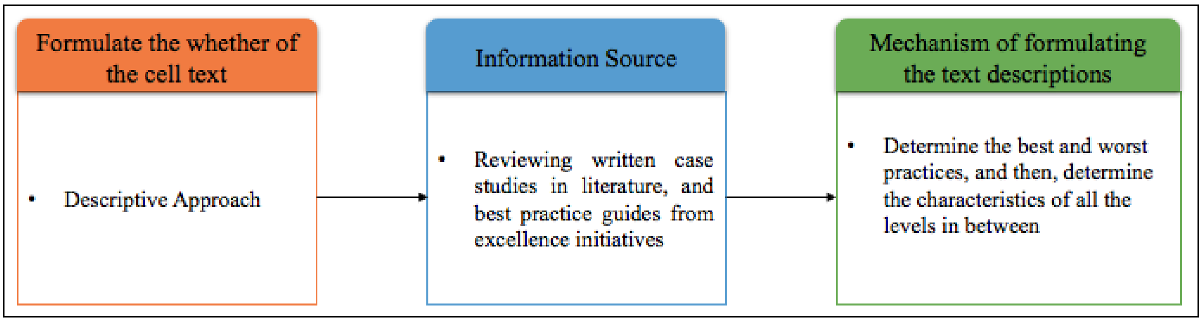

Figure 4.15 Roadmap to discriminate between the maturity levels in the maturity matrix

The proposed assessment matrix was constructed with five levels, and nine core categories (dimensions) were added as cross-reference categories for the five levels. The result was an assessment matrix, the cells of which were completed with descriptions of the process being performed at various levels of maturity, and each level has been built on the level before. The sub-category (sub-dimensions) for each dimension of cloud data governance were embedded in this matrix. The assessment matrix for each dimension is outlined as follows:

a) Cloud Data Governance Office

The assessment matrix aims to describe the level of maturity of the organisation by establishing the cloud data governance office dimension. This dimension is assessed by three sub-dimensions: structure, roles and responsibilities, and communication plan, as illustrated in Table 4.3.

Table 4.2 The cloud data governance office assessment matrix

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Structure	No structure to the cloud data governance office.	Informal structure to the cloud data governance office underway.	Semi-formal structure to the cloud data governance office underway but incomplete.	Semi-formal structure to the cloud data governance office underway and complete.	Formal structure to the cloud data governance office – a part of the organisation structure.
Roles and Responsibilities	No roles and responsibil-ities for cloud data governance.	Informal roles and responsibilities for cloud data governance underway.	Semi-formal roles and responsibilities for cloud data governance underway but incomplete.	Semi-formal roles and responsibilities for cloud data governance underway and complete.	Formal roles and responsibilities for cloud data governance team are documented, implemented and monitored.
Communication Plan	No communicat-ion plan for cloud data governance.	Informal communication plan for cloud data governance underway.	Semi-formal communication plan for cloud data governance underway but incomplete.	Semi-formal communicat-ion plan for cloud data governance underway and complete.	Formal communicat-ion plan between cloud data governance teams is defined, documented and updated.

b) Preparation Requirements

The assessment matrix aims to describe the level of maturity of the organisation by identifying the important requirements that support the decision to implement an effective cloud data governance programme. This dimension is assessed by four sub-dimensions: business case, assess, data governance requirements and data classification, as illustrated in Table 4.4.

Table 4.3 The preparation requirements assessment matrix

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Business Case	No business case of cloud data governance.	Informal business case of cloud data governance underway.	Semi-formal business case of cloud data governance underway but incomplete.	Semi-formal business case of cloud data governance underway and complete.	Formal business case of cloud data governance is developed, documented and updated.
Assess	No assessment criteria for cloud data governance.	Informal assessment criteria for cloud data governance underway.	Semi-formal assessment criteria for cloud data governance underway but incomplete.	Semi-formal assessment criteria for cloud data governance underway and complete.	Formal assessment criteria and process for cloud data governance are implemented, documented and monitored.
Data Governance Requirements	No requirements for cloud data governance.	Informal requirements for cloud data governance underway.	Semi-formal requirements for cloud data governance underway but incomplete.	Semi-formal requirements for cloud data governance underway and complete.	Formal requirements for cloud data governance are defined, documented, and updated.
Data Classification	No cloud data assets are classified in cloud data governance.	Informal classification of cloud data assets in cloud data governance underway.	Semi-formal classification of cloud data assets in cloud data governance underway but incomplete.	Semi-formal classification of cloud data assets in cloud data governance underway and complete.	Formal classification of cloud data assets in cloud data governance is defined, documented, and updated.

c) Cloud Data Governance Functions

The assessment matrix aims to describe the level of maturity of the organisation by defining, setting up and implementing the cloud data governance functions. This dimension is assessed by four sub-dimensions: policies, standards, processes and procedures, as illustrated in Table 4.5.

Table 4.4 The cloud data governance functions assessment matrix

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Policies	No policies specifically covering relevant aspects of cloud data governance.	Informal policies of cloud data governance underway.	Semi-formal policies of cloud data governance underway but incomplete.	Semi-formal policies of cloud data governance underway and complete.	Formal policies of cloud data governance are defined and regularly reviewed and approved by cloud data governance office.
Processes	No processes specifically covering relevant aspects of cloud data governance.	Informal processes of cloud data governance underway.	Semi-formal processes of cloud data governance underway but incomplete.	Semi-formal processes of cloud data governance underway and complete.	Formal processes of cloud data governance are defined and regularly reviewed and approved by cloud data governance office.
Standards	No standards specifically covering relevant aspects of cloud data governance.	Informal standards of cloud data governance underway.	Semi-formal standards of cloud data governance underway but incomplete.	Semi-formal standards of cloud data governance underway and complete.	Formal standards of cloud data governance are defined and regularly reviewed and approved by cloud data governance office.
Procedure	No procedures specifically covering relevant aspects of cloud data governance.	Informal procedures of cloud data governance underway.	Semi-formal procedures of cloud data governance underway but incomplete.	Semi-formal procedures of cloud data governance underway and complete.	Formal procedures of cloud data governance are defined and regularly reviewed and approved by cloud data governance office.

d) Contextual Integration

The assessment matrix aims to describe the level of maturity of the organisation by integrating the cloud data governance functions within the cloud deployment model and service delivery models considered by the organisation when adopting cloud computing. This dimension is assessed by two sub-dimensions: cloud deployment models and cloud service delivery models, as illustrated in Table 4.6.

Table 4.5 The contextual integration assessment matrix

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Cloud Deployment Models	No integration of cloud data governance with the characteristics of the cloud deployment models.	Informal integration of cloud data governance underway with the characteristics of the cloud deployment models.	Semi-formal integration of cloud data governance underway with the characteristics of the cloud deployment models but incomplete.	Semi-formal integration of cloud data governance underway with the characteristics of the cloud deployment models and complete.	Formal integration of cloud data governance with the characteristics of the cloud deployment models is implemented and regularly reviewed and approved by cloud data governance office.
Cloud Service Delivery Models.	No integration of cloud data governance with the characteristics of the cloud service delivery models.	Informal integration of cloud data governance underway with the characteristics of the cloud service delivery models.	Semi-formal integration of cloud data governance underway with the characteristics of the cloud service delivery models but incomplete.	Semi-formal integration of cloud data governance underway with the characteristics of the cloud service delivery models and complete.	Formal integration of cloud data governance with the characteristics of the cloud service delivery models is implemented and regularly reviewed and approved by cloud data governance office.

e) Contextual Alignment

The assessment matrix aims to describe the level of maturity of the organisation by aligning the cloud data governance functions with the other important strategies in the organisation. This dimension is assessed by eight sub-dimensions: environmental strategy, technical strategy, organisational strategy, IT governance strategy, corporate governance strategy, business strategy, cloud governance strategy and e-government strategy, as illustrated in Table 4.7.

Table 4.6 The contextual alignment assessment matrix

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Environmental Strategy	No alignment of cloud data governance with environmental strategy.	Informal alignment of cloud data governance with the environmental strategy.	Semi-formal alignment of cloud data governance with the environmental strategy – underway but incomplete.	Semi-formal alignment of cloud data governance with the environmental strategy – complete.	Formal alignment of cloud data governance with the environmental strategy – egularly reviewed and approved by cloud data governance office.
Technical Strategy	No alignment of cloud data governance with the technical strategy.	Informal alignment of cloud data governance with the technical strategy.	Semi-formal alignment of cloud data governance with the technical strategy – underway but incomplete.	Semi-formal alignment of cloud data governance with the technical strategy – complete.	Formal alignment of cloud data governance with the technical strategy – regularly reviewed and approved by cloud data governance office.
Organisational Strategy	No alignment of cloud data governance with the organisational strategy.	Informal alignment of cloud data governance with the organisational strategy.	Semi-formal alignment of cloud data governance with the organisational strategy – incomplete.	Semi-formal alignment of cloud data governance with the organisational strategy – complete.	Formal alignment of cloud data governance with the organisational strategy – regularly reviewed and approved by cloud data governance office.
IT Governance Strategy	No alignment of cloud data governance with the IT governance strategy.	Informal alignment of cloud data governance with the IT governance strategy.	Semi-formal alignment of cloud data governance with the IT governance strategy –	Semi-formal alignment of cloud data governance with the IT governance strategy –	Formal alignment of cloud data governance with the IT governance strategy – regularly

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
			incomplete.	complete.	reviewed and approved by cloud data governance office.
Corporate Governance Strategy	No alignment of cloud data governance with the corporate governance strategy.	Informal alignment of cloud data governance with the corporate governance strategy.	Semi-formal alignment of cloud data governance with the corporate governance strategy – incomplete.	Semi-formal alignment of cloud data governance with the corporate governance strategy – complete.	Formal alignment of cloud data governance with the corporate governance strategy – regularly reviewed and approved by cloud data governance office.
Business Strategy	No alignment of cloud data governance with the business strategy.	Informal alignment of cloud data governance with the business strategy.	Semi-formal alignment of cloud data governance with the business strategy – incomplete.	Semi-formal alignment of cloud data governance with the business strategy – complete.	Formal alignment of cloud data governance with the business strategy – regularly reviewed and approved by cloud data governance office.
Cloud Governance Strategy	No alignment of cloud data governance with the cloud governance strategy.	Informal alignment of cloud data governance with the cloud governance strategy.	Semi-formal alignment of cloud data governance with the cloud governance strategy – incomplete.	Semi-formal alignment of cloud data governance with the cloud governance strategy – complete.	Formal alignment of cloud data governance with the cloud governance strategy – regularly reviewed and approved by cloud data governance office.
E-government	No alignment of cloud data	Informal alignment of	Semi-formal alignment of	Semi-formal alignment of	Formal alignment of

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Strategy	governance with the e-government strategy.	cloud data governance with the e-government strategy.	cloud data governance with the e-government strategy underway but incomplete.	cloud data governance with the e-government strategy – complete.	cloud data governance with the e-government strategy – regularly reviewed and approved by cloud data governance office.

f) Contractual Context

The assessment matrix aims to describe the level of maturity of the organisation by developing a cloud data governance level agreement that includes cloud data governance requirements. This begins with negotiations between the cloud consumer and cloud provider to verify the ability of the cloud provider to achieve the required level of data governance. This dimension is assessed by two sub-dimensions: negotiation with cloud provider and cloud data governance level agreement, as illustrated in Table 4.8.

Table 4.7 The contractual context assessment matrix

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Negotiation with Cloud Provider	No negotiation with cloud provider for cloud data governance.	Informal negotiation with cloud provider for cloud data governance.	Semi-formal negotiation with cloud provider for cloud data governance, underway but incomplete.	Semi-formal negotiation with cloud provider for cloud data governance, underway and complete.	Formal negotiation with cloud provider for cloud data governance is implemented, documented and regularly reviewed and approved by cloud data governance office.
Cloud data governance level agreement	No cloud data governance level agreement.	Informal cloud data governance level agreement.	Semi-formal cloud data governance level agreement, underway but incomplete.	Semi-formal cloud data governance level agreement, underway and complete.	Formal cloud data governance level agreement is implemented and regularly reviewed and approved by cloud data governance office, and it is part of the cloud SLA.

g) Deploy Context

The assessment matrix aims to describe the level of maturity of the organisation by implementing a formal cloud data governance programme to manage the transformation of its data assets in the cloud computing environment, from non-governed to governed. This dimension is assessed by three sub-dimensions: configuring the cloud data governance programme, reviewing and testing the cloud data governance programme and implementing the cloud data governance programme, as illustrated in Table 4.9.

Table 4.8 The deploy context maturity matrix

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Configuring the Cloud Data Governance Programme	No approach to configuring the cloud data governance programme.	Informal approach to configuring the cloud data governance programme.	Semi-formal approach to configuring the cloud data governance programme, underway but incomplete.	Semi-formal approach to configuring the cloud data governance programme, underway and complete.	Formal approach to configuring the cloud data governance programme is implemented and regularly reviewed and approved by cloud data governance office.
Reviewing and Testing the Cloud Data Governance Programme	No approach to reviewing and testing the cloud data governance programme.	Informal approach to reviewing and testing the cloud data governance programme.	Semi-formal approach to reviewing and testing the cloud data governance programme, underway but incomplete.	Semi-formal approach to reviewing and testing the cloud data governance programme, underway and complete.	Formal approach to reviewing and testing the cloud data governance programme is implemented and regularly reviewed and approved by cloud data governance office.
Implementing the Cloud Data Governance Programme	No implementat-ion approach to the cloud data governance programme.	Informal implementation approach to the cloud data governance programme.	Semi-formal implementat-ion approach to the cloud data governance programme, underway but incomplete.	Semi-formal implementation approach to the cloud data governance programme, underway and complete.	Formal implementation approach to the cloud data governance programme – regularly reviewed and approved by cloud data governance office.

h) Monitor Requirements

The assessment matrix aims to describe the level of maturity of the organisation by developing mechanisms for monitoring the cloud data governance programme. This dimension is assessed by three sub-dimensions: dashboard, metrics and KPIs, and cloud data governance tools, as illustrated in Table 4.10.

Table 4.9 The monitor requirements assessment matrix

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Dashboard	No dashboard to monitor the operation and performance of cloud data governance.	Informal dashboard to monitor the operation and performance of cloud data governance.	Semi-formal dashboard to monitor the operation and performance of cloud data governance, underway but incomplete.	Semi-formal dashboard to monitor the operation and performance of cloud data governance, underway and complete.	Formal dashboard to monitor the operation and performance of cloud data governance is implemented and regularly reviewed and approved by cloud data governance office.
Metrics and KPIs	No metrics and KPIs to measure and monitor cloud data governance.	Informal metrics and KPIs to measure and monitor cloud data governance in place.	Semi-formal metrics and KPIs to measure and monitor cloud data governance, in place but incomplete.	Semi-formal metrics and KPIs to measure and monitor cloud data governance, in place and complete.	Formal metrics and KPIs to measure and monitor cloud data governance are implemented and regularly reviewed and approved by cloud data governance office.
Cloud Data Governance Tool	No tool to measure and monitor cloud data governance.	Informal tool to measure and monitor cloud data governance.	Semi-formal tool to measure and monitor cloud data governance, but incomplete.	Semi-formal tool to measure and monitor cloud data governance and complete.	Formal metrics and tools based on modern technology to monitor cloud data governance are implemented and regularly reviewed and approved by cloud data governance office.

i) Sustain Requirements

The assessment matrix aims to describe the level of maturity of the organisation by developing mechanisms to sustain and continue the cloud data governance programme for a long time. This dimension is assessed by five sub-dimensions: identify CSFs, evaluate the effectiveness of the cloud governance data program, education and training plan, execute the change management plan and execute the cloud data governance change plan, as illustrated in Table 4.11.

Table 4.10 The sustain requirements assessment matrix

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
Identify Critical Success Factors (CSFs)	No approach to identify CSFs to sustain cloud data governance programme.	Informal approach to identify CSFs to sustain cloud data governance programme.	Semi-formal approach to identify CSFs to sustain cloud data governance programme, underway but incomplete.	Semi-formal approach to identify CSFs to sustain cloud data governance programme, underway and complete.	Formal approach to identify CSFs to sustain cloud data governance programme is implemented and regularly reviewed and approved by cloud data governance office.
Evaluation of the Effectiveness of Cloud Data Governance Programme	No approach to evaluating the effectiveness of cloud data governance programme.	Informal approach to evaluating the effectiveness of cloud data governance programme.	Semi-formal approach to evaluating the effectiveness of cloud data governance programme, underway but incomplete.	Semi-formal approach to evaluating the effectiveness of cloud data governance programme, underway and complete.	Formal approach to evaluating the effectiveness of cloud data governance programme is implemented and regularly reviewed and approved by cloud data governance office.
Education and Training Plan	No plan to educate and train employees on cloud data governance programme.	Informal plan is implemented to educate and train employees on cloud data governance programme.	Semi-formal plan is implemented to educate and train employees on cloud data governance programme, underway but	Semi-formal plan is implemented to educate and train employees on cloud data governance programme, underway and	Formal plan is implemented to educate and train employees on cloud data governance programme and is regularly reviewed and approved by

Sub-dimensions/ level	Level 1	Level 2	Level 3	Level 4	Level 5
			incomplete.	complete.	cloud data governance office.
Execute Change Management Plan	No plan to execute change management of cloud data governance programme.	Informal plan is implemented to execute change management of cloud data governance programme.	Semi-formal plan is implemented to execute change management of cloud data governance programme, but incomplete.	Semi-formal plan is implemented to execute change management of cloud data governance programme, complete.	Formal plan is implemented to execute change management of cloud data governance programme and is regularly reviewed and approved by cloud data governance office.
Execute Cloud Data Governance Change Plan	No plan to execute change of cloud data governance.	Informal plan to execute change of cloud data governance.	Semi-formal plan to execute change of cloud data governance, underway but incomplete.	Semi-formal plan to execute change of cloud data governance, underway and complete.	Formal plan is implemented to execute change of cloud data governance programme and is regularly reviewed and approved by cloud data governance office.

4.5.2. Structure of the Assessment Matrix Implementation and Use

The assessment matrix for cloud data governance is a valuable tool for the assessment and improvement of the cloud data governance process in organisations. It is a practical tool aimed at supporting the implementation of cloud data governance programmes. This section aims to present the structure of the assessment matrix implementation and use. Implementing the assessment matrix will provide information on the overall level of maturity of the cloud data governance in the organisation in a number of ways:

- Providing the overall maturity level for the cloud data governance in the organisation based on nine core dimensions.
- Providing the maturity level for each core dimension of the cloud data governance in the organisation based on its sub-dimensions.
- Providing the maturity level for each sub-dimension in each core dimension of the cloud data governance in the organisation.

To implement and use the cloud data governance assessment matrix, the assessment criteria will be developed based on the content of this assessment matrix, and the results of the assessment could be shown graphically. These criteria will be used as statements given to organisations to assess the maturity levels of their cloud data governance, based on the defined dimensions. The statements are based on the content of the assessment matrix for each sub-dimension.

An assessment scenario starts by using multiple statements to assess the sub-dimensions for the first dimension. After assessing these sub-dimensions, the maturity level for this dimension will be calculated. This scenario will be repeated until all the dimensions of the cloud data governance have been assessed. At the end, the overall maturity level for the cloud data governance in the organisation will be calculated, based on nine main dimensions. Figure 4.16 shows the high architecture to implement and use the cloud data governance assessment matrix.

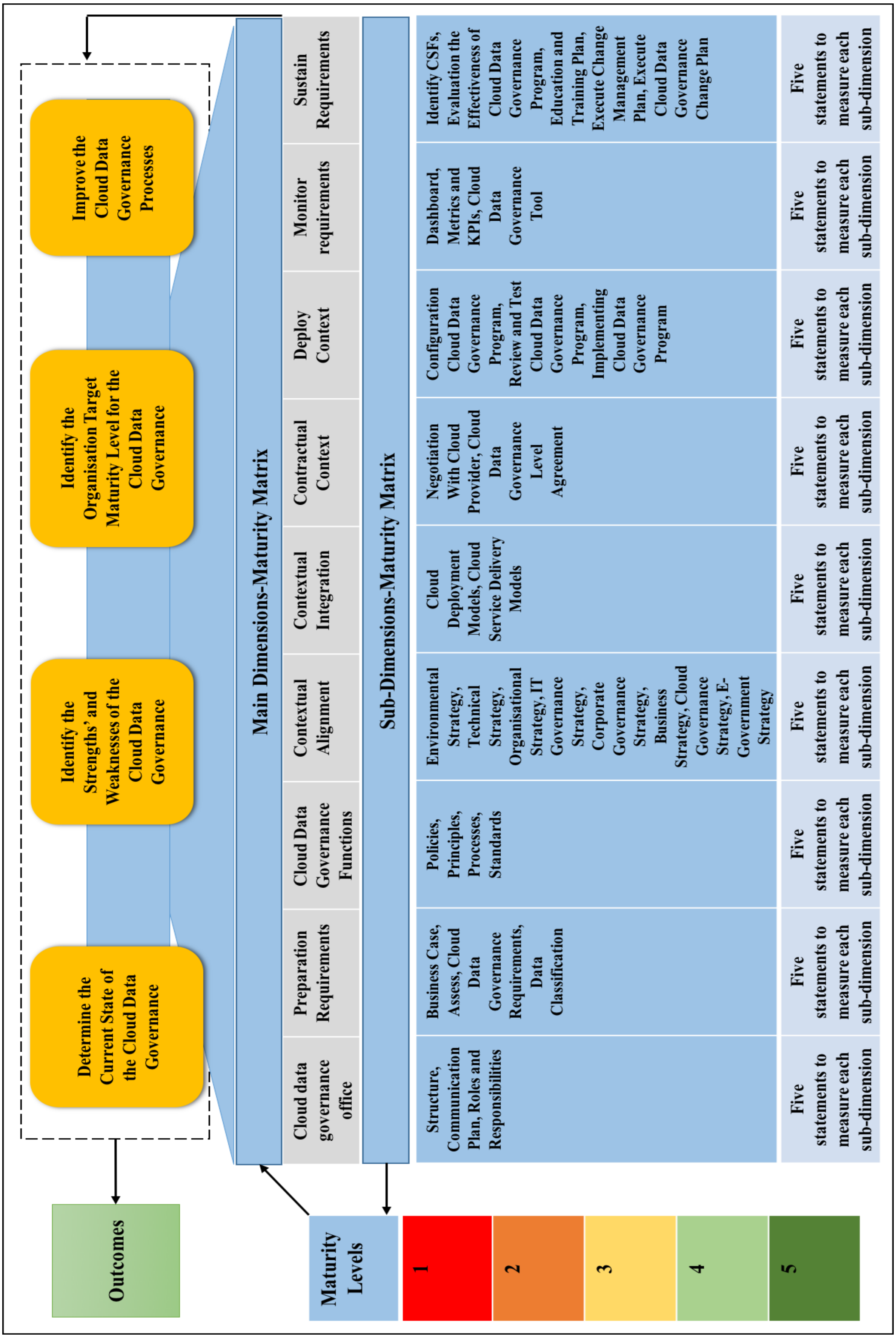

Figure 4.16 The structure to implement the cloud data governance assessment matrix.

4.6. Chapter Summary

This chapter presents the cloud data governance maturity model and an assessment matrix. The systematic literature review showed that the main maturity models in the literature have been developed in two ways: based on the Capability Maturity Model (CMM) and based on the conceptual construction of the topic. Therefore, the maturity model in this research was developed based on the conceptual construction of the cloud data governance as a theoretical foundation. In this chapter, the maturity model was developed based on three components: outcomes, maturity levels and dimensions. The dimensions represent the components of the strategy framework required to design, deploy and sustain an effective cloud data governance programme, which was presented in Chapter Three. This chapter summarises the aims and motivation for the maturity model, and then describes the dimensions used to measure the maturity of cloud data governance in an organisation. The maturity levels were also defined and described in this chapter, along with the relationship between the dimensions and the levels of the maturity model. This study follows a systematic methodology for developing the cloud data governance maturity model. This methodology includes three phases: *Pre-Design, Design and Post-Design.* Each phase has many tasks within it to achieve its aims and objectives. With regard to the assessment matrix, this chapter explained the development process and how to implement the assessment matrix. In the assessment matrix, each level used a statement to describe the current state of the cloud data governance dimensions in the organisation. Finally, the structure of the assessment matrix implementation and use was presented in this chapter. The following chapter will discuss and present the state of cloud data governance in Saudi Arabia, based on the analysis of the findings of the quantitative data collected from the questionnaire.

Chapter 5. State of Cloud Data Governance in Saudi Arabia

5.1. Introduction

This chapter presents and discusses the findings from the quantitative data collected from the questionnaire. The questionnaire aimed to identify the current situation of data governance for cloud computing in public sector organisations in Saudi Arabia. Critical success factors and barriers that influence the implementation of cloud computing in Saudi Arabia have also been considered in this questionnaire in order to support the development of a strategy framework for cloud data governance. Descriptive data analysis was chosen as an appropriate way to analyse the descriptive questionnaire data; frequency and percentage were calculated for each variable. This chapter presents the purpose of the questionnaire in section 2, while section 3 discusses and presents the questionnaire development. Section 4 presents the descriptive statistics of the results finding and finally, the chapter is summarised in section 5.

5.2. Purpose of the Questionnaire

The aim of this questionnaire was to investigate the implementation of data governance related to cloud computing in Saudi Arabia. In addition, this questionnaire aimed to identify the current state of data governance for cloud computing in Saudi Arabia. Critical success factors and barriers that influence the implementation of data governance for cloud computing in Saudi Arabia were also considered in this questionnaire. However, many reasons motivated the design of this questionnaire. The first motivation for this questionnaire was to gather feedback from organisations in Saudi Arabia in order to determine the best solution for cloud consumers to maintain governance of their data in cloud environments. Another motivation was that the literature shows the lack of empirical studies related to the implementation of a cloud data governance programme or strategy in organisations. In the Saudi context, to the best of the author’s knowledge, cloud computing in the country’s public sector is still not well covered by researchers in the academic community, and there is no literature on cloud data governance in Saudi Arabia organisations. Therefore, this study is among the first exploratory studies to provide an empirical study on cloud data governance in the public sector organisations of Saudi Arabia. Certainly, this questionnaire focused on the issues and benefits of data governance and cloud data governance implementation from the users’ perspective, looking at public sector views.

5.3. Questionnaire Development

This section presents the steps that were undertaken to develop the questionnaire.

5.3.1. Questionnaire Design

The questionnaire questions were developed and derived from the literature review results discussed in Chapter Two. Questionnaires can be administered so that they are answered by the respondents themselves (self-administered) or administered by an interviewer (Siniscalco & Auriat, 2005). In this study, a self-administered questionnaire was used to obtain a larger number of respondents. The self-administered questionnaire offers many advantages for the researcher such as: less time spent on administration, easier questioning of larger numbers of people, and no interviewer bias (Burgess, 2001). The survey question types can be classified into three structures: closed-ended, open-ended and contingency (Meadows, 2003). The closed-ended questions request the respondent to choose one answer among a possible set of answers: the response that most closely represents his/her viewpoint (Meadows, 2003). Open-ended questions are free-response questions that are not followed by any choices and the respondent must answer by supplying a response, usually by entering a number, a word or a short text (Meadows, 2003). On the other hand, a contingency question is a special type of closed-ended question because it applies only to a sub-group of respondents (Burgess, 2001). This study developed its questionnaire based on all three types of questions.

The questionnaire consisted of four parts; the first part covered information about the participant who was taking part in the study. The second part covered general information about data governance in terms of its definition, importance and benefits. The state of cloud computing adoption, the current state of data in the cloud, the concerns and type of knowledge/expertise regarding cloud computing that is lacking in organisation were covered in the third part. Finally, the fourth part covered cloud data governance in terms of its current state, barriers and CSFs.

5.3.2. Questionnaire Translation

Questionnaire translation is the most frequently chosen route to implementing “equivalent” instruments in cross-national and cross-lingual survey research (Harkness & Schoua-Glusberg, 1998). Saunders et al. (2009) stated that “*translating questions and associated instructions into another language requires care, especially if your translated or target* *questionnaire is to be decoded and answered by respondents in the way you intended*". In this study, the survey questionnaire was provided in two languages, English and Arabic. The respondents targeted are Saudi Arabian, thus the study cannot ignore the fact that the first language in Saudi Arabia is Arabic, even if some of the targeted respondents were fluent in English. The translation process was conducted in this study in two phases in order to obtain the best accuracy and adequacy. First, the questionnaire was translated by the researcher into English. Then, the English version was translated back into Arabic by a professional translation service located in Saudi Arabia. The researcher asked five Saudi academic members (PhD holders at Staffordshire University) and IT managers in Saudi Arabian organisations to assist in examining the Arabic version and evaluating how closely it matched the English version. After that, minor amendments took place in the Arabic version, which was then sent back to the professional translation office; the English versions can be found in the Appendix E.

5.3.3. Pilot Study

Piloting the study is one of the most important processes to determine questionnaire reliability and validity and for error testing (Burgess, 2001). In this study, a pilot study was conducted in two phases. A workshop was conducted to test the participants' comprehension of the questionnaire, to ensure that the questions were related to their objectives and were easy to understand, and to test the technical compatibility with different devices (computer, laptop, iPad and smartphone). The workshop consisted of six members from the Mobile Fusion Centre at Staffordshire University. The second phase of the pilot study was conducted with information system professionals from government organisations and academia in Saudi Arabia who speak Arabic and English fluently. Fifteen questionnaires were sent to these professionals. Some changes were made following the comments from the pilot participants, including changes to some questions to ensure and provide more clarity.

5.3.4. Administration of the Questionnaire

A number of researchers have begun to conduct research via the internet using electronic mail (email) and web-based questionnaires (Fox et al., 2003; Siniscalco & Auriat, 2005). The internet offers many advantages over more traditional methods of research; these advantages have been cited for web-based questionnaires as reduced cost, and ease and speed of administration (Fox et al., 2003). Therefore, the questionnaire in this study was distributed using a web-based questionnaire platform (Qualtrics online survey software). The Qualtrics online survey software allows the researcher to design a version of the questionnaire based on multiple languages in one link. In addition, the questionnaire was available in Arabic and in English; the link was sent to the participants by email and by social media applications such as WhatsApp to the public sector organisations in Saudi Arabia during the period from 13/11/2016 to 31/1/2017.

5.4. Descriptive Statistics

This section aims to analyse and describe the statistics for the results of the empirical data in the questionnaire.

5.4.1. Response Rate

Response rate refers to the percentage of people who respond to a survey, and it is calculated by dividing the number of participants who completed the questionnaire by the total number of participants who were asked to participate (Burgess, 2001; Fox et al., 2003; Weill & Ross, 2007). In this study, out of 429 questionnaires distributed during the period from 13/11/2016 to 31/1/2017, 292 responses were received. From those responses, 206 responses were found to be complete and valid. Another 86 responses were discarded because 77 were not complete, and 9 respondents did not agree to complete the questionnaire. The response rate of 68.06% is considered a very good response rate. The sample shows a confidence interval of 4.13% at 95% confidence level. In this study, 206 valid questionnaires have been received, thus; the sample size in this study is sufficient for data analysis and to achieve the purpose of this exploratory study(Abu-Musa, 2010; Fan et al., 2016).

5.4.2. Demographic Analysis

The following table, Table 5.1, provides a general overview of the demographic characteristics of the participants: organisation size, organisation sector, role in the organisation, number of IS specialists, participant’s experience, data governance experience and cloud computing experience. The Pie charts below show individual characteristics of the participants demographic.

Table 5.1 The demographic characteristics of the participants

Characteristics	Frequency (n)	Percent (%)
Organisation Size:		
More than 5000 employees	69	33.50%
5000-1000 employees	64	31.07%

Characteristics	Frequency (n)	Percent (%)
1000-500 employees	31	15.05%
Less than 500 employees	42	20.39%
Organisation Sector:		
Military	39	18.93%
Financial Services	31	15.05%
Healthcare	33	16.02%
Education	42	20.39%
Telecommunication & Information Technology	25	12.14%
Other	36	17.48%
Role in the organisation:		
CEO	10	4.85%
CIO	15	7.28%
Vice President	7	3.40%
IT Manager	42	20.39%
Cloud Manager	6	2.91%
IT Specialist	59	28.64%
Other	67	32.52%
Number of IS Specialists:		
Less than 10 Specialists	68	33.05%
Between 11 and 20 Specialists	22	10.67%
Between 21 and 30 Specialists	29	14.07%
Between 31 and 40 Specialists	20	9.70%
Between 41 and 50 Specialists	9	4.36%
More than 50 Specialists	58	28.15%
Participant's experience in current job:		
More than 10 years	72	32.52%
Between 5 and 10 years	53	25.73%
Between 2 and 5 years	64	31.06%
Less than 2 years	17	8.25%
Participant's data governance experience:		
No experience and knowledge	47	22.82%
No experience but good knowledge	55	26.69%
More than 10 years	31	15.05%
Between 5 and 10 years	27	13.11%
Between 2 and 5 years	33	16.02%
Less than 2 years	13	6.31%
Participant's cloud computing experience:		
No experience and knowledge	42	20.38%
No experience but good knowledge	68	33.01%
More than 10 years	30	14.56%
Between 5 and 10 years	33	16.02%
Between 2 and 5 years	24	11.65%
Less than 2 years	9	4.38%

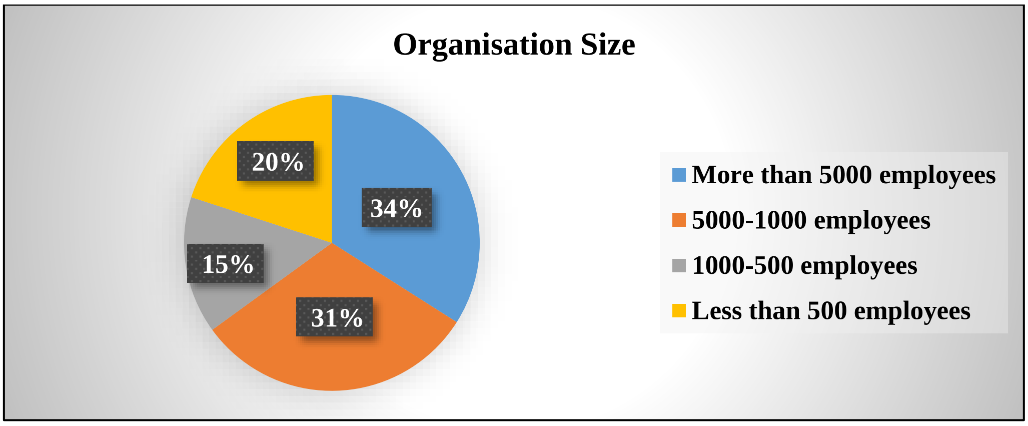

Figure 5.1 Organisation size

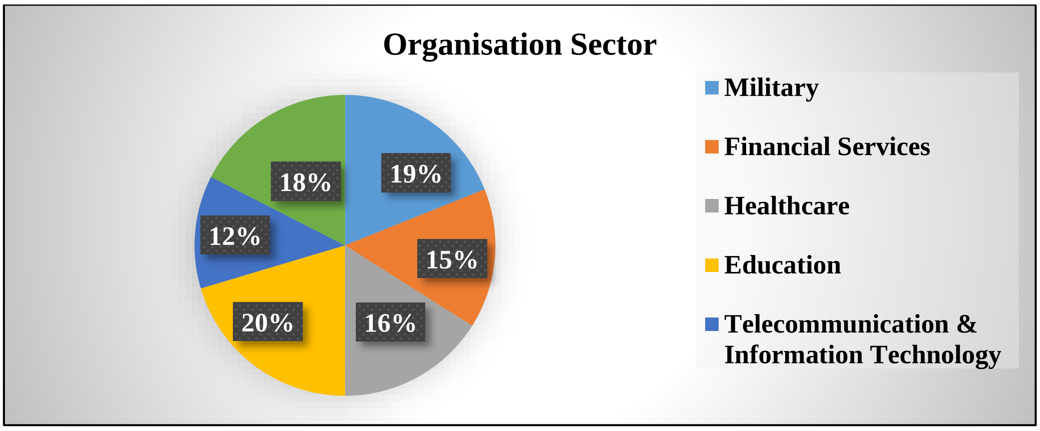

Figure 5.2 Organisation sector

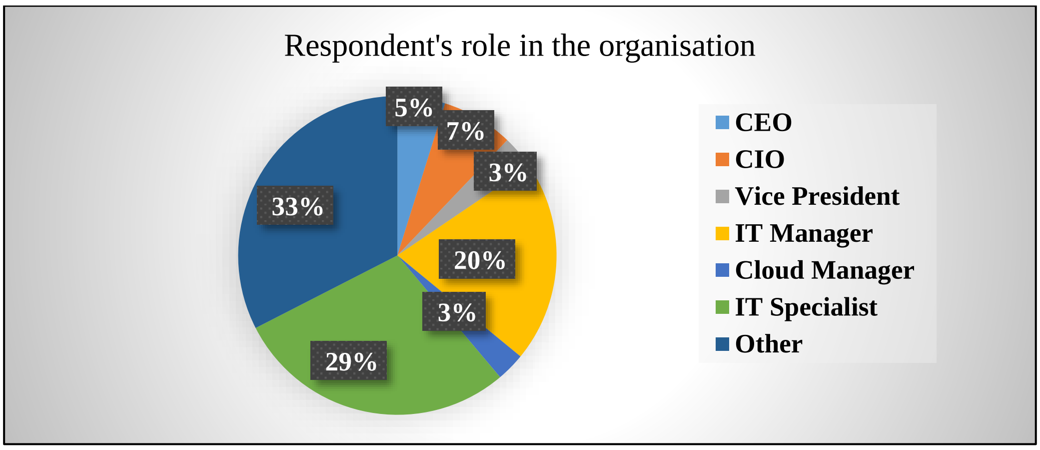

Figure 5.3 The respondents’ role in their organisation

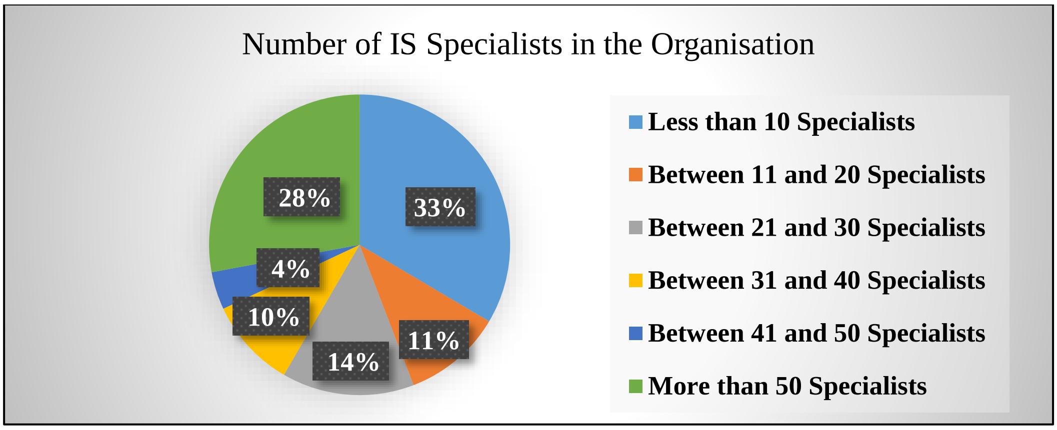

Figure 5.4 The number of IS specialists in the organisation

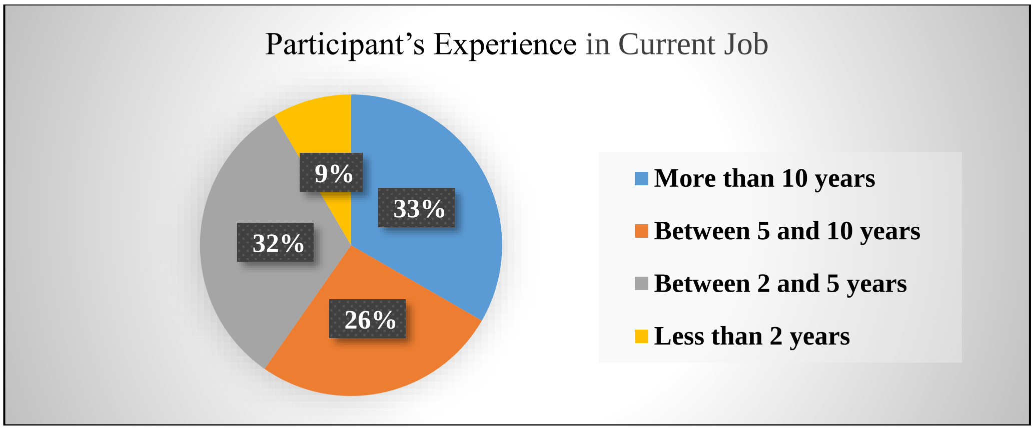

Figure 5.5 The respondents' experience in current job

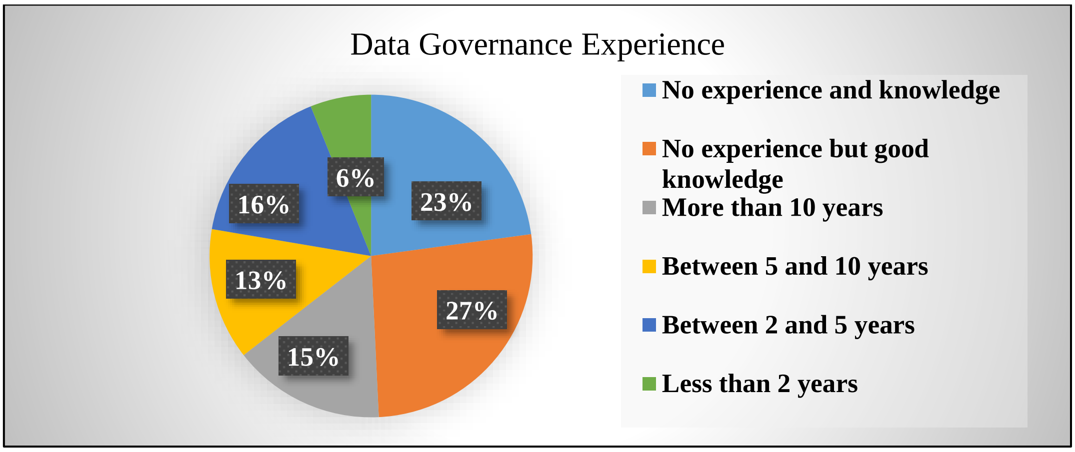

Figure 5.6 The respondents' experience with data governance

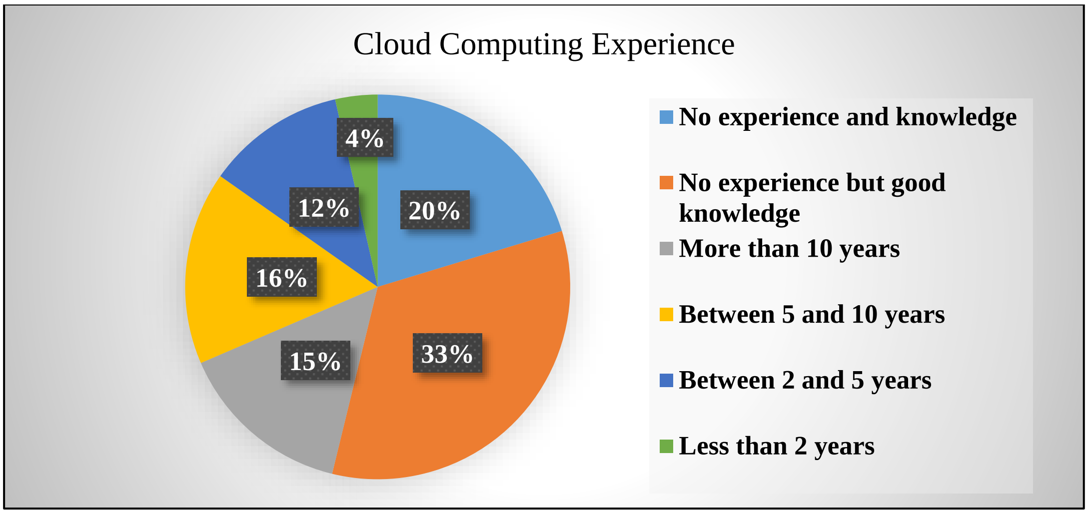

Figure 5.7 The respondent's experience with cloud computing

5.4.3. Data Governance

The respondents were asked to define the term 'data governance'; thus, this section aims to analyse and describe the results of the empirical data findings related to data governance and this is considered to be the second part of the questionnaire survey. The data governance term has been investigated in this part based on its definition, importance and benefits.

- **Data Governance Definition**

There is no official definition of data governance in the literature; thus, this study adopts the popular data governance definition that has been defined by the Data Governance Institute (DGI). The DGI defines data governance as "*the framework for decision rights and accountabilities to encourage desirable behavior in the use of data, to promote desirable behavior, data governance develops and implements corporate-wide data policies, guidelines, and standards that are consistent with the organization's mission, strategy, values, norms, and culture*" (Thomas, 2009).

The goal of the data governance definition question is to investigate and understand if this definition agrees with the concept of data governance in public sector organisations in Saudi Arabia. The approach taken by Kooper et al. (2011) was adopted to measure the information governance definition status in organisations based on the IBM definition. The responses to the data governance definition question were classified as follows:

- The definition is essentially the same in my organisation.
- My organisation has another definition.
- My organisation has no definition for data governance.

- Do not know.

The respondents were asked to describe areas where their organisation's definition of data governance differed from that of the DGI. Figure 5.8 provides a pie chart detailing the participants' responses.

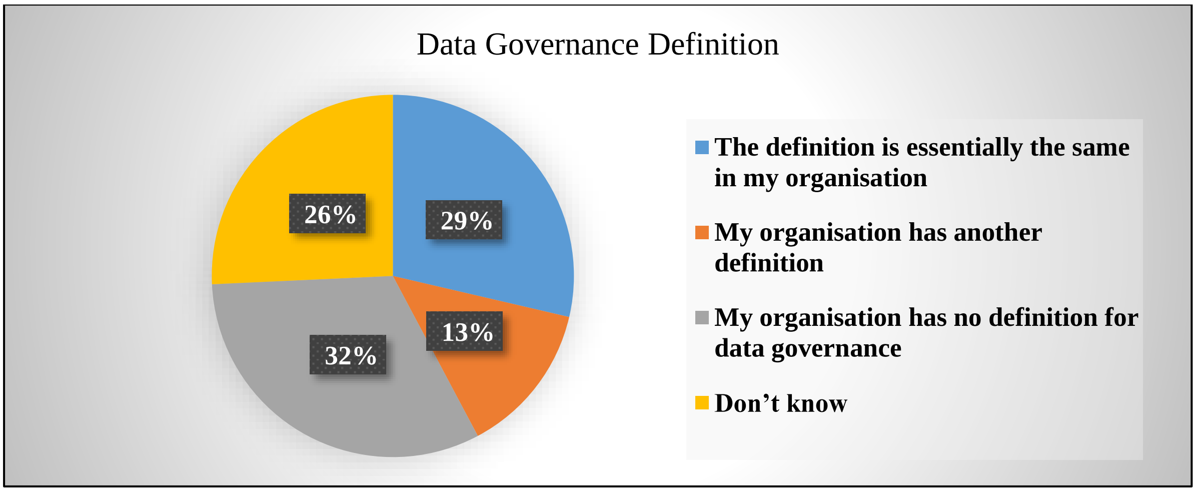

Figure 5.8 The respondents' answers regarding the data governance definition

- **Importance of Implementing a Data Governance Programme**

To identify the importance of implementing a data governance programme in the organisation, the survey asked the respondents to indicate the importance of doing so in their own organisation. The responses to the data governance definition question were classified as follows: important, not important and do not know. The results are illustrated in Figure 5.9.

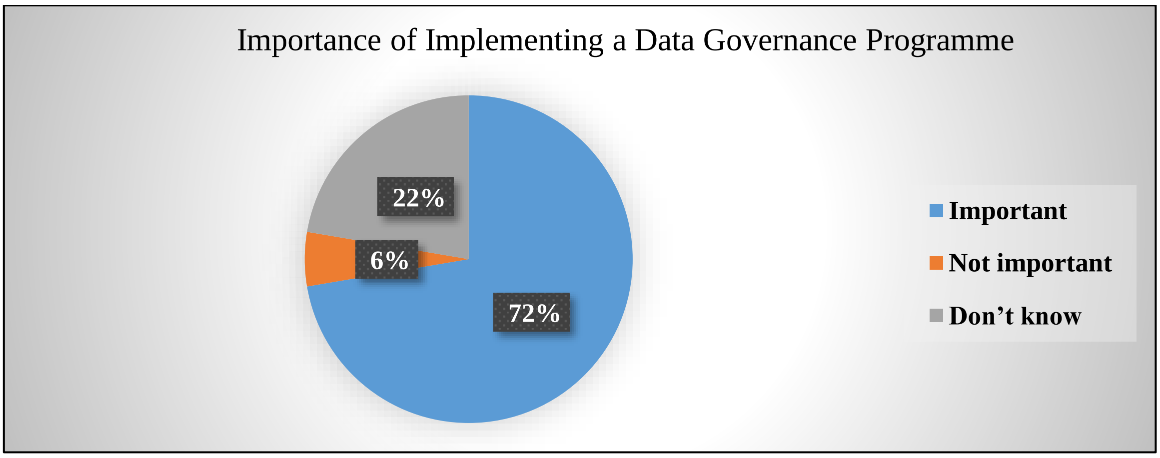

Figure 5.9 The respondents' answers regarding the importance of implementing a data governance programme

- **Benefits from Implementing a Data Governance Programme in Organisations**

In terms of the benefits to be gained from implementing a data governance programme, the respondents were asked to assess the value of data governance in achieving specific benefits from their perspectives. In the literature, a few sources highlight some benefits of data governance, and most of the literature presents governance and information governance benefits (Salido et al. 2010; Debreceny & Gray 2013; Medved, 2014). Thus, based on the different benefits that have been proposed in the literature, this study reviews and identifies the most common benefits listed in the literature of implementing data governance in organisations. These benefits have been assessed by the respondents. All participants used the scale of 1 to 5 (5 = essential and 1 = not at all valuable). The results show that more than 60% of the respondents see the high value of data governance (rated "essential" or "very valuable", 5 or 4) with mean =>3.95 (see Table 5.2).

Table 5.2 Data governance benefits for Saudi Arabia's public sector

Benefits / Scale	Essential	Very valuable	Valuable	Somewhat valuable	Not at all valuable	Statistical	
	%	**%**	**%**	**%**	**%**	**Mean**	**S.D**
Data can be a strategic asset	60.91	28.93	7.11	2.54	0.51	4.47	0.78
Data governance ensures trusted and used of data to make decisions	59.39	30.46	7.11	1.52	1.52	4.45	0.81
Data Governance can ensure data quality	57.87	28.93	8.63	3.55	1.02	4.39	0.86
Data Governance can ensure policy compliance	50.25	28.93	16.24	3.55	1.02	4.24	0.92
Data Governance can ensure repeatable business processes	37.06	31.98	23.86	3.55	3.55	3.95	1.03
Data Governance can ensure cross functional collaboration	42.64	36.04	16.24	4.06	1.02	4.15	0.91
Data Governance can ensure change awareness throughout the organisation	45.69	38.07	12.18	2.54	1.52	4.24	0.87
Governance leverages data to achieve operational goals	50.76	29.44	16.24	3.05	0.51	4.27	0.87
Cost issues can be reduced by data governance	46.70	31.98	15.23	3.55	2.54	4.17	0.98
Making data consistent	51.27	30.46	13.71	3.55	1.02	4.27	0.90
Data governance can be Improving business planning	52.79	32.99	11.17	2.03	1.02	4.35	0.83
Data governance can be improving financial performance	49.75	32.49	12.69	4.06	1.02	4.26	0.90

5.4.4. Cloud Computing Adoption

This section aims to investigate cloud computing adoption in public sector organisations in Saudi Arabia. The respondents were asked to specify the current state of cloud computing adoption in their organisations in terms of its general state, deployment model state and cloud service delivery models. In addition, cloud computing benefits and concerns were considered in the questionnaire survey.

- **The Current State of Cloud Computing**

The current state of cloud computing refers to the extent to which cloud computing has been adopted in public sector organisations in Saudi Arabia. This study adopted the measurement approach to investigate cloud computing adoption status, as described by Oliveira et al., (2014). The current state of cloud adoption was measured using closed questions (Yes, No, Don't Know). With regard to the option “No”, sub-question options were added in order to investigate the organisation’s plan for adopting cloud computing. The results show that only 29% of the participants reported that their organisations have adopted cloud computing services. The results are shown in Figure 5.10.

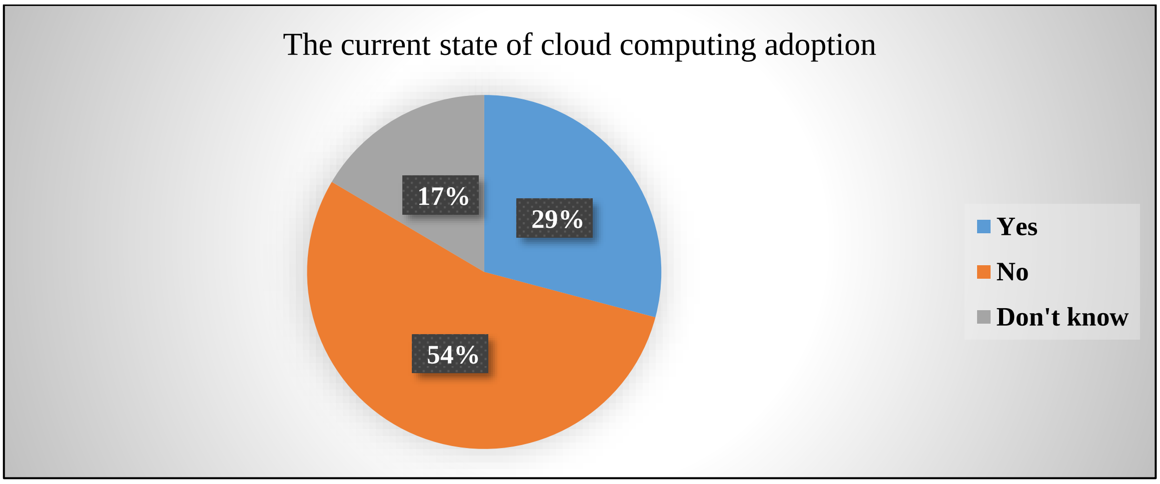

Figure 5.10 The current state of cloud computing adoption by Saudi Arabia’s public sector

With regard to the participants who reported that their organisations had not adopted cloud computing, further data was obtained from the sub-questions. The results show that 33.50 % of the other public sector organisations in Saudi Arabia are planning to adopt cloud computing in the next two years. The results are shown in Figure 5.11.

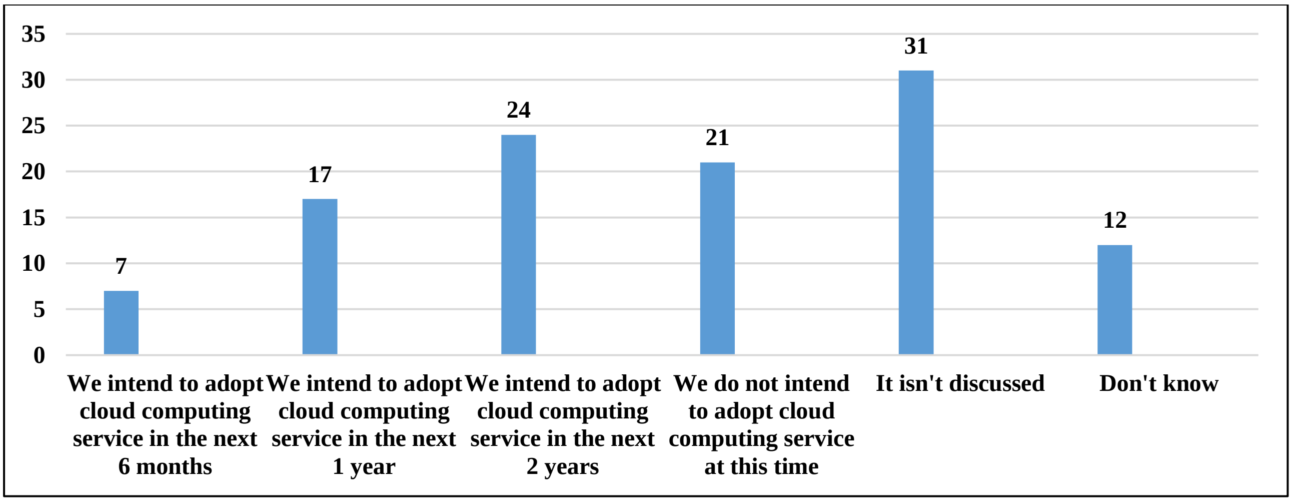

Figure 5.11 Organisations' plans for cloud computing adoption in Saudi Arabia's public sector

- **Cloud Computing Deployment Model Adoption**

To identify the cloud deployment model adoption, the questionnaire asked the respondents who had reported that their organisations had already adopted some cloud computing services to describe the type of deployment model adopted. The question was formulated based on multiple-choice questions to allow the respondents to choose all the cloud deployment model types that had been adopted by their organisations. The results are shown in Figure 5.12.

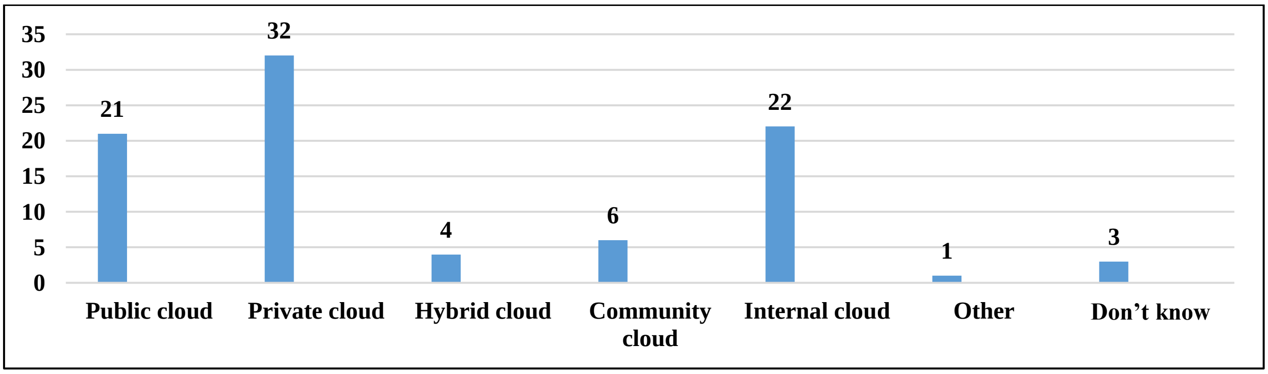

Figure 5.12 Cloud computing deployment models adopted by Saudi Arabia's public sector

- **Cloud Service Delivery Model Adoption**

To identify the cloud service delivery model adoption, the questionnaire asked the respondents who reported that their organisations had already adopted some cloud computing services to describe the type of service delivery model adopted. The question was formulated based on multiple-choice questions to allow the respondents to choose all the cloud service delivery model types that had been adopted by their organisation. The results are shown in Figure 5.13.

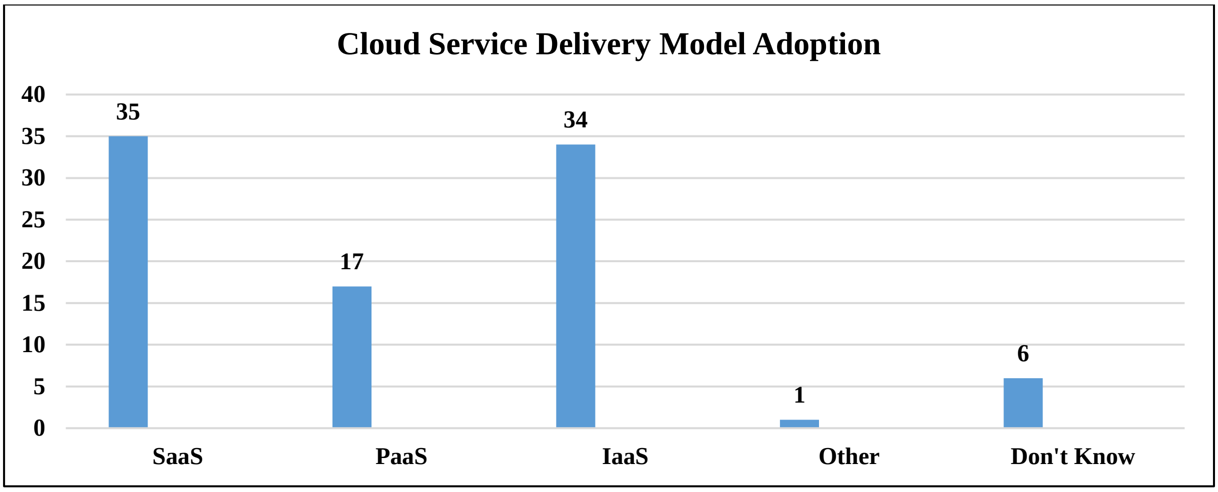

Figure 5.13 The type of cloud service delivery models adopted by Saudi Arabia's public sector

- **Organisation's Data is Stored in the Cloud**

The questionnaire asked the respondents who reported that their organisations had already adopted some cloud computing services to describe the percentage of the organisation's data that is stored in the cloud environment. The results are shown in Figure 5.14.

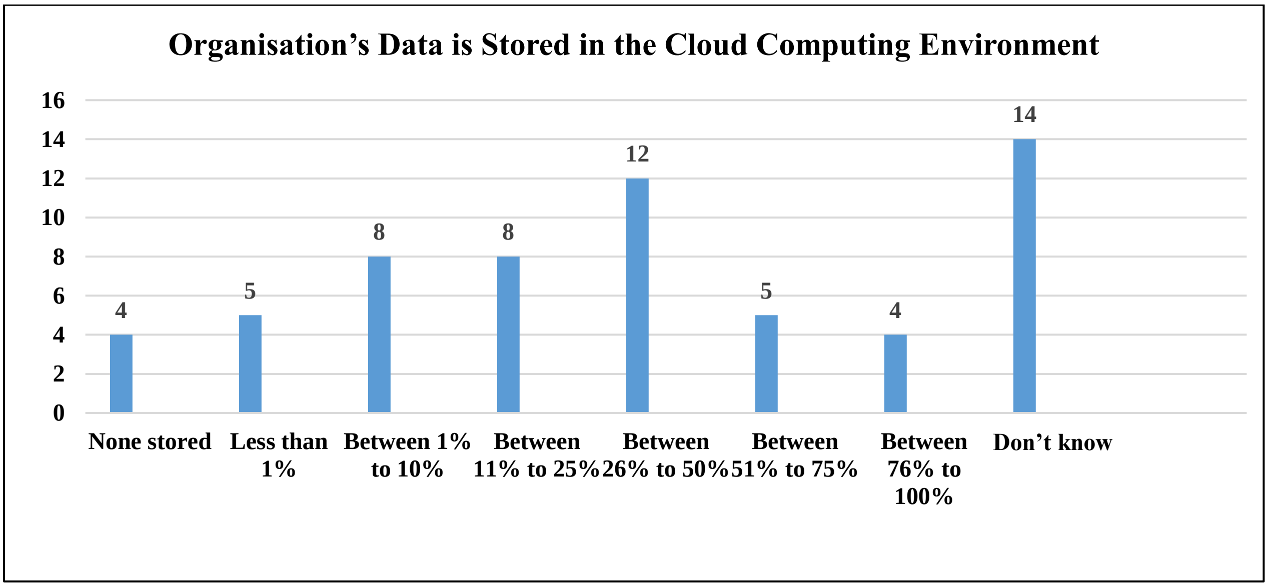

Figure 5.14 Percentage of an organisation's data that is stored in the cloud computing environment in Saudi Arabia's public sector

In terms of the percentage of an organisation's data stored in a cloud environment that is not managed or controlled by the organisation's specialist, this question was answered by 60 respondents whose organisations had adopted cloud computing. The results are shown in Figure 5.15.

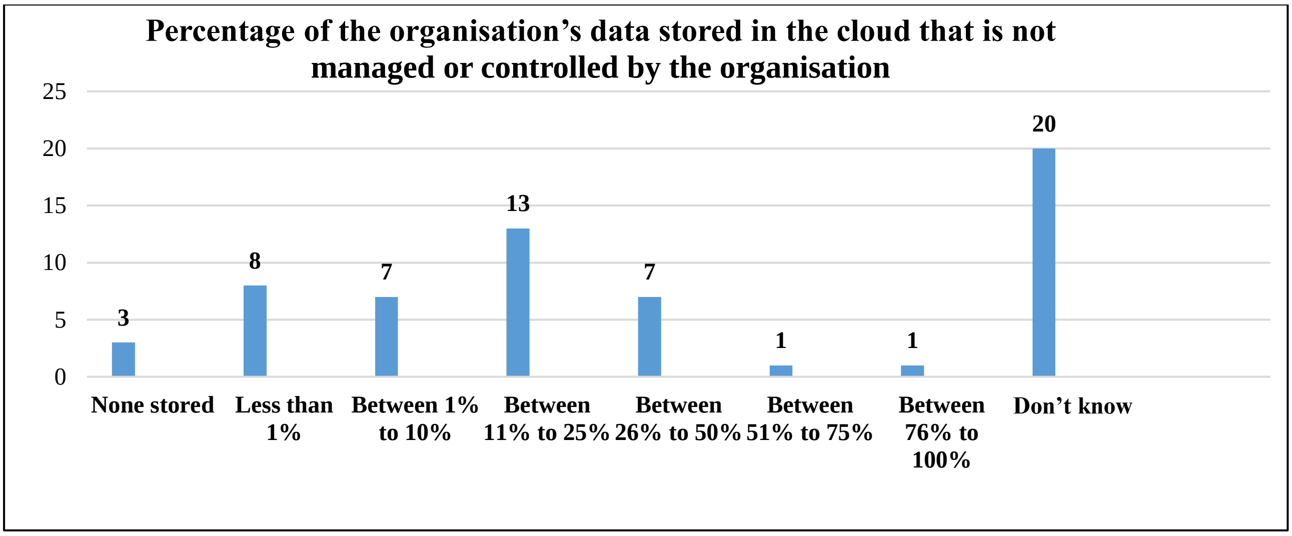

Figure 5.15 Organisation's data stored in the cloud that is not managed or controlled by the organisation in Saudi Arabia's public sector

- **Data Classification in Cloud Computing**

Regarding classifying an organisation's data in a cloud computing environment based on its sensitivity, this question was answered by 60 respondents whose organisations had adopted cloud computing. The results show that only 32% of the participants reported that their organisations have classifying their data in cloud computing. Figure 5.16 shows the state of data classification in cloud computing.

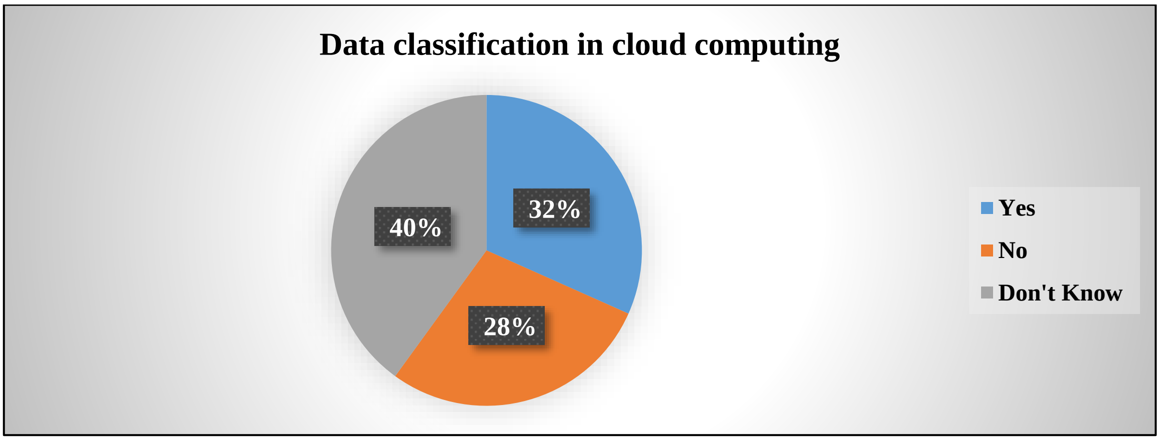

Figure 5.16 State of data classification in cloud computing in Saudi Arabia's public sector

- **Type of Knowledge/Lack of Expertise within the Organisation regarding Cloud Computing**

The aim of this question was to investigate the type of knowledge/lack of expertise/ regarding cloud computing within organisations that were adopting cloud computing. The question was answered by 60 respondents and it allowed them to tick the appropriate multiple-choice response. Figure 5.17 shows the results.

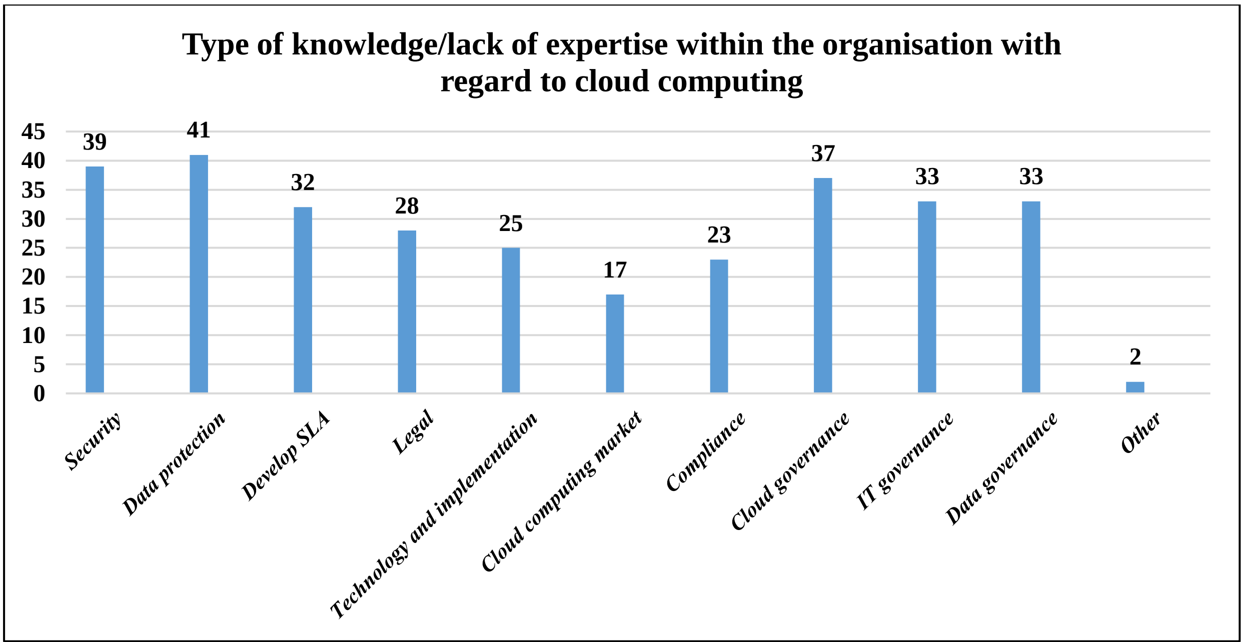

Figure 5.17 Type of knowledge/lack of expertise within the organisation with regard to cloud computing in Saudi Arabia's public sector

- **The Level of Concern in the Organisation when adopting Cloud Computing**

Cloud computing is a recent stage in the ICT evolution of recent decades, and it brings some benefits to organisations (Maaref, 2012; Khalil et al., 2014). Although cloud computing offers a range of benefits, decision makers are influenced by a number of concerns when deciding whether or not to adopt cloud computing (Rajvanshi et al., 2013; Merrill & Kang, 2014; Khalil et al., 2014). In the literature, some sources highlight the cloud computing concerns that are influencing the adoption of cloud computing in organisations. Therefore, based on the cloud computing concerns extracted from the literature, the study identified the common concerns, and the respondents were asked to assess these concerns from their perspectives. Based on the obtained results, there seems to be a general agreement among all participants (=> 53%) that the majority of the identified concern are significant concerns for adopting cloud computing in the public sector in Saudi Arabia, with mean =>3.47. Table 5.3 shows the cloud computing concerns based on the participants' responses.

Table 5.3 Cloud computing concerns Saudi Arabia's public sector

Concerns / Scale	**Extremely concerned**	**Moderately concerned**	**Somewhat concerned**	**Slightly concerned**	**Not at all concerned**	**Mean**
	%	%	%	%	%	
Insufficient financial benefits	27.41	26.90	21.32	13.71	10.66	3.47
Immature Cloud Computing	38.07	22.34	23.35	9.64	6.60	3.76
Not know where their data is being held	44.67	23.86	16.75	7.61	7.11	3.91

Concerns / Scale	Extremely concerned	Moderately concerned	Somewhat concerned	Slightly concerned	Not at all concerned	Mean
	%	%	%	%	%	
Lack of functionalities	30.96	26.40	26.90	12.69	3.05	3.69
Lack of performance	30.96	29.95	21.83	13.71	3.55	3.71
Loss of control	44.16	27.92	17.26	8.60	2.03	4.04
Loss of data governance	43.15	27.92	18.27	9.64	1.02	4.03
Vendor lock-in	30.96	22.84	32.99	8.63	4.57	3.67
Insecure availability	31.98	29.95	23.86	10.66	3.55	3.80
Integration issues	27.92	32.49	25.89	8.63	5.08	3.70
Trust issues	47.21	27.41	16.75	5.08	3.55	4.10
Privacy issues	50.25	28.43	12.18	4.06	5.08	4.15
Compliance issues	31.47	36.04	22.34	7.11	3.04	3.86
Legal issues	39.09	34.01	15.74	6.09	5.07	3.96
Security issues	48.22	24.37	17.77	5.08	4.56	4.07

5.4.5. Cloud Data Governance

Cloud computing is an emerging technology, and recently it has been receiving a great deal of attention in government organisations (Smitha et al., 2012). There are differences between cloud computing and a traditional infrastructure (on the organisation's premises), as the cloud makes it possible to access information from anywhere at any time, while a traditional infrastructure setup requires the organisation or person wishing to access the data to be in the same location as the data storage device – the cloud takes away that step (Huth & Cebule, 2014). Part of the empirical study focused on the implementation of a data governance programme for cloud computing in public sector organisations in Saudi Arabia. The study aimed to obtain sufficient information about the current state of cloud data governance programmes in public sector organisations and their perspective regarding cloud data governance. The gathered data can be processed in three categories centred on the current state of cloud data governance, and the barriers and obstacles that are preventing organisations from implementing a cloud data governance programme. Additionally, the CSFs for implementing a cloud data governance programme have been investigated in this study.

- **Cloud Computing Brings New Issues for Data Governance Compared to Traditional Infrastructure**

The questionnaire asked the respondents to describe whether cloud computing brings new issues for data governance compared to traditional infrastructure (on the premises). The results show that most of the participants (58%) agree the cloud computing brings new issues for data governance. Figure 5.18 shows the respondents' answers.

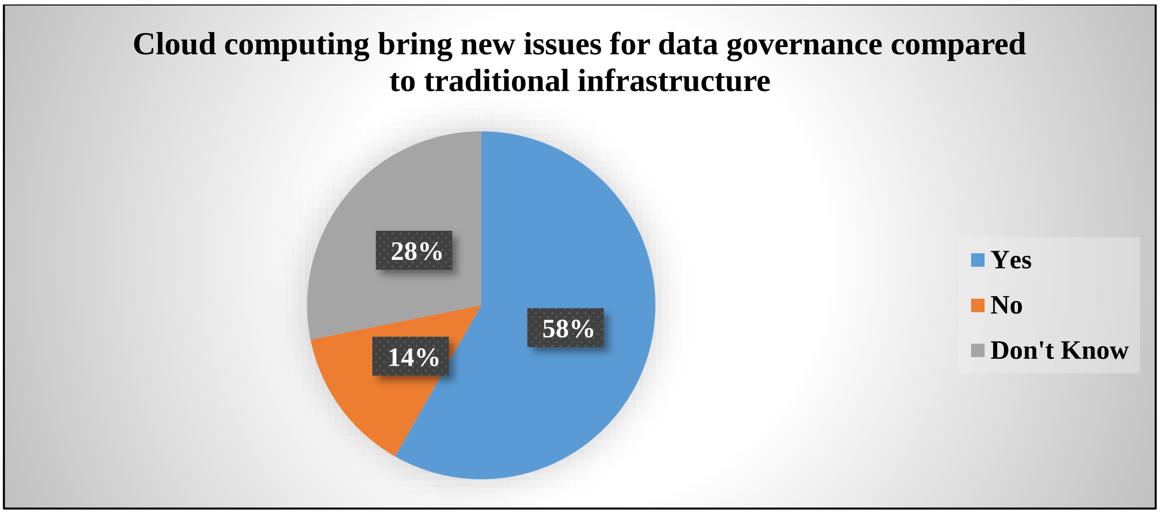

Figure 5.18 Cloud computing brings new issues for data governance compared to traditional infrastructure (on the premises)

- **The Current State of Cloud Data Governance Programme Implementation**

The current state of cloud data governance refers to the extent of cloud data governance programme implementation in public sector organisations in Saudi Arabia. Kooper et al. (2011) adopted an approach to measure information governance status in IBM. Therefore, this study adopted this measurement approach to investigate the current state of cloud data governance programme implementation in public sector organisations in Saudi Arabia. This was measured using closed questions (Yes, No, Don't Know). The results show that only 14% of the participants reported that their organisations have implemented cloud data governance programme. Figure 5.19 shows the current state of implementation of cloud data governance programmes.

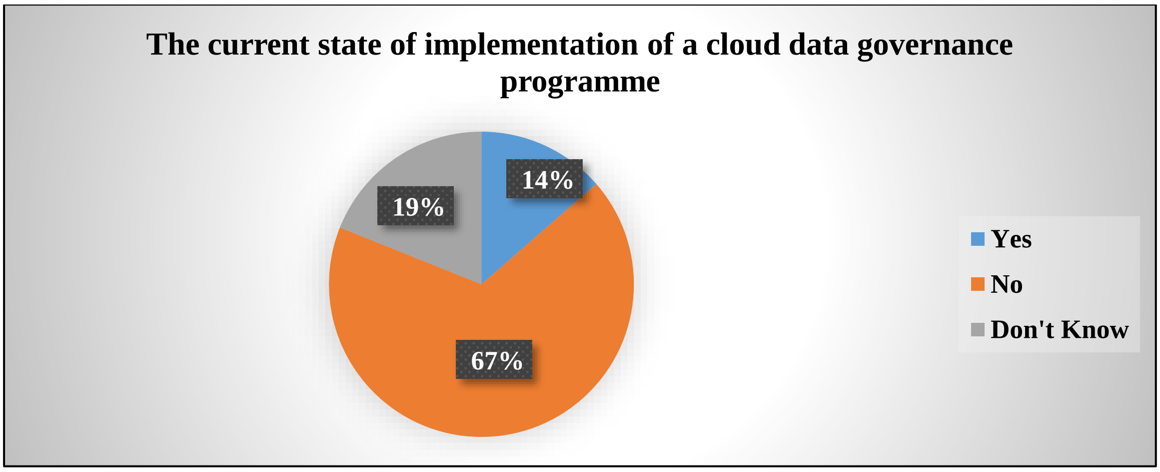

Figure 5.19 The current state of implementation of a cloud data governance programme in Saudi Arabia’s public sector

Further data was obtained from those participants who reported that their organisation had not implemented a cloud data governance programme, via sub-questions. The results show that 25.89 % of the other public sector organisations in Saudi Arabia are planning to implement cloud data governance programme in the next two years. The results are shown in Figure 5.20.

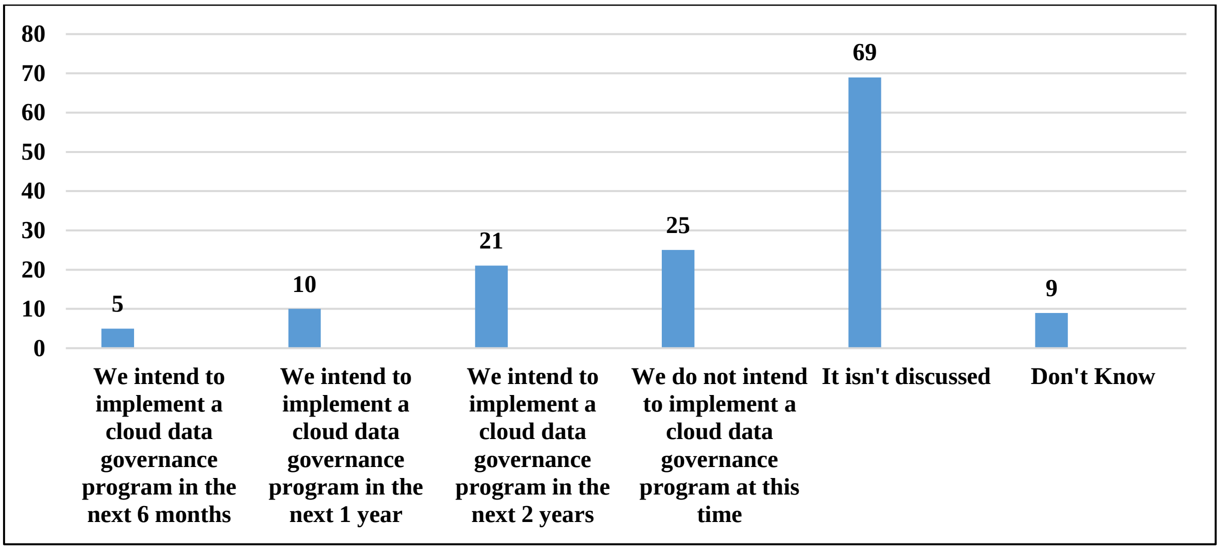

Figure 5.20 The current state of implementation of a cloud data governance programme by Saudi Arabia's public sector

- **The Levels of the Cloud Data Governance Process Within the Organisations**

To investigate the levels of cloud data governance in the organisations that had implemented a cloud data governance programme, the questionnaire asked the respondents to describe the level of the cloud data governance programme achieved in their organisations. This question was answered by 28 respondents. Based on the CMM, five levels define a scale for measuring the maturity of an organisation's software processes; these levels are Initial, Repeatable, Defined, Managed and Optimised (Software Engineering Institute, 2010). Therefore, this study adopted this measurement approach to investigate the levels of cloud data governance process within public sector organisations in Saudi Arabia. Moreover, the 'Don't know' option was also included in the responses to this question. The results show that the cloud data governance implementation in the Saudi organisations is still in initial level and it needs more efforts to get to the high maturity level of cloud data governance. Figure 5.21 shows the levels of cloud data governance processes within Saudi organisations.

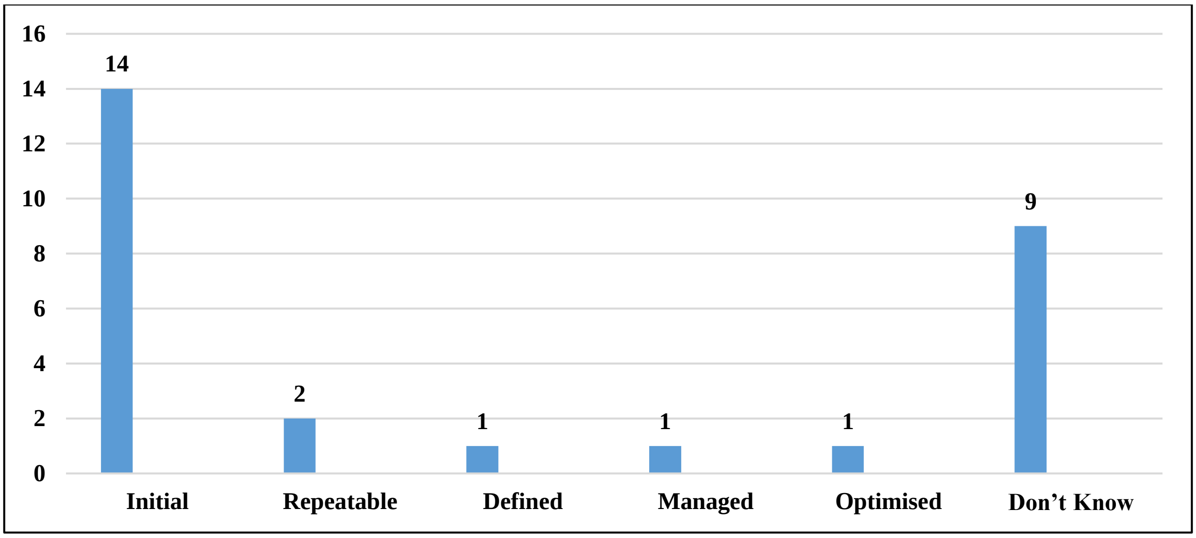

Figure 5.21 The levels of the cloud data governance processes within Saudi organisations

- **The Source of Threats to the Cloud Data Governance Profile**

The aim of this question was to understand the source of threats to the cloud data governance profile in the respondents' organisations; this question was answered by 28 respondents who were implementing cloud data governance programmes in their organisations. Figure 5.22 shows the source of threats to the cloud data governance profile.

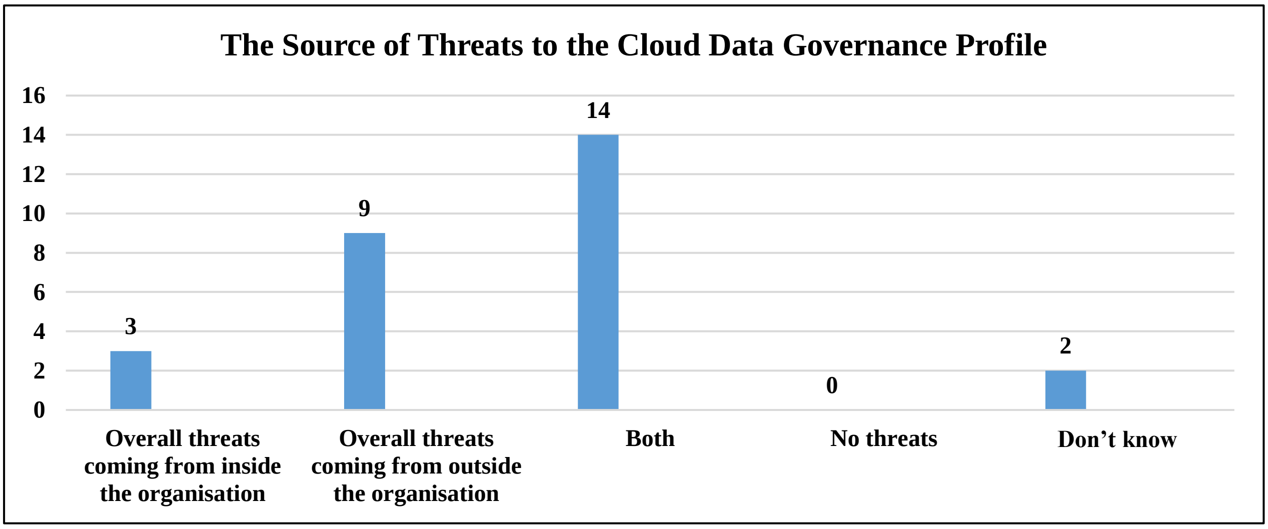

Figure 5.22 The source of threats to the cloud data governance profile in Saudi Arabia's public sector

5.4.6. CSFs for Implementing Cloud Data Governance in Saudi Arabia

The literature review identified different CSFs related to data governance. These were therefore analysed and extracted; some of the CSFs were mentioned in the same expression but in different meanings or contexts. This study has dealt with CSFs based on their meanings or contexts. In addition, these factors have been classified into eight main factors, and under each main factor there are sub-factors. The main factors are namely: organisational (OF), technological (TF), environmental (EF), stakeholder's involvement (SIF), strategic planning (SPF), strategic management (SMF), strategic alignment (SAF), and monitoring & ongoing (MOF). In addition, this study aims to examine those CSFs that influence the implementation of cloud data governance in the public sector in Saudi Arabia. In the survey, the questions were presented as variables with coding options where applicable. A Likert scale was coded from 1 to 5, with 1 representing "Strongly Agree", and 5 representing "Strongly Disagree". This section analyses the findings of our study related to the CSFs. The study uses statistical tests to measure the respondents' answers – mean, standard deviation (SD) and variance. To recall, Table 5.4 presents all identified CSFs.

Table 5.4 All identified CSFs of cloud data governance

Code	CSFs
OF1	Setting up a clear cloud data governance office structure
OF2	Ongoing funding for cloud data governance requirements
OF3	Improvement of staff's skills and experience in cloud data governance
OF4	Top management support for cloud data governance implementation
OF5	Business case
OF6	Leadership and commitment of top management to the adoption of a risk management strategy for the organisation
TF1	Integrate data governance functions with cloud deployment model features
TF2	Integrate data governance functions with cloud service delivery model features
TF3	Data risk in cloud computing is assessed and managed on time
TF4	Automation of cloud data governance
EF1	Building cloud data governance into the SLA of the cloud computing project
EF2	Support compliance enforcement to implement cloud data governance
EF3	Regulatory environment & compliance requirements to support cloud data governance implementation
SIF1	Involvement of board of directors & top management support and ownership to support the implementation of cloud data governance
SIF2	Involvement of cloud provider in cloud data governance
SIF3	Involvement of other cloud actors in cloud data governance (cloud broker, cloud auditor, cloud carrier)
SPF1	Analysis and evaluation of the current state of cloud data governance
SPF2	Identify and articulate priorities to implement cloud data governance
SPF3	Setting up a clear cloud data governance mission and vision
SPF4	Setting up a clear communication plan
SPF5	Setting up a clear change management plan to implement cloud data governance
SPF6	Defining data value
SPF7	Classify data in the cloud
SMF1	Setting up clear cloud data governance policies
SMF2	Setting up clear cloud data governance procedures

SMF3	Setting up clear cloud data governance standards
SMF4	Setting up clear cloud data governance processes
SMF5	Defining clear roles and responsibilities for cloud data governance team
SMF6	Configuring cloud data governance programme activities
SMF7	Regular communication with all cloud data governance participants
SMF8	Create a clear risk management strategy
SAF1	Effective alignment with cloud computing regulation
SAF2	Effective alignment with organisation's strategy
SAF3	Effective alignment with business strategy
SAF4	Effective alignment with IT strategy
SAF5	Effective alignment with environmental strategy
SAF6	Effective alignment with corporate governance
SAF7	Effective alignment with IT governance
SAF8	Effective alignment with other strategies
MOF1	Measuring and reporting for continuous improvement of cloud data governance
MOF2	Training and education of the organisation's staff on the cloud data governance programme
MOF3	Execute a cloud data governance change plan

Table 5.5 shows the analysis of CSFs affecting the implementation of cloud data governance in the Saudi public sector, based on the participants' responses to the designated questionnaire, provided in (Appendix E). Based on the obtained results, there seems to be a general agreement among all participants (=> 73%) that all of the identified CSFs are significantly important for implementing effective cloud data governance in the public sector in Saudi Arabia, with mean =>4. One can notice that for two CSFs, *SPF6 and TF1*, at least 20% of the respondents were neutral.

Table 5.5 Statistical analysis of CSFs affecting cloud data governance implementation in the Saudi public sector

CSFs / Scale	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Statistical		
	%	%	%	%	%	Mean	S.D	Variance
OF1	48.22	32.99	15.74	2.54	0.51	4.18	0.85	0.72
OF2	42.64	32.99	19.80	3.55	1.02	4.13	0.92	0.84
OF3	49.24	33.50	13.71	3.05	0.51	4.28	0.85	0.72
OF4	46.70	34.01	16.75	2.54	0.00	4.25	0.82	0.67
OF5	43.65	37.06	16.75	1.52	1.02	4.21	0.84	0.71
OF6	46.19	35.53	14.21	3.05	1.02	4.23	0.87	0.77
TF1	36.04	39.09	20.81	3.55	0.51	4.13	0.87	0.75
TF2	47.72	34.52	15.23	1.52	1.02	4.29	0.85	0.72
TF3	44.16	37.56	16.24	2.03	0.00	4.22	0.83	0.68
TF4	46.19	34.52	17.77	1.52	0.00	4.26	0.84	0.71

CSFs / Scale	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Statistical		
	%	%	%	%	%	Mean	S.D	Variance
EF1	46.19	32.99	16.24	4.57	0.00	4.21	0.87	0.76
EF2	40.61	39.59	17.26	2.03	0.51	4.18	0.82	0.67
EF3	41.12	38.58	16.24	3.55	0.51	4.16	0.86	0.74
SIF1	45.18	32.99	18.27	2.54	1.02	4.19	0.89	0.79
SIF2	38.58	41.62	15.74	2.54	1.52	4.07	0.87	0.75
SIF3	46.19	35.53	16.24	1.52	0.51	4.14	0.92	0.85
SPF1	40.61	41.12	15.23	1.52	1.52	4.18	0.85	0.72
SPF2	45.69	32.49	16.24	5.08	0.51	4.18	0.91	0.84
SPF3	44.67	36.55	14.72	4.06	0.00	4.23	0.84	0.71
SPF4	43.65	38.07	14.72	2.54	1.02	4.21	0.86	0.73
SPF5	43.65	37.06	16.75	1.52	1.02	4.21	0.84	0.71
SPF6	41.12	31.98	21.32	4.57	1.02	4.08	0.94	0.89
SPF7	47.21	30.46	17.77	4.57	0.00	4.20	0.89	0.79
SMF1	48.22	35.53	13.71	1.02	1.52	4.28	0.85	0.72
SMF2	47.21	36.55	13.20	2.54	0.51	4.27	0.82	0.68
SMF3	48.73	34.01	14.21	2.03	1.02	4.27	0.85	0.73
SMF4	45.18	36.55	16.24	1.52	0.51	4.24	0.81	0.66
SMF5	48.22	35.53	12.69	2.03	1.52	4.27	0.87	0.76
SMF6	42.13	37.06	15.23	4.06	1.52	4.13	0.92	0.85
SMF7	43.65	38.07	15.74	2.03	0.51	4.22	0.82	0.67
SMF8	49.24	35.03	12.18	2.54	1.02	4.29	0.85	0.72
SAF1	50.25	32.49	13.71	3.55	0.00	4.29	0.83	0.70
SAF2	44.67	36.55	15.23	2.54	1.02	4.21	0.86	0.75
SAF3	45.69	34.01	17.26	2.03	1.02	4.21	0.87	0.76
SAF4	50.76	29.44	17.77	2.03	0.00	4.29	0.83	0.68
SAF5	49.24	32.49	15.74	2.54	0.00	4.28	0.82	0.67
SAF6	49.75	31.47	16.75	1.52	0.51	4.28	0.83	0.69
SAF7	46.19	35.03	16.24	2.03	0.51	4.24	0.83	0.69
SAF8	42.13	34.52	19.80	2.54	1.02	4.14	0.89	0.79
MOF1	50.76	32.99	13.20	1.52	1.52	4.30	0.86	0.75
MOF2	39.59	39.09	15.74	5.58	0.00	4.13	0.87	0.76
MOF3	44.67	36.04	16.24	3.05	0.00	4.22	0.83	0.68

Figure 5.23 provides an overall ranking of the importance of the identified CSFs for implementing cloud data governance in the Saudi public sector, based on the participants' responses. To do this, an overall mean for each main factor was calculated.

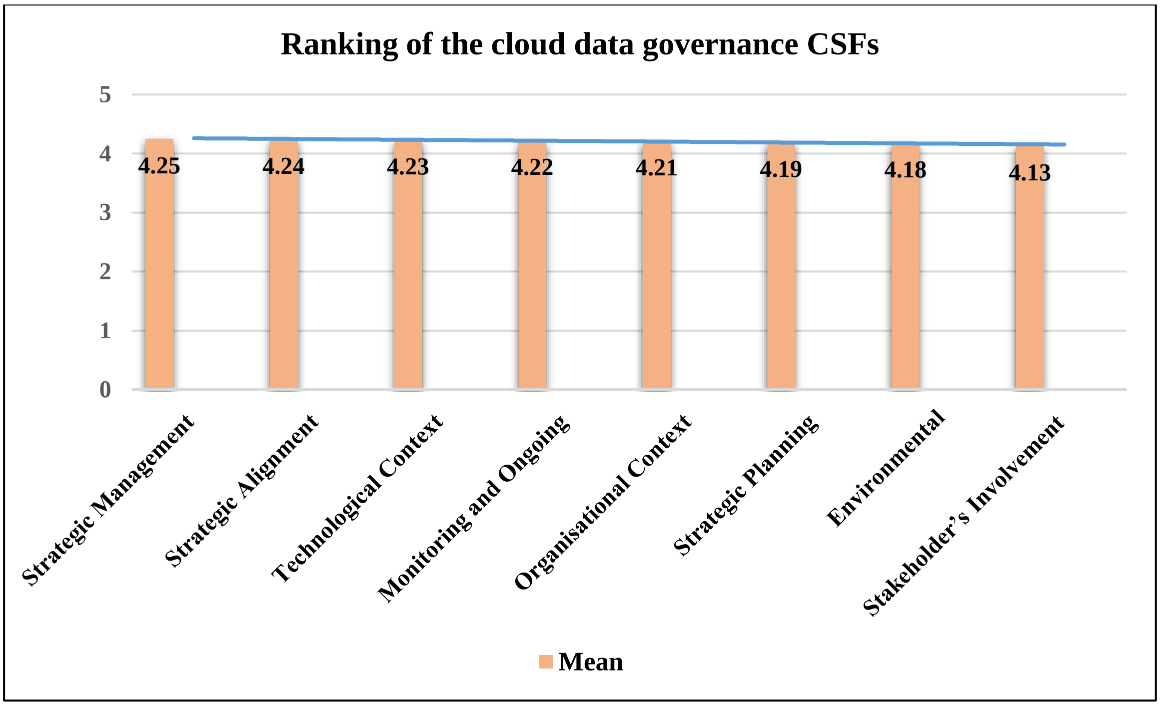

Figure 5.23 Ranking of the cloud data governance CSFs from the perspective of the Saudi Arabian public sector

5.4.7. Barriers to Implementing Cloud Data Governance in Saudi Arabia

The literature review found that different barriers related to data governance have been discussed in different sources. Therefore, this study has analysed and extracted those barriers; some of those barriers have been mentioned in the same expression but in different meanings or contexts. This study has dealt with them based on their meanings or contexts. In addition, those barriers have been classified into eight main barriers, and under each main barrier there are sub-barriers. The main barriers are namely: organisational (OB), Technological (TB), Environmental (EB), Functional (FB), Financial (FIB), Cultural (CB), Human (HB) and Knowledge (KB). The sub-barriers have been coded based on the main category code. In the survey, the questions were presented as variables with coding options where applicable. A Likert scale was coded from 1 to 5, with 1 representing 'Strongly Agree', and 5 representing 'Strongly Disagree'. This section analyses the findings of our study related to the barriers to the implementation of cloud data governance. The study uses statistical tests to measure the respondents' answers by mean, standard deviation (SD) and variance. To recall, Table 5.6 presents all identified barriers.

Table 5.6 All identified barriers of cloud data governance

Code	Barriers
OB1	The priority of cloud data governance compared to other projects
OB2	The inability to communicate the business value of cloud data governance
OB3	Lack of focus on cloud data governance charter, mission and vision within the organisation.
OB4	Designing a communication plan.
OB5	The change management plan
OB6	Lack of a cloud data governance office in the organisation
OB7	Organisations do not view data as a strategic asset in the organisation
OB8	Lack of time to implement cloud data governance in the organisation
OB9	Cloud computing not quite adopted in the organisation
TB1	Cloud data governance being perceived as too complex
TB2	Lack of technology used to implement and monitor cloud data governance in the organisation
TB3	The complexity of storage and processing data in the cloud
TB4	Complexity of the cloud deployment models
TB5	Complexity of the cloud service delivery models
TB6	Lack of simple mechanisms to assess the trustworthiness of potential partners
EB1	Lack of compliance enforcement in the organisation
EB2	Cloud data governance is not built into the SLA of the cloud computing service with the cloud provider
EB3	Compliance hazard
EB4	Lack of cloud regulation
FB1	Lack of focus on cloud data governance policies
FB2	Lack of focus on cloud data governance procedures
FB3	Lack of focus on cloud data governance processes
FB4	Lack of focus on defined roles and responsibilities for cloud actors within the organisation
FIB1	Lack of financial resources
FIB2	Cost
CB1	The cloud data governance is not part of most Saudi Arabian organisations' culture
CB2	Resistance to change
KB1	The organisations do not know where to start when they intend to implement cloud data governance
KB2	Lack of knowledge about cloud data governance
KB3	Lack of training on the cloud data governance programme in the organisation
KB4	Lack of understanding of how to create a communication plan for cloud data governance in organisations
KB5	Lack of understanding of how to build cloud data governance matrices and measures in the organisation
HB1	Lack of people who support the implementation of cloud data governance in the organisation
HB2	Lack of executive and stakeholder support
HB3	Lack of people who have skills and experience to implement cloud data governance in the organisation

Table 5.7 shows the analysis of the barriers affecting cloud data governance implementation in the Saudi public sector, based on the participants' responses to the designated questionnaire, provided in (Appendix E). Based on the obtained results, there seems to be a general agreement among all participants (=> 58%) that the majority of the identified barriers are significant barriers for implementing effective cloud data governance in the public sector in Saudi Arabia, with mean =>3.35. There is one exception – the lack of time to implement cloud data governance in the organisation (OB8). The results show that the majority of respondents (81.73%) do not believe that this is a barrier to implementing cloud data governance in the public sector in Saudi Arabia (mean = 2.46).

Table 5.7 Statistical analysis of the barriers affecting cloud data governance implementation in the Saudi public sector

Barriers / Scale	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Statistical		
	%	%	%	%	%	Mean	S.D	Variance
OB1	44.16	32.49	15.74	5.58	2.03	4.11	1.00	.99
OB2	37.06	36.04	20.81	5.08	1.02	4.03	.88	.77
OB3	43.15	35.03	19.29	1.02	1.52	4.17	.93	.87
OB4	39.09	38.07	18.27	3.05	1.52	4.10	.88	.77
OB5	38.58	33.50	21.83	4.06	2.03	4.03	.91	.82
OB6	45.18	31.98	17.26	2.54	3.05	4.14	.97	.95
OB7	34.52	31.98	23.86	6.60	3.05	3.88	1.05	1.11
OB8	12.18	6.09	25.38	27.92	28.43	2.46	1.29	1.67
OB9	41.12	30.96	21.83	4.57	1.52	4.06	.97	.95
TB1	33.50	31.47	25.89	6.60	2.54	3.87	1.03	1.07
TB2	33.50	28.93	23.86	9.64	4.06	3.88	1.13	1.28
TB3	32.99	26.90	27.41	10.15	2.54	3.88	1.09	1.19
TB4	23.86	34.01	30.96	7.11	4.06	3.66	1.04	1.09
TB5	26.40	32.49	29.95	8.12	3.05	3.71	1.04	1.08
TB6	34.52	33.50	24.87	4.57	2.54	3.93	1.00	1.00
EB1	32.99	29.95	31.47	3.55	2.03	3.88	.98	.96
EB2	38.58	28.93	25.89	4.57	2.03	3.97	1.00	1.01
EB3	29.95	29.44	34.01	5.08	1.52	3.81	.97	.94
EB4	54.31	29.95	12.18	3.55	0.00	3.35	.83	.68
FB1	40.10	34.52	20.81	2.03	2.54	4.08	.96	.91
FB2	40.61	34.52	21.32	1.02	2.54	4.10	.94	.88
FB3	42.64	35.03	17.77	2.54	2.03	4.14	.93	.87
FB4	44.67	31.47	18.78	3.55	1.52	4.15	.95	.89
FIB1	31.98	31.98	17.77	8.12	10.15	3.68	1.28	1.63
FIB2	31.98	28.43	21.83	11.68	6.09	3.69	1.21	1.45
CB1	43.15	31.47	20.30	2.54	2.54	4.10	.98	.95
CB2	51.27	31.47	14.72	2.54	0.00	4.31	.81	.66
KB1	30.96	31.98	24.87	7.61	4.57	3.80	1.11	1.22

Barriers / Scale	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Statistical		
	%	%	%	%	%	Mean	S.D	Variance
KB2	43.65	29.95	19.80	3.55	3.05	4.08	1.02	1.04
KB3	44.67	35.03	15.74	1.52	3.05	4.17	.95	.91
KB4	41.12	32.49	18.78	4.06	3.55	4.04	1.04	1.08
KB5	39.09	31.47	23.35	3.05	3.05	4.01	1.01	1.02
HB1	40.10	33.50	20.30	3.55	2.54	4.05	.99	.97
HB2	40.61	30.96	21.83	5.08	1.52	4.04	.98	.96
HB3	41.62	29.44	20.81	6.60	1.52	4.03	1.01	1.02

Figure 5.24 provides the overall ranking of the importance of the identified barriers for implementing cloud data governance in the Saudi public sector, based on the participants' responses. To do this, an overall mean for each main barrier was calculated.

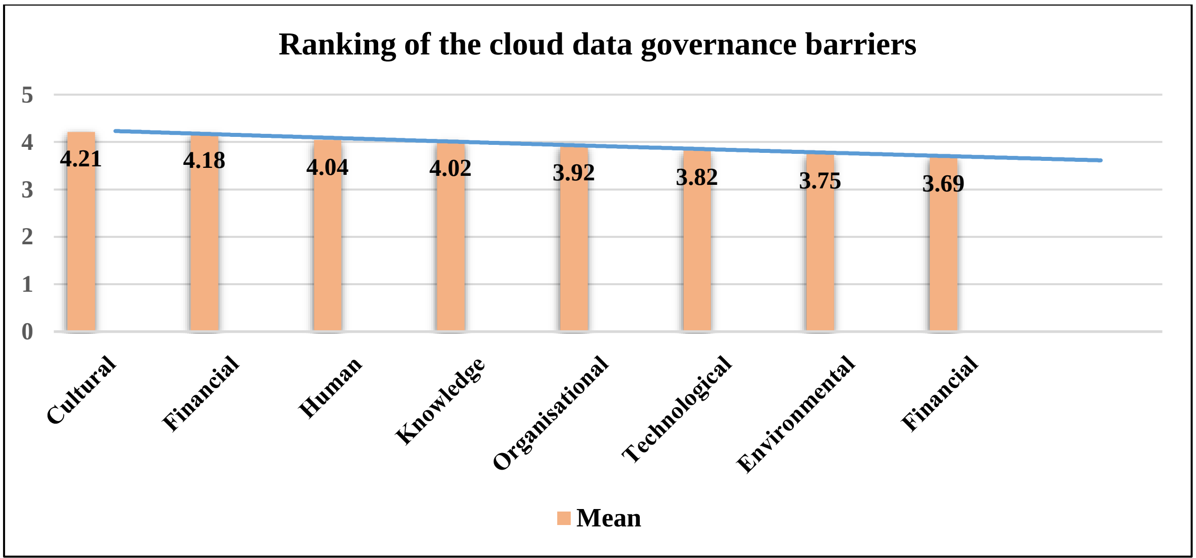

Figure 5.24 Ranking of the cloud data governance barriers from the perspective of the Saudi Arabian public sector

5.5. Chapter Summary

This chapter has discussed and presented the analysis findings of the quantitative data collected from the questionnaire. The questionnaire aimed to identify the current situation of cloud computing adoption and cloud data governance implementation in the public sector organisations of Saudi Arabia. Regarding cloud computing adoption, the results show that only 29% of the participants reported that their organisations have adopted cloud computing services, and 33.50 % of the participants showed that their organisations are planning to adopt cloud computing in the next two years. With regards to a cloud data governance implementation, the results show that only 14% of the participants reported that their organisations have implemented cloud data governance programme, and 25.89 % of the participants showed that their organisations are planning to implement cloud data governance programme in the next two years. Thus, the results show that cloud data governance processes within Saudi organisations are still in initial level. CSFs and barriers that influence the implementation of cloud data governance in Saudi Arabia have also been considered in this questionnaire to support the development of a strategy framework for cloud data governance. Based on the obtained results, there seems to be a general agreement among all participants that the identified CSFs and barriers are influence the implementation of cloud data governance in Saudi Arabia. In addition, cloud data governance CSFs and barriers have been ranked based on the perspective of the Saudi Arabian public sector. The validation and evaluation of the cloud data governance framework will be presented in the following chapter.

Chapter 6. Validation and Evaluation of the Cloud Data Governance Framework

6.1. Introduction

A validation technique is a key part of the framework/model development process; it increases confidence in the framework/model and makes it more valuable (Kennedy et al., 2005). Validation can be defined as "*the process of determining the degree to which a model is an accurate representation of the real world from the perspective of the intended uses of the model*"(Oberkampf & Trucano, 2008, p.719). Therefore, validation provides evidence to substantiate how accurately the computational model simulates the real world for the system of focus. In comparison to the real world, the assessment of accuracy will be provided by expert opinion. In the existing works, many methods have been used to validate frameworks and models, namely: surveys, case studies, questionnaires, focus groups, interviews and workshops (Kennedy et al., 2005; Oberkampf & Trucano, 2008; Fernández & Llorens, 2009). In this research, the proposed framework was validated through a focus group for the Case Study of Saudi Arabia, and the proposed framework was evaluated and assessed by Structural Equation Modelling (SEM) based on the questionnaire finding.

6.2. Design of the Validation Approach

The motivation of this thesis was to support the Saudi Public Section implement effective cloud data governance programmes, therefore the outcomes of the research was validated by for this Case Study. A Focus group approach was adopted for this purpose. This approach is an effective one, for exploring the awareness, behaviour, concerns, beliefs, experiences, motivation, operating practices and intentions related to a particular topic and sub-issues (Freitas et al., 1998). The focus group is particularly useful for generating an in-depth understanding of issues, since a skilled moderator can amplify individual responses through group comments or individual feedback. In addition, a skilled moderator can follow up or probe certain tangents or views that were unanticipated in the design of the moderator's guide, often yielding new information or additional nuances of existing information (Rennekamp & Nall, 2002). The focus group comprised for our case study involved ten (10) participants, all of whom have some experience related to data governance. The data from the focus group and the discussion were documented by writing notes. In addition, a questionnaire was distributed to the focus group members, examining two different types of basic questions: open-ended questions and closed questions. This questionnaire was used to validate the proposed framework and to elicit recommendations, information and knowledge from the participants to improve the framework. The focus group data was analysed to update and improve the proposed framework, in order to produce the final version of the framework. One focus group session was used to validate this work, as follows:

- Conduct one focus group involving participants from government organisations (cloud consumers) and from telecommunication and information technology industry (cloud providers) in Saudi Arabia.
- Distribute the questionnaire to validate the proposed framework in order to:
  - Validate the framework design.
  - Validate the framework phases.
  - Validate the components of the framework phases.
  - Validate the usability of implementing the framework.
  - Obtain suggestions from the participants to improve the cloud data governance framework.
- Perform content analysis of collected data.
- Provide a report on the collated content analysis, detailing suitable content and a format for validating the proposed framework.

6.3. Focus Group Scope

The scope of the focus group session was based on three tasks: define and explain the research problem, describe the focus group discussion and update the proposed framework of cloud data governance after validation by the focus group participants. Figure 6.1 shows the focus group process and the session's scope.

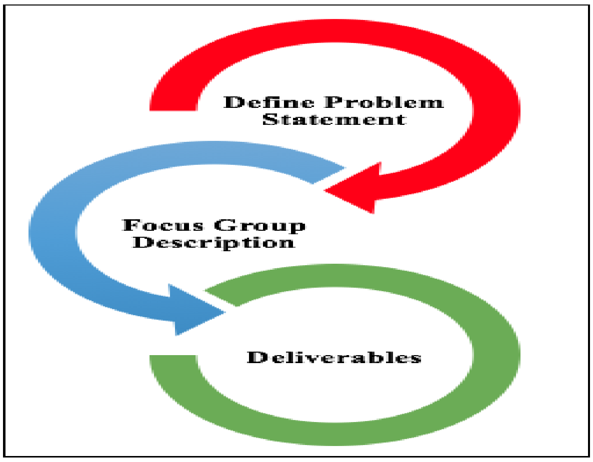

Figure 6.1 Focus group session's scope

a) Define Problem Statement

The focus group started by defining the research problem to the focus group participants. The research problem emanated from organisations' concerns when they move their data to a cloud computing environment (Mary et al., 2011). The literature review shows that the loss of data governance in cloud computing environments is considered to be one of the main issues when organisations are thinking about adopting cloud computing (Groß & Schill, 2012). There is no clear solution to help organisations to understand how to design, deploy and sustain a cloud data governance programme. This work provides a solution by developing a strategy framework to design, sustain and deploy an effective cloud data governance programme; this will help organisations to understand how to develop their own cloud data governance programme.

b) Focus Group Description

This section highlights and describes the focus group session, as follows:

- ***Focus Group Session***

This focus group is called the cloud data governance framework focus group; its discussion was based on the given guidelines (see Appendix D). The process of the validation session took around three hours, including:

1. Presentation, in which the background of the research was discussed, including the problem, aim, objectives, and the desired outcomes of the research.
2. Presentation of the proposed framework and explanation of the framework implementation.
3. Open discussion to gather the participants' experience and thereby validate the proposed framework.
4. Closed questions with a five-point Likert scale to obtain feedback from the focus group participants.
5. Gathering feedback through the use of open-ended questions and open discussion to obtain feedback from the focus group participants to improve and update the proposed framework.

c) Deliverables

A deliverable in this context is any unique and verifiable result of the focus group discussion that details changes and improvements that must occur to complete a process, phase, framework objective, framework design or phase component. The deliverable within this stage permitted improvements and updates to be made to the proposed framework. These were driven by the recommendations and results of the validation, provided by the focus group.

6.4. Participant Profiles

The focus group comprised 10 participants, who were coded P1 to P10; 7 participants were from government organisations, and 3 participants were from cloud providers. The participants from government organisations were representatives of the Ministry of Interior, Ministry of Finance, Ministry of Education, Directorate General for Passports, Prince Mohammad bin Abdulaziz Hospital and King Abdulaziz City for Science and Technology. The cloud provider participants represented the three biggest cloud provider companies in Saudi Arabia: Mobily, STC and Elm. The participants in this focus group were chosen to be similarly homogenous with respect to their education, and recent experience with cloud computing, building strategy and aspects of governance. To gather feedback from a mix of participants with different organisations, the focus group session was conducted with all the participants at the same time. Table 6.1 shows the participants' demographics.

Table 6.1 The demographic characteristics of the participants

Participant group	Participant code	Position	Experience in current job	Cloud experience	Strategy experience	Governance experience
Government Organisation	P1	IT Manager	11 years	2-5 Years	2-5 Years	1-2 Years
	P2	CIO	2-5 Years	5-10 years	1-2 Years	2-5 Years
	P3	IT Manager	5-10 years	2-5 Years	2-5 Years	1-2 Years
	P4	Data centre administrator	13 years >10	1-2 Years	1-2 Years	<1 year
	P5	CIO/IT Manager	18 years >10	5-10 years	5-10 years	5-10 years
	P6	IT Manager	13 years >10	1-2 Years	2-5 Years	2-5 Years
	P7	IT Manager	12 years >10	1-2 Years	1-2 Years	<1 year
Cloud Provider	P8	Cloud Manager	5-10 years	2-5 Years	1-2 Years	5-10 years
	P9	Data centre administrator	12 years >10	5-10 years	5-10 years	5-10 years
	P10	Cloud Manager	1-2 Years	2-5 Years	1-2 Years	2-5 Years

6.5. Data Analysis

Both quantitative and qualitative data analysis tools have been used in this research for validation purposes, based on the participants' feedback. In terms of the quantitative feedback, a five-point Likert scale was used to validate each statement in the validation criteria: these are framework design, framework phases, components of the framework phases and usability. Regarding qualitative feedback, the validation of the framework contained open-ended statements to give a short rationale for the participants' opinions and the opportunity to express further comments and recommendations to update and improve the framework. It was necessary to find an equilibrium between both the validation results and the participants' suggestions to improve the framework. This was to ensure that the proposed framework would be more accurately implemented across the different organisations. Figure 6.2 shows the balancing point to obtain an accurate framework.

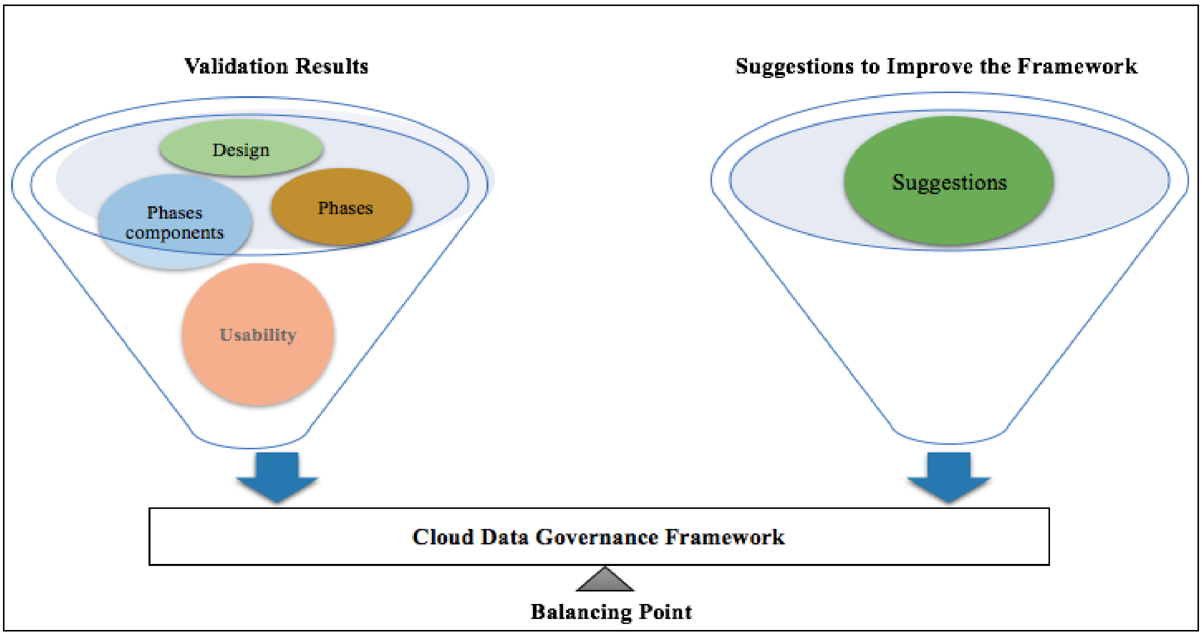

Figure 6.2 The balancing point for accuracy of the framework

6.5.1. Framework Design Validation

The goal of this step is to investigate whether the framework design achieves the research aim and objectives. This step includes seven statements, which were coded St 1.1 to St 1.7. A Likert scale ranging from 5 (strongly agree) to 1 (strongly disagree) was used to indicate whether the participants agreed or disagreed with each statement, in order to rate the design of the framework. Figure 6.3 shows the participants' feedback on these statements.

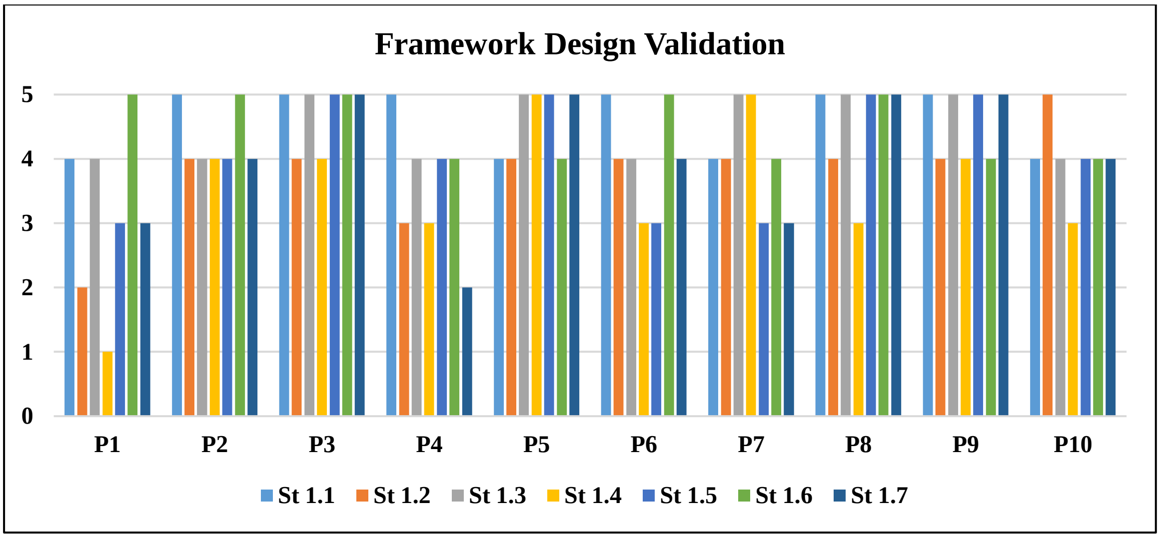

Figure 6.3 The participants' feedback on validation statements of the framework design

Figure 6.3 shows the participants' feedback on the seven statements regarding the validation of the framework design. The results show that the majority of the participants agreed with these statements with mean => 3.5. Based on the results above, Table 6.2 shows the means of the participants' feedback to validate the framework design.

Table 6.2 The means of the participants' feedback on the statements to validate the framework design

St 1.n	Statements	Mean
1.	Framework provides a strategy to design, deploy and sustain an effective cloud data governance programme.	4.60
2.	Framework supports organisational learning and innovation in cloud data governance.	3.80
3.	Framework provides a structured methodology for supporting decision makers to understand important processes to implement a cloud data governance programme.	4.50
4.	Framework will help organisations to reduce the cost, time and effort involved in the cloud data governance process.	3.50
5.	Framework reduces loss of data governance in cloud computing.	4.10
6.	Framework helps government organisations to implement their cloud data governance programme.	4.50
7.	Framework helps government organisations to control their data in the cloud computing environment.	4.00

6.5.2. Framework Phases Validation

The goal of this step is to determine whether the participants agree with the framework phases in terms of whether these phases support important processes and increase understanding of cloud data governance requirements. This step comprises five statements, which were coded St 2.1-St 2.5. A Likert scale of importance from 5 (very important) to 1 (not important) was used to indicate the participants' feedback to each statement and to rate the phases of the framework. Figure 6.4 shows the participants' feedback on these statements.

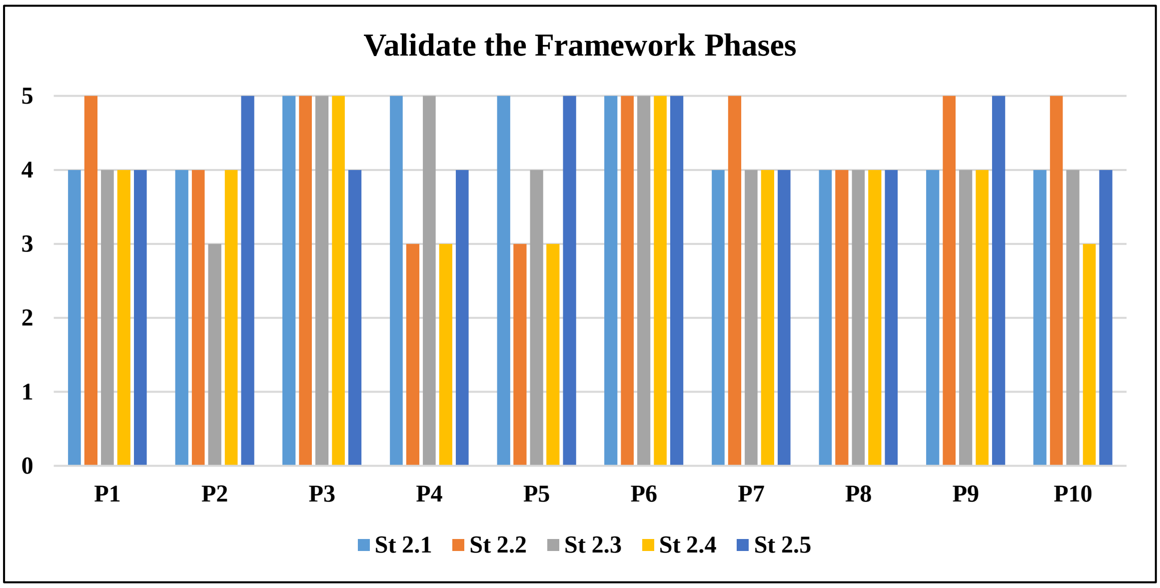

Figure 6.4 The participants' feedback on validation statements of the framework phases

Figure 6.4 shows the participants' feedback on the five statements in order to validate the phases of the proposed framework. The results show that all of the participants indicated that the statements were important, with mean => 3.9. Based on the results above, Table 6.3 shows the means of the participants' feedback to validate the framework phases.

Table 6.3 The means of the participants' feedback on the statements to validate the framework phases

St2.n	Statements	Mean
1.	The initial phase is crucial to support important processes in understanding cloud data governance requirements.	4.40
2.	The design phase is crucial to support important processes in designing a cloud data governance programme.	4.40
3.	The deploy phase is crucial to support important processes in implementing a cloud data governance programme.	4.20
4.	The monitor phase is crucial to support important processes to ensure that the cloud data governance programme is going in the right direction.	3.90
5.	The sustain phase is crucial to support important processes that keep the cloud data governance programme ongoing.	4.40

6.5.3. Validate the Components of the Framework Phases

In the previous section, the framework phases in general have been validated; thus, this section aims to validate each component in these phases. In this section, a Likert scale of importance from 5 (very important) to 1 (not important) was used to indicate the participants' feedback to each statement to rate each component in the framework phases.

- **Validation Results of the Initial Phase**

This step aims to validate the initial phase components to make sure that these components are important when identifying the significant requirements for building the strategy framework. This step includes seven statements, coded St 3.1.1 to St 3.1.7. Figure 6.5 shows the participants' feedback on these statements.

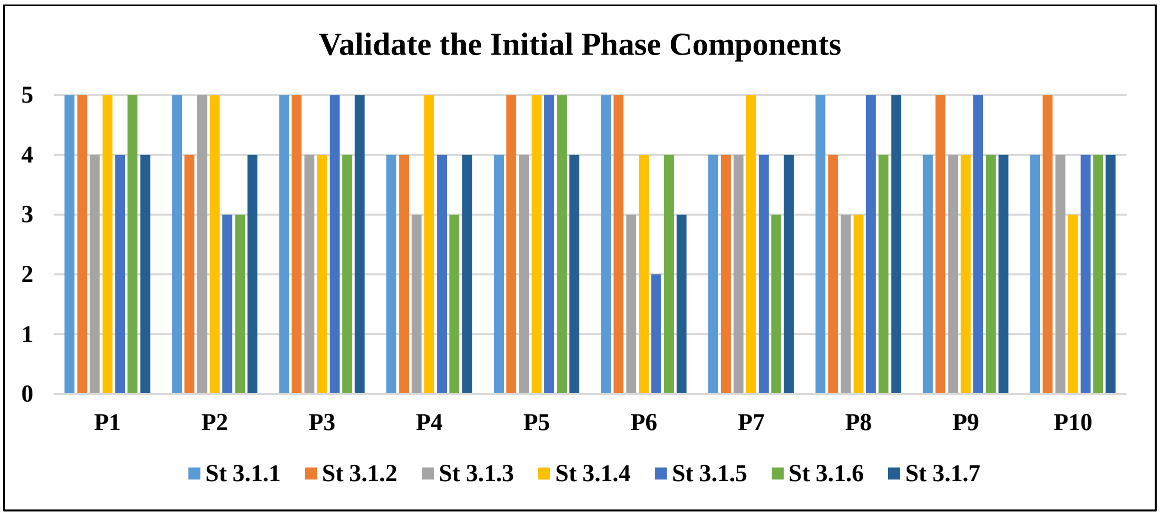

Figure 6.5 The participants' feedback on validation statements of the initial phase components

Figure 6.5 shows the participants' feedback on the seven statements in order to validate the initial phase components in the framework. The results show that all participants agreed with the importance of these statements, with mean => 3.80. Table 6.4 shows the means of the participants' feedback to validate the initial phase components.

Table 6.4 The means of the participants' feedback on the statements to validate the initial phase components

St 3.1.n	Statements	Mean
1.	Establish the cloud data governance office.	4.50
2.	Build structure for the cloud data governance office.	4.60
3.	Develop a communication plan for the cloud data governance office.	3.80
4.	Establish cloud data governance roles and responsibilities.	4.30
5.	Define the cloud data governance business case.	4.10

St 3.1.n	Statements	Mean
6.	Set up a cloud data governance assessment guide.	3.90
7.	Define cloud data governance requirements.	4.10

- **Validation Results of the Design Phase**

This criterion aims to validate the design phase components to make sure that these components are important for the strategy framework. This step includes five statements, coded St 3.2.1 to St 3.2.5. Figure 6.6 shows the participants' feedback on these statements.

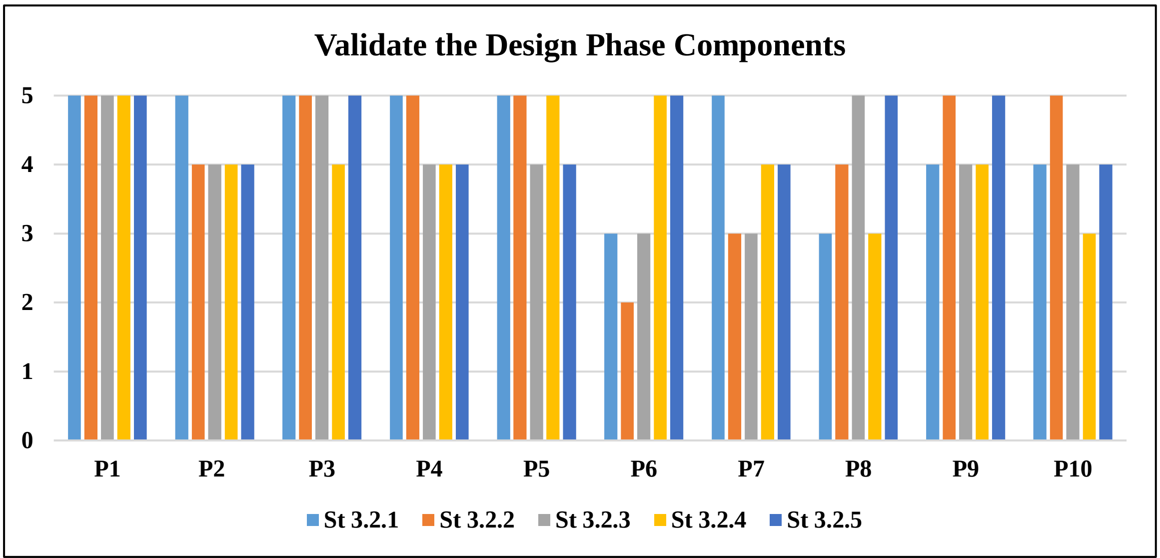

Figure 6.6 The participants' feedback on validation statements of the design phase components

Figure 6.6 shows the participants' feedback on the five statements in order to validate the components of the design phase in the framework. The results show that the majority of the participants agreed with the importance of these statements with mean => 4.10. Based on the results above, Table 6.5 shows the means of the participants' feedback to validate the design phase components.

Table 6.5 The means of the participants' feedback on the statements to validate the design phase components

St 3.2.n	Statements	Mean
1.	Establish cloud data governance functions.	4.40
2.	Integrate data governance functions within the cloud computing context.	4.30
3.	Align data governance functions with other strategies in the organisation.	4.10

4.	Establish a negotiating contract between cloud consumer and provider for cloud data governance.	4.10
5.	Develop a data governance level agreement.	4.50

- **Validation Results of the Deploy Phase**

This step aims to validate the deploy phase components to make sure that these components are important for the strategy framework. This step includes two statements, coded St 3.3.1 and St 3.3.2. Figure 6.7 shows the participants' feedback on these statements.

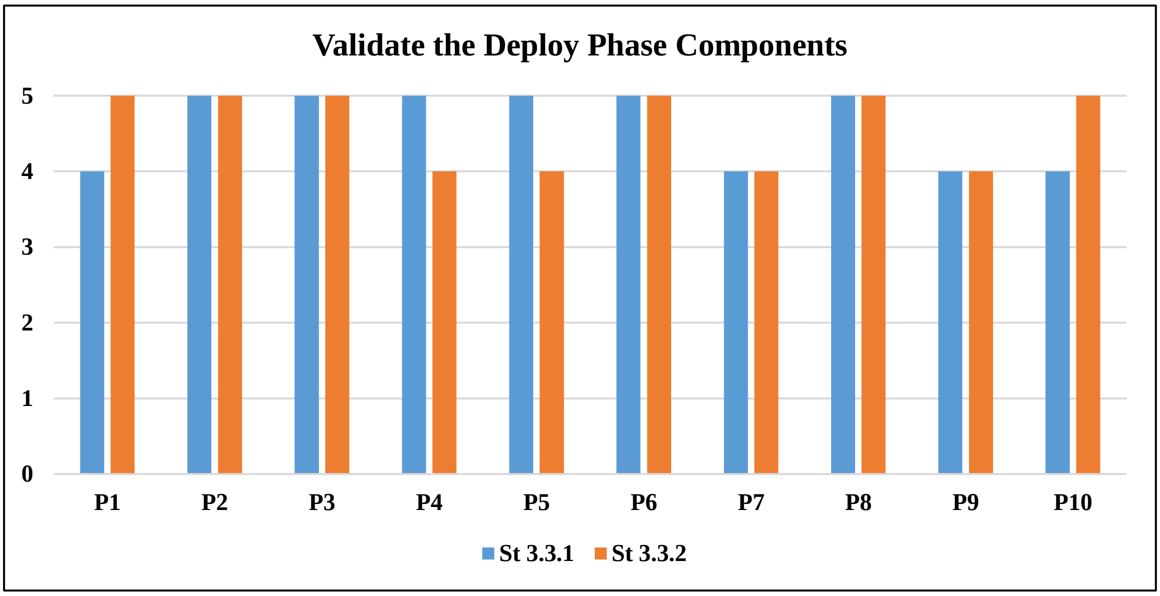

Figure 6.7 The participants' feedback on validation statements of the deploy phase components

Figure 6.7 shows the participants' feedback on the two statements in order to validate the components of the deploy phase in the framework. The results show that all the participants indicated that these statements are important, with mean = 4.60. Based on the results above, Table 6.6 shows the means of the participants' feedback for the deploy phase components.

Table 6.6 The means of the participants' feedback on the statements to validate the deploy phase components

St 3.3.n	Statements	Mean
1.	Configuring cloud data governance programme.	4.60
2.	Implementing cloud data governance programme.	4.60

- **Validation Results of the Monitor Phase**

This step aims to validate the monitor phase components to make sure that these components are important for the strategy framework. This step includes two statements, coded St 3.4.1. and St 3.4.2. Figure 6.8 shows the participants' feedback on these statements.

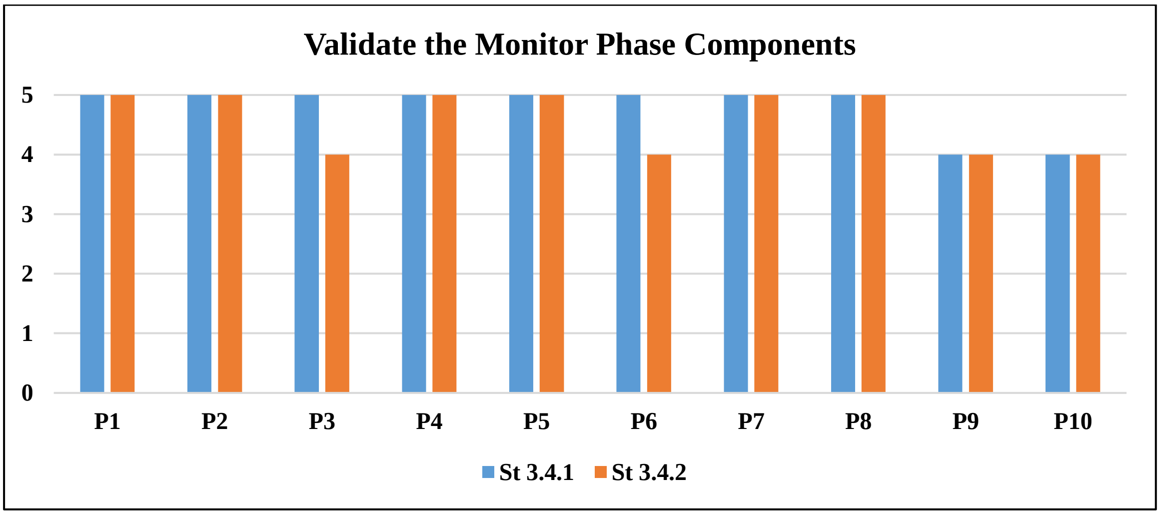

Figure 6.8 The participants' feedback on validation statements of the monitor phase components

Figure 6.8 shows the participants' feedback on the two statements in order to validate the components of the monitor phase in the framework. The results show that all the participants indicated that these statements are important, with mean => 4.60. Based on the results above, Table 6.7 shows the means of the participants' feedback to validate the monitor phase components.

Table 6.7 The means of the participants' feedback on the statements to validate the monitor phase components

St 3.4.n	Statements	Mean
1.	Establish cloud data governance metrics and KPIs.	4.80
2.	Establish cloud data governance tool based on modern technology to monitor cloud data governance activities.	4.60

- **Validation Results of the Sustain Phase**

This step aims to validate the sustain phase components to make sure that these components are important for the strategy framework. This step includes five statements, coded St 3.5.1. to St 3.5.5. Figure 6.9 shows the participants' feedback on these statements.

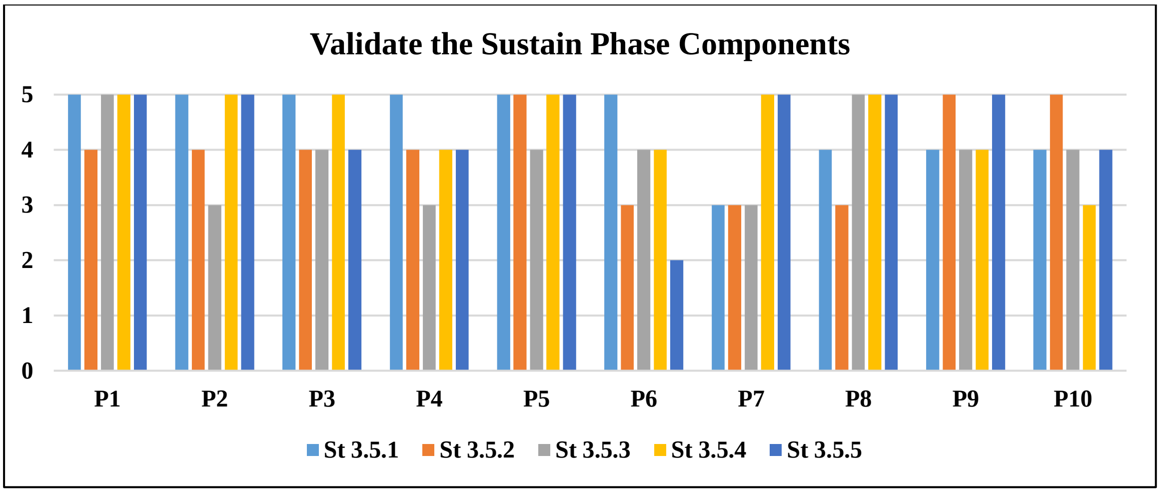

Figure 6.9 The participants' feedback on validation statements of the sustain phase components

Figure 6.9 shows the participants' feedback on the five statements in order to validate the components of the sustain phase in the framework. The results show that the majority of the participants agreed with the importance of these statements with mean => 3.90. Based on the results above, Table 6.8 shows the means of the participants' feedback to validate the sustain phase components.

Table 6.8 The means of the participants' feedback on the statements to validate the sustain phase components

St 3.5.n	Statements	Mean
1.	Identify Critical Success Factors (CSFs) for cloud data governance.	4.50
2.	Establish/update education and training plan.	3.90
3.	Execute change management plan.	4.50
4.	Execute cloud data governance change plan.	4.40

6.5.4. Validation Results of the Framework's Usability

The usability step is critical in order to ensure that the framework meets the requirements and specifications and can be applied in the organisation. Therefore, this section aims to validate the framework usability in terms of: ease of use, ease of learning, clarity, coverage of data governance strategy, practically, flexibility and efficiency. This step includes eight statements, coded St 4.1 to St 4.8. A Likert scale of agreement from 5 (strongly agree) to 1 (strongly disagree) was used to indicate the participants' agreement or disagreement with each statement and to rate the usability of the framework. Figure 6.10 shows the participants' feedback on these statements.

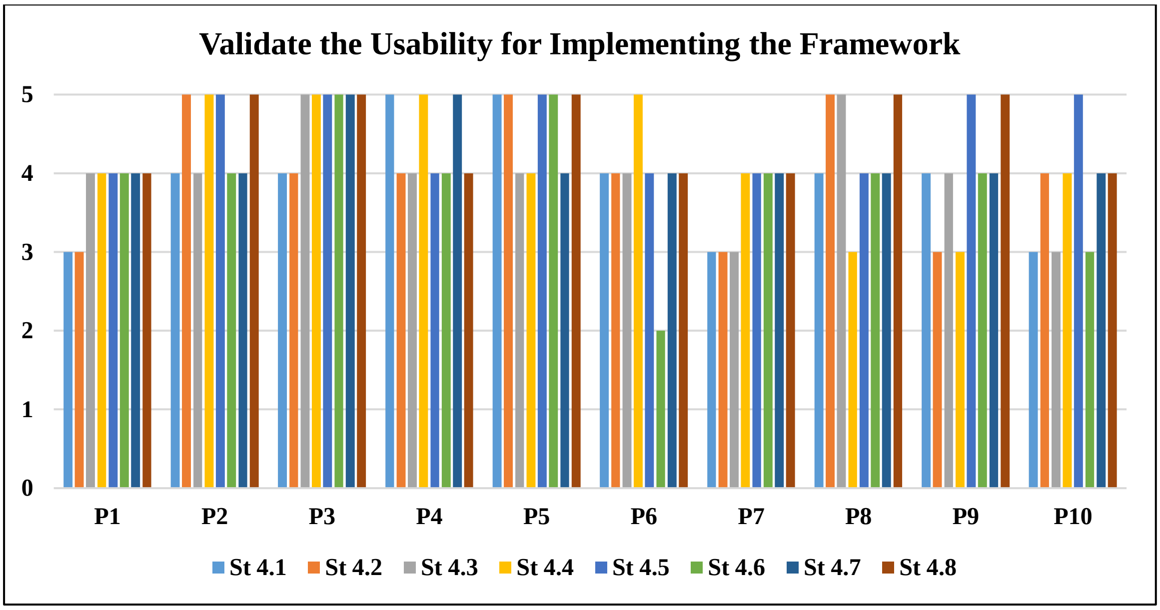

Figure 6.10 The participants' feedback on validation statements of the framework's usability

Figure 6.10 shows the participants' feedback on the eight statements in order to validate the framework's usability. The results show that the majority of the participants agreed with these statements, with mean => 3.90. Based on the results above, Table 6.9 shows the means of the participants' feedback to validate the framework's usability.

Table 6.9 The means of the participants' feedback on the statements to validate the framework's usability

St 4.n	Statements	Mean
1.	The framework is easy to use.	3.90
2.	The framework is easy to learn.	4.00
3.	The framework is clear.	4.00
4.	The framework provides comprehensive coverage of processes involved in developing the strategy to implement the cloud data governance programme.	4.20
5.	The framework is useful.	4.50
6.	The framework can be practically used.	3.90
7.	The framework is flexible and efficient.	4.20
8.	The framework provides a systematic approach to implementing a cloud data governance programme.	4.50

6.5.5. Finding and Discussion

Based on the focus group discussion, this study found that there is slight interest among government organisations in implementing cloud data governance programmes in their organisations. Participants from government organisations mentioned that they had not yet implemented a cloud data governance programme for many reasons, namely: cloud computing adoption in the organisation is not mature, there are no official cloud computing regulations, and there is a lack of existing skills and knowledge among IT professionals in the organisation related to implementing and managing cloud data governance.

Additionally, there is no data governance office in the structure of the majority of public sector organisations to manage the cloud data governance programme. In the majority of organisations, the IT department is responsible for protecting data and the IT professionals' focus is on practical ways to ensure data security. The cloud provider participants also agreed with these reasons.

Given the focus group results analysis above, the Likert scale frequency was used to measure the participants' feedback. The Likert scale answer for each statement, and the mean to obtain the overall participant results for each validation statement, have been considered in the data analysis. Table 6.3 refers to the data analysis as assessed by the participants to validate the framework design by supporting cloud data governance's aim and objectives. The frequency results show that most of the participants agree with all the statements. Regarding the validation of the framework phases, the results show that most of the participants agree that all the given statements are crucial to support important processes in the framework.

The focus group also validated the importance of each phase's proposed components. The means obtained show that the participants are in general agreement with all the given statements with some recommendations to add new components. In addition, the focus group also validated the framework's usability in terms of ease, clarity, coverage of the data governance strategy, practicality, flexibility and efficiency. Table 6.10 shows the means of the data analysis as assessed by the participants for validating the framework's usability.

Regarding the rationale for their views, the participants provided some comments to support their opinions, as follows:

- The participants mentioned that the framework is important for organisations that are adopting or thinking about adopting cloud computing, for many reasons:

    - The framework design follows a systematic approach to designing a strategy and it covers all the important foundation phases.
    - The framework phases cover the most important components for developing a strategy that helps organisations to implement a data governance programme for cloud computing.
    - The framework covers the integration between data governance functions and cloud computing features.
    - The framework helps decision makers in the organisation to understand how to implement a data governance programme for cloud computing services.
    - The framework refers to the establishment of a data governance office in the organisation's structure; this was one of the main barriers to implementing an effective cloud data governance programme in organisations.
    - Considering the data governance office in the framework will assist the decision makers with ensuring that there are professionals in their organisation responsible for managing and monitoring the cloud data governance programme. This will ensure that the cloud data governance programme is effective and that improvements can be implemented in the future.
- The participants mentioned some suggestions that need to be addressed in the proposed framework; these suggestions will be discussed in section 6.5.7 below.

The focus group participants concluded, in the context of the Saudi Public Sector, that establishing a framework for a strategy to understand how to design, deploy and sustain a cloud data governance programme in the organisations would be useful for cloud consumers and providers to understand the important processes required to implement the cloud data governance programme.

6.5.6. Overall Summary for the Validation of the Proposed Framework

Table 6.10 shows the participants' feedback on the framework based on each criterion and each participant group.

Table 6.10 The participant groups' feedback on the framework based on each criterion

Criterion	Design	Phases	Usability
Statement	Validate the framework design by supporting cloud data governance aim and objectives.	Validate the framework phases.	Validate the usability for implementing the framework.
Government Organisations	4.04	4.31	4.21
Cloud Providers	4.38	4.13	4.00
Mean for Each Criterion	4.21	4.22	4.11

Table 6.10 shows the results summary regarding the participants' answers to the three criteria (design, phases, usability) in terms of the validation of the cloud data governance framework. The framework phases' criteria have been ranked highest based on the participants' answers (mean= 4.22). The results show that the government organisations indicated their satisfaction with the framework phases with high scores (mean = 4.31), followed by the cloud provider group with a mean score of 4.13.

The design criteria have been ranked second by the group of participants (mean = 4.21). The results show that the cloud providers indicated their satisfaction that the framework design supports cloud data governance's aim and objectives (mean = 4.38), followed by the government organisations group (mean= 4.04). The usability criteria have been ranked third with a mean score of 4.11.

The results show that the government organisations indicated their satisfaction with the framework usability by a mean score of 4.21, followed by the cloud provider group with a mean score of 4.00. The overall views of each participant group regarding each phase in the framework have also been analysed in this section. These phases are initial, design, deploy, monitor and sustain. Table 6.11 shows the participants' overall feedback for each phase of the framework based on each phase and each participant group.

Table 6.11 The participant groups' feedback on each phase of the framework

	Initial Phase	**Design Phase**	**Deploy Phase**	**Monitor Phase**	**Sustain Phase**
Statements	The components of the initial phase are important for building the framework for the strategy to design, deploy and sustain an effective cloud data governance programme.	The components of the design phase are important for building the framework for the strategy to design, deploy and sustain an effective cloud data governance programme.	The components of the deploy phase are important for building the framework for the strategy to design, deploy and sustain an effective cloud data governance programme.	The components of the monitor phase are important for building the framework for the strategy to design, deploy and sustain an effective cloud data governance programme.	The components of the sustain phase are important for building the framework for the strategy to design, deploy and sustain an effective cloud data governance programme.
Government Organisations	4.20	4.34	4.64	4.86	4.25
Cloud Providers	4.13	4.13	4.50	4.33	4.26
Mean for Each Criterion	4.17	4.24	4.57	4.60	4.26

Table 6.11 shows the results summary regarding the groups' answers in terms of the validation of each phase in the cloud data governance framework. The monitor phase has been ranked as the highest among the other phases (mean = 4.60). The results show that the government organisations indicated their satisfaction with the monitor phase with high scores (mean = 4.86), followed by the cloud provider group with a mean score of 4.33. The deploy phase has been ranked second by the group of participants (mean = 4.57). The results show that the government organisations indicated their satisfaction with the deploy phase (mean = 4.64), followed by the cloud provider group (mean = 4.50). The sustain phase has been ranked third with a mean score of 4.26. The results show that the cloud provider group indicated their satisfaction with the sustain phase with a mean score of 4.26, followed by the government organisations group with a mean score of 4.25. In addition, the phase ranked fourth by the participant groups was the design phase (mean = 4.24). The results show that the government organisations indicated their satisfaction with the design phase (mean = 4.34), followed by the cloud provider group (mean= 4.13). Finally, the initial phase has been

ranked the last phase with a mean of 4.17. The results show that the government organisations indicated their satisfaction with the initial phases (mean = 4.20), followed by the cloud provider group with a mean score of 4.13. Figure 6.11 shows that both participant groups indicated their agreement with the validation of each phase of the cloud data governance framework.

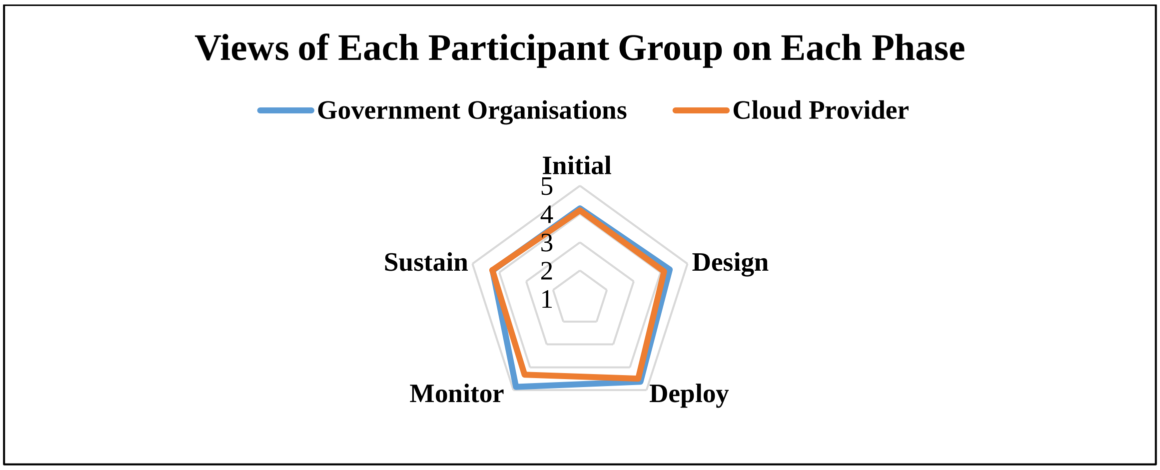

Figure 6.11 Participants' feedback to validate each phase of the framework

6.5.7. Suggestions for Framework Changes and Improvements

Regarding qualitative feedback, the validation of the framework contained open-ended statements to give an opportunity to express further comments and recommendations to update and improve the proposed framework. Therefore, the qualitative feedback indicated that the focus group produced some recommendations to improve the proposed framework, the recommended amendments include:

a. **Initial phase:** The majority of the focus group participants suggested adding a data classification component in this phase.
b. **Design phase:** Most of the focus group participants suggested considering an e-government strategy in the contextual alignment activities.
c. **Deploy phase:** All of the focus group participants suggested adding a reviewing and testing component for the cloud data governance programme before its implementation.
d. **Monitor phase:** Most of the focus group participants suggested adding a dashboard component in this phase to create and present a physical monitoring report for decision makers.
e. **Sustain phase:** The majority of the focus group participants suggested adding

an evaluation of the effectiveness of the cloud data governance programme component in this phase.

All recommendations from the Focus group were summarised and discussed with all participants during the focus group session, which received full support by all participants.

6.5.8. Framework Refinement

The validation process was designed to test whether the proposed framework could be used in the Saudi Arabia context by adding or removing components to the proposed framework shown in Figure 3.27 in Chapter Three. The phase components identified for the proposed framework in Chapter Three were validated through the focus group and the results of the investigation are presented in Table 6.12.

Table 6.12 The results of the investigation through the focus group

Framework Phase	Phase Component	Confirmation of the Component
Initial Phase	Cloud data governance office	Fully Confirmed
	Structure	Fully confirmed
	Communication plan	Fully confirmed
	Roles and responsibilities	Fully confirmed
	Business case	Fully confirmed
	Assess	Fully confirmed
	Cloud data governance requirements	Fully confirmed
	Data Classification	Fully confirmed to be a new component
Design Phase	Cloud data governance functions	Fully confirmed
	Contextual integration of cloud computing	Fully confirmed with add a new sub-component (e-government strategy)
	Contextual alignment	Fully confirmed
	Contractual context	Fully confirmed
Deploy Phase	Configuring cloud data governance programme	Fully confirmed
	Implementing cloud data governance programme	Fully confirmed
	Reviewing and testing the cloud data governance programme	Fully confirmed to be a new component
Monitor Phase	Cloud data governance metrics and KPIs	Fully confirmed
	Cloud data governance Tool	Fully confirmed
	Dashboard	Fully confirmed to be a new component
Sustain Phase	Identify Critical Success Factors (CSFs)	Fully confirmed
	Education and training plan	Fully confirmed
	Execute change management plan	Fully confirmed

	Execute cloud data governance change plan	Fully confirmed
	Evaluate the effectiveness of cloud data governance programme	Fully confirmed to be a new component

As discussed above, the qualitative feedback indicated that the focus group participants suggested improving the development of the proposed framework. Therefore, the participant suggestions in the focus group session have been considered and incorporated into this research to improve the proposed framework. These recommendations were considered and the proposed framework was amended as follows:

- **Initial phase:** a data classification component was added in this phase, and the new components of the initial phase after validation are presented in Figure 6.12.

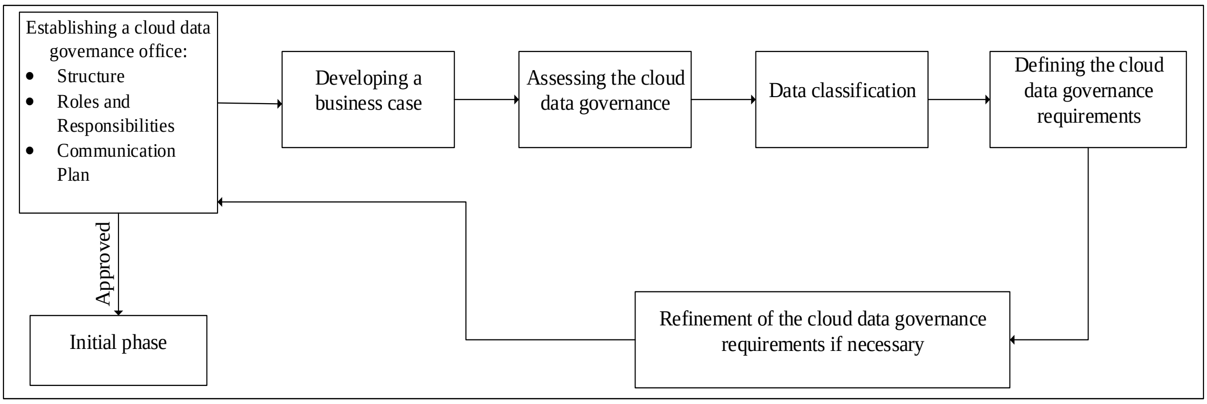

Figure 6.12 The new proposed components of the initial phase after validation

- **Design phase:** E-government strategy component was added in this phase.
- **Deploy phase:** Reviewing and testing the cloud data governance programme component was added in this phase, and the new components of the deploy phase after validation are presented in Figure 6.13.

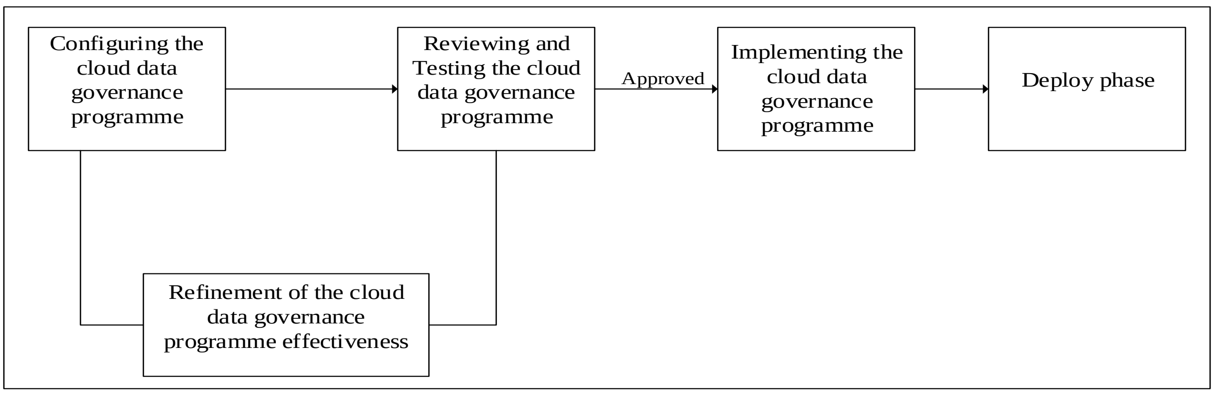

Figure 6.13 The new proposed components of the deploy phase after validation

- **Monitor phase:** A dashboard component was added in this phase, and the new components of the monitor phase after validation are presented in Figure 6.14.

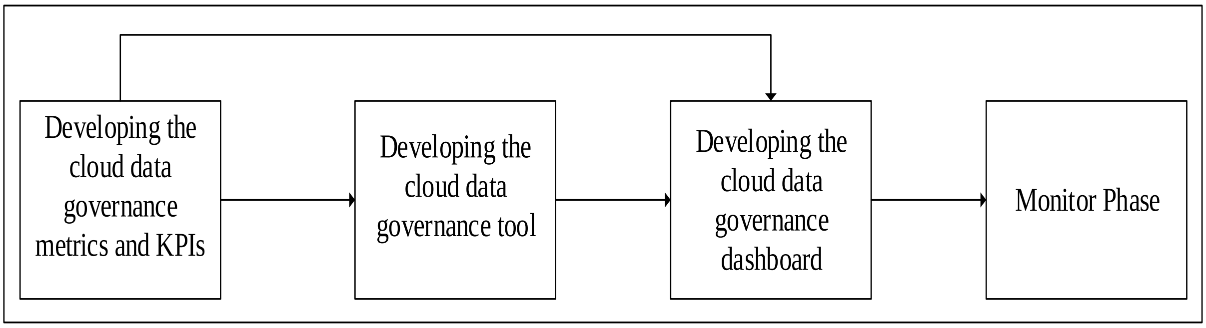

Figure 6.14 The new proposed components of monitor phase after validation

- **Sustain phase:** Evaluating the effectiveness of the cloud data governance programme component was added in this phase, and the new components of the sustain phase after validation are presented in Figure 6.15.

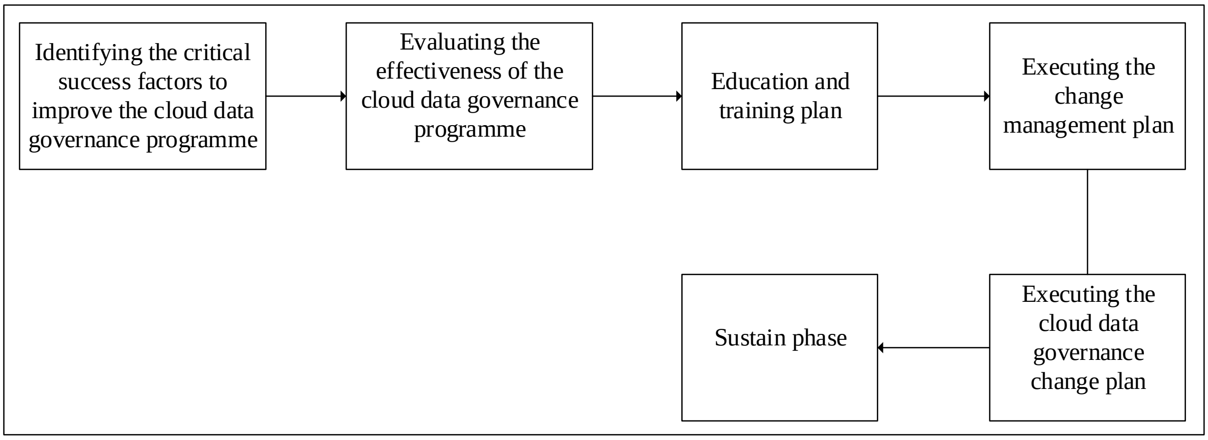

Figure 6.15 The new proposed components of the sustain phase after validation

The amended design of the proposed strategy framework to design, deploy and sustain an effective cloud data governance programme is presented in Figure 6.16.

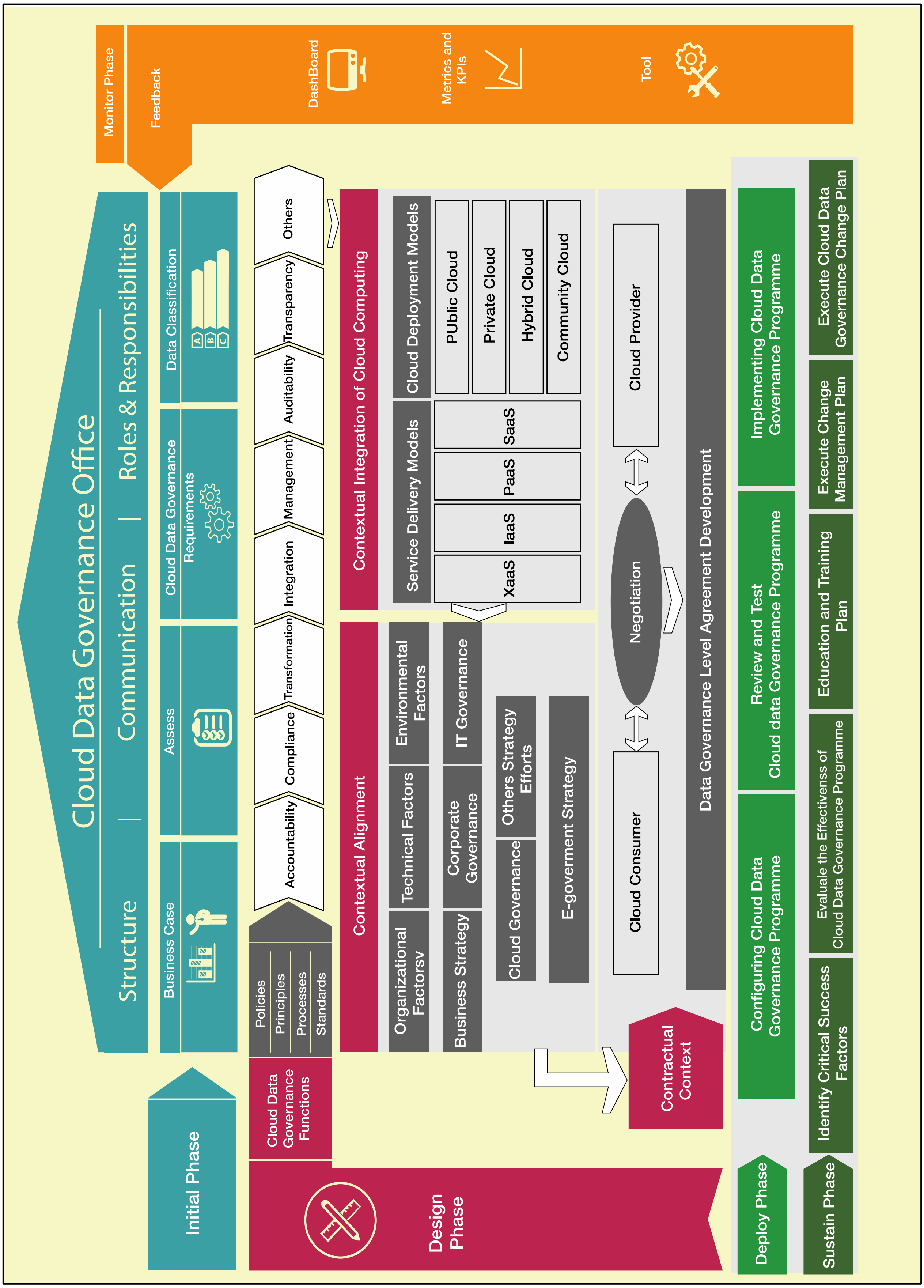

Figure 6.16 Amended framework after participants' feedback

6.6. Cloud Data Governance Framework Evaluation by Structural Equation Modelling

The purpose of this section is to evaluate and assess the proposed cloud data governance framework in chapter Three by Structural Equation Modelling (SEM). SEM requires developing research model and the research hypotheses to evaluate and assess a phenomenon of the research. Research model and hypotheses have been developed in this research. therefore, SEM was used to evaluate and assess the research model and to test the research hypotheses based on the questionnaire findings.

The research model will be assessed in two parts. The first part involves measurement of the research model, with emphasis on the reliability and validity of the research model constructs and their items. This means that each construct in the model will be analysed and that their reliability, validity and other characteristics will be evaluated. The reliability is measured by Cronbach's alpha and composite reliability (CR), and the validity is measured by convergent and discriminant validity. The second part of the model assessment concerns the structural model. This part aims to assess the relationship between the research model constructs and testing the research hypotheses, and it focuses on how the research model fits.

The overall model fit expanded over a sample size of 206 was tested with SEM using Moment of Structures Software (AMOS) version 24.0 as the modelling tool. The Statistical Package for Social Sciences (SPSS) version 24.0 was used to analyse the descriptive statistics and construct reliability. In addition, the research hypotheses will be discussed in this chapter. The research hypotheses' structural relationships have been designed based on the evaluation objective, and these have been divided into two types: associative and causal hypotheses. Twenty-eight hypotheses have been formulated; 21 represent the associative path between the model constructs, and seven represent the causal path between the model constructs. Furthermore, the SEM overview, analysis process and the findings from testing the research model will be provided in this chapter.

6.6.1. Structural Equation Modelling (SEM): Overview

SEM is a general and powerful statistical modelling technique that is widely used in the behavioural sciences(Hox & Bechger, 2007). Two decades ago, SEM became one of the most popular statistical modelling tools across many disciplines due to its generality and flexibility (Suhr, 2006). Morris et al. (2011) defined SEM as "*an analysis approach that accounts for* *both the causal relationships between variables and the errors associated with the measurement of these variables*”(Morris et al., 2011, p.278). Another definition of SEM was reported in 2013 by Merchant et al.: “*a collection of statistical techniques used to determine the degree to which a proposed theoretical model is supported by data*” (Merchant et al., 2013, p.407). Therefore, SEM is a valuable approach for personality assessment that researchers can add to their analysis toolkit. SEM includes a diverse set of mathematical models, computer algorithms and statistical methods that fit networks of constructs to data (Suhr, 2006).

The SEM normally consists of two types of models: the measurement model and the structural model (Merchant et al., 2013; Ratnam et al., 2014; Fan et al., 2016). The measurement model represents the theory and specifies how measured variables come together to represent latent factors (Hox & Bechger, 2007; Ratnam et al., 2014). On the other hand, the structural model represents the theory specifying how constructs are related to other constructs in the model (Henseler et al., 2014). In addition, SEM is a combination of two statistical methods, confirmatory factor analysis (CFA) and path analysis (PA) (Fan et al., 2016). CFA originated in psychometrics, and its objective is to estimate latent psychological traits, such as satisfaction and attitude (Merchant et al., 2013). Confirmatory factor analysis can be defined as “*a statistical technique used to verify the factor structure of a set of observed variables*” (Suhr, 2006, p.1). Therefore, this technique allows the researcher to test the hypothesis that a relationship between observed variables and their underlying latent constructs exists.

To test the hypothesis statistically, the researcher uses knowledge of the theory, empirical research, or both, postulating the relationship pattern a priori (Suhr, 2006). On the other hand, PA can be defined as “*the statistical technique used to examine causal relationships between two or more variables*”(Fan et al., 2016, p.6). It is based upon a linear equation system and was first developed by Sewall Wright in the 1930s for use in phylogenetic studies. Path analysis was adopted by the social sciences in the 1960s and it has been used with increasing frequency in the ecological literature since the 1970s. In addition, PA had its beginning in biometrics, where it aimed to find the causal relationship between variables by creating a path diagram (Fan et al., 2016). The PA in earlier econometrics was presented with simultaneous equations.

Furthermore, the basic statistic in SEM is covariance. Within information systems research, partial least squares (PLS) models are sometimes also described as SEMs, but this use of the term is an exception within the wider SEM community (Rouse & Corbitt, 2008). SEM software includes LISREL, AMOS, EQS and SEPATH. In this research, a two-step approach has been followed. First, the whole measurement model was assessed to assess its validity and unidimensionality; then the structural model was assessed to test the relationships between the constructs. In both steps, SEM was employed using the SPSS and AMOS version 24.0 package.

6.6.2. Research Model: Constructs and Hypotheses

This section will present the overview of the research model constructs and hypotheses, as follows:

- **Research Model Constructs**

The research model in the research was developed based on the the proposed cloud data governance framework in chapter Three. The proposed framework aims to develop a strategy to design, deploy and sustain an effective cloud data governance programme. The framework has been developed based on an analytic theory by deducting an approach for understanding the important processes required to construct the framework. Thus, the framework is based on the results of the research procedure in the literature review, which include existing frameworks, CSFs for implementing cloud data governance (see chapter Two), cloud data governance dimensions and cloud characteristics.

The framework was developed based on five phases and these phases include nine constructs: cloud data governance office, preparation requirements, cloud data governance functions, contextual alignment, contextual integration, contractual context, deploy context, sustain requirements and monitor requirements. The definitions of these constructs and their components were discussed in Chapter Three. Figure 6.17 shows the main structure of the research model and the relationships between its constructs.

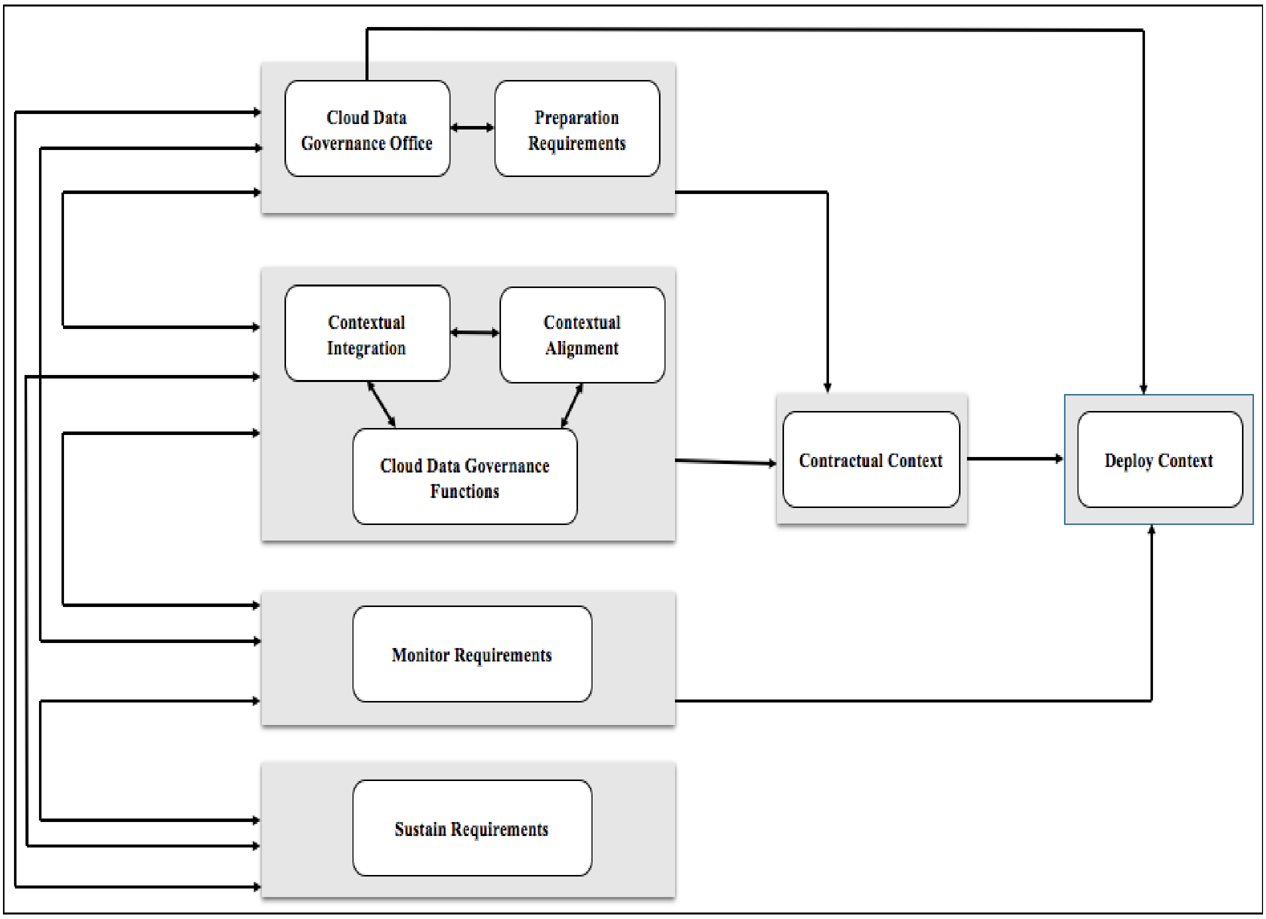

Figure 6.17 Research model

- **Research Model Hypotheses**

A hypothesis can be defined as "*a tentative explanation of the research problem, a possible outcome of the research, or an educated guess about the research outcome*" (Mhlanga et al., 2014, p.3). There are seven common types of research hypotheses: null, simple, complex, directional, non-directional, associative and causal (Suhr, 2006). In this study, associative and causal hypotheses have been chosen to formulate the research model hypotheses. The research model hypotheses were formulated to test the structure of the research model, which was developed based on nine constructs. Each construct was developed based on many items identified from the literature and investigated by the questionnaire. Therefore, the research hypotheses have been formulated to evaluate the research model and to make sure that its outcome supports the research aim.

a) Associative Hypotheses

Associative hypotheses refer to a relationship between variables that occurs or exists in natural settings without manipulation; thus, this hypothesis is used in correlational research studies (Wright, 2006). In this study, the associative hypotheses are used to examine the relationships between seven constructs, where the relationships between these constructs provide a positive influence on the implementation of cloud data governance in the organisation. Twenty-one hypotheses have been formulated to test the relationships between seven constructs through the questionnaire results, and these hypotheses were coded with the prefix Ha. Table 6.13 highlights the associative hypotheses that are to be specifically tested in this study.

Table 6.13 The associative hypotheses

Code	Research Hypotheses
Ha1	There is a positive relationship between establishing a cloud data governance office and defining the preparation requirements to design the cloud data governance strategy.
Ha2	There is a positive relationship between establishing a cloud data governance office and designing the cloud data governance functions to design the cloud data governance strategy.
Ha3	There is a positive relationship between establishing a cloud data governance office and contextual alignment to align the cloud data governance functions with other strategies in the organisation.
Ha4	There is a positive relationship between establishing a cloud data governance office and contextual integration to integrate the cloud data governance functions with the cloud computing context.
Ha5	There is a positive relationship between establishing a cloud data governance office and the monitor requirements to monitor the cloud data governance implementation.
Ha6	There is a positive relationship between establishing a cloud data governance office and the sustain requirements to sustain the cloud data governance in the organisation.
Ha7	There is a positive relationship between defining the preparation requirements and the cloud data governance functions to design the cloud data governance strategy.
Ha8	There is a positive relationship between defining the preparation requirements and contextual alignment to align the cloud data governance functions with other strategies in the organisation.
Ha9	There is a positive relationship between defining the preparation requirements and contextual integration to integrate the cloud data governance functions with the cloud computing context.
Ha10	There is a positive relationship between defining the preparation requirements and the monitor requirements to monitor the cloud data governance implementation.
Ha11	There is a positive relationship between defining the preparation requirements and the sustain requirements to sustain the cloud data governance in the organisation.
Ha12	There is a positive relationship between designing the cloud data governance functions and contextual alignment to align the cloud data governance functions with other strategies in the organisation.
Ha13	There is a positive relationship between designing the cloud data governance functions and contextual integration to integrate the cloud data governance functions with the cloud computing context.
Ha14	There is a positive relationship between designing the cloud data governance

Code	Research Hypotheses
	functions and the monitor requirements to monitor the cloud data governance implementation.
Ha15	There is a positive relationship between designing the cloud data governance functions and the sustain requirements to sustain the cloud data governance in the organisation.
Ha16	There is a positive relationship between contextual alignment to align the cloud data governance functions with other strategies in the organisation and contextual integration to integrate the cloud data governance functions with the cloud computing context.
Ha17	There is a positive relationship between contextual alignment to align the cloud data governance functions with other strategies in the organisation and the monitor requirements to monitor the cloud data governance implementation.
Ha18	There is a positive relationship between contextual alignment to align the cloud data governance functions with other strategies in the organisation and the sustain requirements to sustain cloud data governance in the organisation.
Ha19	There is a positive relationship between contextual integration to integrate the cloud data governance functions with the cloud computing context and the monitor requirements to monitor the cloud data governance implementation.
Ha20	There is a positive relationship between contextual integration to integrate the cloud data governance functions with the cloud computing context and the sustain requirements to sustain cloud data governance in the organisation.
Ha21	There is a positive relationship between sustain requirements to sustain cloud data governance in the organisation and the monitor requirements to monitor the cloud data governance implementation.

b) Causal Hypotheses

The term 'causal hypotheses' refers to the measurement of an independent variable to examine the effect of a dependent variable that is manipulated by the researcher (Wright, 2006). In this study, the causal hypotheses are used to examine the relationships between seven independent and two dependent variables. The cloud data governance office (CDGO), preparation requirements (PR), cloud data governance functions (CDF), contextual alignment (CA), contextual integration (CI), sustain requirements (SR) and monitor requirements (MR) are the exogenous (independent) constructs, whereas contractual context (CC) and deploy context (DPC) have been specified as the endogenous (dependent) constructs. Furthermore, seven hypotheses have been formulated to test the relationships between independent and dependent constructs based on the questionnaire results.

These hypotheses were coded with the prefix Hb. Table 6.14 highlights the causal hypotheses that are to be specifically tested in this study.

Table 6.14 The causal hypotheses

Code	Research Hypotheses
Hb1	Establishing a cloud data governance office has a positive influence on deploying cloud data governance in the organisation.
Hb2	Defining the preparation requirements to design the cloud data governance strategy has a positive influence on developing the contractual context with the cloud provider to implement cloud data governance.
Hb3	Designing the cloud data governance functions has a positive influence on developing the contractual context with the cloud provider to implement cloud data governance.
Hb4	Alignment with the other strategies in the organisation has a positive influence on developing the contractual context with the cloud provider to implement cloud data governance.
Hb5	Integration with the cloud computing context has a positive influence on developing the contractual context with the cloud provider to implement cloud data governance.
Hb6	Developing the contractual context with the cloud provider has a positive influence on implementing and deploying the cloud data governance.
Hb7	Designing the monitor requirements has a positive influence on monitoring the cloud data governance deployment.

6.6.3. Research Model Assessment Process

The assessment process has applied a two-step approach in SEM to analyse this study: the measurement model and the structure model. In the first step, the model was evaluated by examining the reliability and validity of latent constructs using CFA. Cronbach's alpha (α) and composite reliability (CR) have been used to examine the reliability, and discriminant and convergent validity have been used to examine the validity. SPSS was used to analyse the data results from the questionnaire. In the second step, the structural model was assessed by hypothesis testing and examining the model fit. The structural model depicts the relationship among the latent constructs, as presented in Figure 6.13. In other words, it aims to specify which constructs directly/indirectly influence the values of other constructs in the model. Table 6.15 shows the research model assessment steps.

Table 6.15 Steps of the research model assessment

Model Assessment Steps	Assessment Process	Statistic Testing
Measurement Model	Reliability	Cronbach's alpha (α)
		Composite reliability (CR)
		Discriminant validity

Model Assessment Steps	Assessment Process	Statistic Testing
	Validity	Convergent validity
Structural Model	Hypothesis testing	P-Value
		Standard Path coefficient (Beta)
		Standard Error
		t-Value
	Model fit	Chi-Square (X^2)
		Digress of Freedom (df)
		Probability level
		Chi-Square/ df
		Goodness-of-fit index (GFI)
		The adjusted goodness-of-fit index (AGFI)
		Incremental-fit index (IFI)
		Tucker-Lewis index (TLI)
		Comparative Fit Index (CFI)
		The Root Mean Square Error of Approximation (RMSEA)

6.6.4. Measurement of the Model Assessment

This section aims to measure and assess the research model constructs of cloud data governance by linking the measured variables to latent variables. The measurement of the model assessment will be based on CFA. Based on the results of the CFA for the model constructs, items will be accepted or rejected as important factors for the cloud data governance framework. Confirmatory factor analysis is a powerful statistical approach applied to verify the factor structure of a set of observed variables (Suhr, 2006). In addition, it enables the researcher to test whether the measures applied for a particular factor are consistent and measure the same factor (Albright, 2008). The factor loading for each item should be 0.5 or above, as has been suggested by some researchers in the literature (Suhr, 2006; Albright, 2008). Based on the outcomes of the CFA, all the items have been accepted as factors in this research. The factor loading for each item of the research model constructs is shown in Table 6.16.

Table 6.16 The factor loading

Construct	Item	Factor Loading	Construct	Item	Factor Loading
Cloud Data Governance Office	CDGO1	0.882	Contextual Integration	CI1	0.925
	CDGO1	0.801		CI2	0.925
	CDGO1	0.887	Cloud Data Governance Functions	CDF1	0.896
Preparation Requirements	PR1	0.797		CDF2	0.906
	PR2	0.747		CDF3	0.885
	PR3	0.766		CDF4	0.745
	PR4	0.828	Contractual Context	CC1	0.901
Contextual Alignment	CA1	0.871		CC2	0.901
	CA2	0.868	Deploy Context	DPC1	0.848
	CA3	0.886		DPC2	0.848
	CA4	0.882	Sustain Requirements	SR1	0.896
	CAF5	0.848		SR2	0.822
	CAF6	0.877		SR3	0.835
				SR4	0.814
	CAF7	0.846	Monitor Requirements	MR1	0.956
	CAF8	0.874		MR2	0.956

- **Reliability**

Proving the reliability of the phases' items of the cloud data governance framework is necessary for testing. Beck (1994) defined reliability as "*the degree to which measures are free from error and therefore yield consistent results (i.e. the consistency of a measurement procedure)*". In the literature, a coefficient alpha is the most common method of assessing internal consistency and reliability estimates (Hair et al., 2010), and Cronbach's coefficient alpha is the most widely used of these (Beck, 1994). Cronbach's alpha is a reliability coefficient that measures inter-item reliability or the degree of internal consistency/homogeneity between variables measuring one construct/concept, i.e., the degree to which different items measuring the same variable attain consistent results. In the literature, some authors suggest that Cronbach's alpha can be acceptable if it is 0.6 or above (Hair et al., 2010). Hinton et al. (2004) propose four degrees to the reliability scale: excellent (0.90 and above); high (0.70 to 0.90); high moderate (0.50 to 0.70); and low (0.50 and below)(Fan et al., 2016). Cronbach's alpha coefficient was used to investigate the reliability of the model constructs used in this study. In this study, nine constructs were used in the survey questionnaire to measure the constructs proposed in the framework (Figure 6.14). A scale reliability analysis was completed to assess the internal consistency, in order to prove that those scales satisfied the model constructs accurately and consistently. The results of the analysis show that the majority of the constructs achieved an excellent and high reliability of more than 0.7, except one construct that achieved a moderate reliability of more than 0.6. Cronbach's alpha values for all constructs are highlighted in Table 6.17.

Table 6.17 Cronbach's alpha results

Construct	No. of Items	Cronbach's Alpha (α)	Comments
Cloud Data Governance Office (CDGO)	3	0.819	High Reliability
Preparation Requirements (PR)	4	0.790	High Reliability
Cloud Data Governance Functions (CDF)	4	0.881	High Reliability
Contextual Integration (CI)	2	0.830	High Reliability
Contextual Alignment (CA)	8	0.954	Excellent Reliability
Contractual Context (CC)	2	0.767	High Reliability
Deploy (DEP)	2	0.697	High Moderate Reliability
Sustain Requirements (SR)	4	0.809	High Reliability
Monitor Requirements (MR)	2	0.906	Excellent Reliability

- **Validity**

Validity has been defined as "*the extent to which any measuring instrument measures what it is intended to measure*"(Thatcher, 2010, p.5). Confirmatory factor analysis (CFA) was used for the research model construct validity assessment, which was based on assessing both convergent and discriminant validity. The following validity assessment types were used in this study:

a) Convergent Validity

Convergent validity is an agreement between measures of the same construct assessed by different methods (Guo et al., 2008). The convergent validity of the constructs was assessed by composite reliability (CR) and average variance extracted (AVE). A construct has convergent validity if the CR is 0.7 or above and the AVE is 0.5 or above (Fornell & Larcker, 1981; Hair et al., 2010). CR and AVE were calculated according to the following formula (Hair et al., 2010):

$$\text{Composite Reliability} = \frac{\left(\sum_{i=1}^{n}\lambda_i\right)^2}{\left(\sum_{i=1}^{n}\lambda_i\right)^2 + \left(\sum_{i=1}^{n}\delta_i\right)} \qquad \text{Equation 6.1}$$

Where: n = total number of items; λ_i = standardised factor loadings; and ε = error variance term.

$$\text{Average variance extracted (AVE)} = \frac{\sum_{i=1}^{n} \lambda^2{}_i}{n} \qquad \text{Equation 6.2}$$

Where: n = total number of items and λ_i = standardised factor loadings.

The convergent validity result shows that the AVE for each construct exceeds the criterion of 0.50, and it also shows that all composite reliabilities exceeded the criterion of 0.70. Table 6.18 shows that the convergent validity across all the research model constructs was accepted.

Table 6.18 Convergent validity for the constructs

Construct	*AVE	*CR	Comments
Cloud Data Governance Office (CDGO)	0.735	0.893	Accepted
Preparation Requirements (PR)	0.616	0.865	Accepted
Cloud Data Governance Functions (CDF)	0.740	0.919	Accepted
Contextual Integration (CI)	0.854	0.922	Accepted
Contextual Alignment (CA)	0.755	0.961	Accepted
Contractual Context (CC)	0.811	0.896	Accepted
Deploy (DEP)	0.767	0.868	Accepted
Sustain Requirements (SR)	0.724	0.887	Accepted
Monitor Requirements (MR)	0.913	0.955	Accepted
* Accepted if the AVE ≥ 0.5 and CR ≥ 0.7			

a) Discriminant Validity

Discriminant validity assessment has become a generally accepted prerequisite for analysing relationships between latent variables (Henseler et al., 2014). Discriminant validity ensures that a construct measure is empirically unique and represents phenomena of interest that other measures in a structural equation model do not capture (Hair et al., 2010). Without discriminant validity, researchers cannot be certain whether results confirming hypothesised structural paths are real or whether they are a result of statistical discrepancies (Farrell, 2010). Technically, discriminant validity requires that "*a test not correlate too highly with measures from which it is supposed to differ*" (Campbell 1960, p. 548). Moreover, the discriminant validity measurement can be determined by evaluating the square root of the AVE for a given hypothesised construct and the correlations between those constructs (Ratnam et al., 2014). When the square root of the AVE is higher than the correlations, then the constructs are said to have discriminant validity (Fornell & Larcker, 1981). Table 6.19 shows the discriminant validity results for the research model measurement; the result definitely confirms adequate discriminant validity because all AVE square roots are higher than the correlations between constructs.

Table 6.19 Discriminant validity results for the model measurement

Constructs	CDGO	PR	CDF	CI	CA	CC	DEP	SR	MR
CDGO	0.857								
PR	0.408	0.785							
CDF	0.359	0.383	0.860						
CI	0.393	0.383	0.371	0.924					
CA	0.301	0.282	0.315	0.320	0.869				
CC	0.320	0,320	0.375	0.380	0.259	0.901			
DEP	0.323	0.352	0.366	0.311	0.246	0.352	0.876		
SR	0.502	0.535	0.559	0.525	0.425	0.478	0.523	0.851	
MR	0.316	0.325	0.298	0.297	0.304	0.247	0.268	0.413	0.956

6.6.5. Analysis of Research Model Constructs

This section aims to provide further statistical details of the analysis for each construct of the research model. The statistical information for each research model construct includes: correlation between the construct items, factor loading, CR, average variance extracted (AVE), Cronbach's alpha, convergent validity and the Kaiser-Meyer-Olkin (KMO) test. In addition, the analysis begins by providing statistical information about the correlation between the items of the research model constructs. In the literature, there are some views about appropriate correlation coefficients values, which determine whether they are suitable for factor analysis. (Sheridan, 2005) suggest that the correlation coefficients should be more than 0.3 to be suitable for factor analysis. The statistical results show that the correlation coefficients for each item in this study are more than 0.3, thus they are suitable for factor analysis. Regarding the factor loading for each item as mentioned in Table 6.16 above, the results showed that the factor loading for each item is more than 0.7 and that has been accepted.

Cronbach's alpha, AVE and CR have been described in Tables 6.17 and 6.18 above. Cronbach's alpha is used to measures inter-item reliability, and a value of 0.6 or above is acceptable. AVE and CR were used to assess the validity of the constructs; the AVE is acceptable at 0.5 or above, and the CR is acceptable at 0.7 or above for each construct. In addition, the Kaiser-Meyer-Olkin (KMO) test was used in this analysis. The KMO represents the square correlation ratio between variables to the square partial correlation between variables (Taherdoost et al., 2014). Moreover, Kaiser (1970) recommends that an acceptable KMO value should be no less than 0.5(Taherdoost et al., 2014).

- **Analysis of the Cloud Data Governance Office (CDGO)**

The items of this construct have been built based on the literature review results and they have been investigated by a questionnaire. Based on the results of the questionnaire, the cloud data governance office was measured by three items. The correlation coefficients between the cloud data governance office items were greater than 0.3, and the factor loading for each item in the cloud data governance office was greater than 0.7; thus, these items are suitable for factor analysis. The Cronbach's alpha for the cloud data governance office was 0.819 (over 0.6); thus, this construct has a high reliability. The convergent validity for this construct is satisfied as the AVE was 0.735 (over 0.5) and the CR was 0.893 (over 0.7). Furthermore, the KMO value for the cloud data governance office was 0.692, which is greater than the minimum acceptance value (0.5). Table 6.20 shows the results of the cloud data governance office (CDGO) analysis.

Table 6.20 The results of the cloud data governance office (CDGO) analysis

		CDGO1	CDGO2	CDGO3
Correlation	CDGO1	1.000	0.541	0.711
	CDGO2	0.541	1.000	0.552
	CDGO3	0.711	0.552	1.000
Factor loading		0.882	0.801	0.887
Average Variance Extracted (AVE)	0.735			
Cronbach's alpha	0.819			
Composite Reliability (CR)	0.893			
Convergent Validity	Accepted			
KMO test	0.692			

- **Analysis of the Preparation Requirements (PR)**

The items of this construct have been built based on the literature review results and have been investigated by a questionnaire. Based on the literature review and the results of the questionnaire, the preparation requirements construct was measured by four items. The correlation coefficients between the preparation requirements items were greater than 0.3, and the factor loading for each item in the preparation requirements construct was greater than 0.7; thus, these items are suitable for factor analysis. The Cronbach's alpha for the preparation requirements construct was 0.790 (over 0.6); thus, this construct has a high reliability. The convergent validity for this construct is satisfied as the AVE was 0.616 (over 0.5) and the CR was 0.865 (over 0.7). Furthermore, the KMO value for the preparation requirements construct was 0.752, which is greater than the minimum acceptance value (0.5). Table 6.21 shows the results of the preparation requirements (PR) construct analysis.

Table 6.21 The results of the preparation requirements (PR) construct analysis

		PR1	PR2	PR3	PR4
Correlation	PR1	1.000	0.393	0.510	0.579
	PR2	0.393	1.000	0.452	0.522
	PR3	0.510	0.452	1.000	0.454
	PR4	0.579	0.522	0.454	1.000
Factor loading		0.882	0.797	0.747	0.766
Average Variance Extracted (AVE)	0.616				
Cronbach's alpha	0.790				
Composite Reliability (CR)	0.865				
Convergent Validity	Accepted				
KMO test	0.752				

- **Analysis of the Cloud Data Governance Function (CDF)**

The items of this construct have been built based on the literature review results and have been investigated by a questionnaire. Based on the literature review and the results of the questionnaire, the cloud data governance function was measured by four items. The correlation coefficients between the cloud data governance function items were greater than 0.3, and the factor loading for each item in the cloud data governance function was greater than 0.7; thus, these items are suitable for factor analysis. The Cronbach's alpha for the cloud data governance function was 0.881 (over 0.6), thus this construct has a high reliability. The convergent validity for this construct is satisfied as the AVE was 0.740 (over 0.5) and the CR was 0.919 (over 0.7). In addition, the KMO value for the cloud data governance function was 0.819, which is greater than the minimum acceptance value (0.5). Table 6.22 shows the results of the cloud data governance function (CDF) analysis.

Table 6.22 The results of the cloud data governance function (CDF) analysis

		CDF1	CDF2	CDF3	CDF4
Correlation	CDF1	1.000	0.793	0.730	0.526
	CDF2	0.793	1.000	0.740	0.552
	CDF3	0.730	0.740	1.000	0.553
	CDF4	0.526	0.552	0.553	1.000
Factor loading		0.896	0.906	0.885	0.745
Average Variance Extracted (AVE)	0.740				
Cronbach's alpha	0.881				
Composite Reliability (CR)	0.919				
Convergent Validity	Accepted				
KMO test	0.819				

- **Analysis of the Contextual Integration (CI)**

The items of this construct have been built based on the literature review results and have been investigated by a questionnaire. Based on the literature review and the results of the questionnaire, the contextual integration was measured by two items. The correlation coefficients between the contextual integration items were greater than 0.3, and the factor loading for each item in the contextual integration was greater than 0.7; thus, these items are suitable for factor analysis.

The Cronbach's alpha for the contextual integration was 0.830 (over 0.6); thus, this construct has a high reliability. The convergent validity for this construct is satisfied as the AVE was 0.854 (over 0.5) and the CR was 0.922 (over 0.7). Furthermore, the KMO value for the contextual integration was 0.500, which is equal to the minimum acceptance value (0.5). Table 6.23 shows the results of the contextual integration (CI) analysis.

Table 6.23 The results of the contextual integration (CI) analysis

		CI1	CI2
Correlation	CI1	1.000	0.710
	CI2	0.710	1.000
Factor loading		0.925	0.925
Average Variance Extracted (AVE)	0.854		
Cronbach's alpha	0.830		
Composite Reliability (CR)	0.922		
Convergent Validity	Accepted		
KMO test	0.500		

- **Analysis of the Contextual Alignment (CA)**

The items of this construct have been built based on the literature review results and have been investigated by a questionnaire. Based on the literature review and the results of the questionnaire, the contextual alignment was measured by eight items. The correlation coefficients between the contextual alignment items were greater than 0.3, and the factor loading for each item in the contextual alignment was greater than 0.7; thus, these items are suitable for factor analysis. The Cronbach's alpha for the contextual integration was 0.954 (over 0.6); thus, this construct has a high reliability. The convergent validity for this construct is satisfied as the AVE was 0.755 (over 0.5) and the CR was 0.961 (over 0.7). Moreover, the KMO value for contextual alignment was 0.924, which is greater than the minimum acceptance value (0.5). Table 6.24 shows the results of the contextual alignment (CA) analysis.

Table 6.24 The results of the contextual alignment (CA) analysis

		CA1	CA2	CA3	CA4	CA5	CA6	CA7	CA8
Correlation	CA1	1.000	0.822	0.795	0.738	0.675	0.685	0.636	0.683
	CA2	0.822	1.000	0.824	0.710	0.675	0.686	0.620	0.693
	CA3	0.795	0.824	1.000	0.804	0.656	0.689	0.686	0.695
	CA4	0.738	0.710	0.804	1.000	0.726	0.708	0.702	0.738
	CA5	0.695	0.675	0.656	0.726	1.000	0.769	0.681	0.704
	CA6	0.685	0.686	0.689	0.708	0.769	1.000	0.781	0.783
	CA7	0.636	0.620	0.686	0.702	0.681	0.781	1.000	0.783
	CA8	0.683	0.693	0.695	0.738	0.704	0.783	0.783	1.000
Factor loading		0.871	0.868	0.886	0.882	0.848	0.877	0.846	0.874

Average Variance Extracted (AVE)	0.755
Cronbach's alpha	0.954
Composite Reliability (CR)	0.961
Convergent Validity	Accepted
KMO test	0.924

- **Analysis of the Contractual Context (CC)**

The items of this construct have been built based on the literature review results and have been investigated by a questionnaire. Based on the literature review and the results of the questionnaire, the contractual context was measured by two items. The correlation coefficients between the contractual context items were greater than 0.3, and the factor loading for each item in the contractual context was greater than 0.7; thus, these items are suitable for factor analysis. The Cronbach's alpha for the contractual context was 0.767 (over 0.6); thus, this construct has a high reliability. The convergent validity for this construct is satisfied as the AVE was 0.811 (over 0.5) and the CR was 0.896 (over 0.7). The KMO value for the contractual context was 0.500, which is equal to the minimum acceptance value (0.5). Table 6.25 shows the results of the contractual context (CC) analysis.

Table 6.25 The results of the contractual context (CC) analysis

		CC1	CC2
Correlation	CC1	1.000	0.622
	CC2	0.622	1.000
Factor loading		0.901	0.901
Average Variance Extracted (AVE)	0.811		
Cronbach's alpha	0.767		
Composite Reliability (CR)	0.896		
Convergent Validity	Accepted		
KMO test	0.500		

- **Analysis of the Deploy Context (DEP)**

The items of this construct have been built based on the literature review results and have been investigated by a questionnaire. Based on the results of the questionnaire, the deploy phase was measured by two items. The correlation coefficients between the deploy phase items were greater than 0.3, and the factor loading for each item in the deploy phase was greater than 0.7; thus, these items are suitable for factor analysis. The Cronbach's alpha for the deploy phase was 0.609 (over 0.6); thus, this construct has a high moderate reliability. The convergent validity for this construct is satisfied as the AVE was 0.719 (over 0.5) and the CR was 0.836 (over 0.7). The KMO value for the deploy context was 0.500 which is equal to the minimum acceptance value (0.5). Table 6.26 shows the results of the deploy phase (DEP) analysis.

Table 6.26 The results of the deploy context (DEP) analysis

		DEP1	DEP2
Correlation	DEP1	1.000	0.536
	DEP2	0.536	1.000
Factor loading		0.876	0.876
Average Variance Extracted (AVE)	0.767		
Cronbach's alpha	0.697		
Composite Reliability (CR)	0.868		
Convergent Validity	Accepted		
KMO test	0.500		

- **Analysis of the Sustain Requirements (SR)**

The items of this construct have been built based on the literature review results and have been investigated by a questionnaire. Based on the results of the questionnaire, the sustain requirements was measured by four items. The correlation coefficients between the sustain requirements items were greater than 0.3, and the factor loading for each item in the sustain phase was greater than 0.7; thus, these items are suitable for factor analysis. The Cronbach's alpha for the sustain phase was 0.809 (over 0.6); thus, this construct has a high reliability. The convergent validity for this construct is satisfied as the AVE was 0.724 (over 0.5) and the CR was 0.887 (over 0.7). The KMO value for the sustain requirements was 0.683, which is greater than the minimum acceptance value (0.5). Table 6.27 shows the results of the sustain requirements (SR) analysis.

Table 6.27 The results of the sustain requirements (SR) analysis

		SR1	SR2	SR3	SR4
Correlation	SR1	1.000	0.624	0.647	0.730
	SR2	0.624	1.000	0.488	0.645
	SR3	0.647	0.488	1.000	0.760
	SR4	0.730	0.645	0.760	1.000
Factor loading		0.896	0.822	0.835	0.814
Average Variance Extracted (AVE)	0.724				
Cronbach's alpha	0.809				
Composite Reliability (CR)	0.887				
Convergent Validity	Accepted				
KMO test	0.683				

- **Analysis of the Monitor Requirements (MR)**

The items of this construct have been built based on the literature review results and have been investigated by a questionnaire. Based on the results of the questionnaire, the monitor requirement was measured by two items. The correlation coefficients between the monitor requirements items were greater than 0.3, and the factor loading for each item in the monitor phase was greater than 0.7; thus, these items are suitable for factor analysis.

The Cronbach's alpha for the monitor requirements was 0.906 (over 0.6); thus, this construct has a high reliability. The convergent validity for this construct is satisfied as the AVE was 0.913 (over 0.5) and the CR was 0.955 (over 0.7). The KMO value for the monitor requirements was 0.500, which is equal to the minimum acceptance value (0.5). Table 6.28 shows the results of the monitor requirements (MR) analysis.

Table 6.28 The results of the monitor requirements (MR) analysis

		MR1	MR2
Correlation	MR1	1.000	0.828
	MR2	0.828	1.000
Factor loading		0.956	0.956
Average Variance Extracted (AVE)	0.913		
Cronbach’s alpha	0.906		
Composite Reliability (CR)	0.955		
Convergent Validity	Accepted		
KMO test	0.500		

6.6.6. Structural Model Assessment

This is the second step in the evaluation of the structural model assessments to assess the accuracy of the framework building and the relationships between its constructs. This step came after the assessment of the measurement model was completed successfully (Henseler et al., 2014; Fan et al., 2016). The structural model was designed by associative (double-headed) and causal (single-headed) arrows between the model constructs to identify the strong relationships between the model constructs to support the research aim, which is to develop a framework for a strategy to understand how to design, deploy and sustain an effective cloud data governance programme. These arrows represent the research hypotheses formulated in Tables 6.13 and 6.14 above. In addition, to assess the model structure, testing of the research hypotheses and the model fit process will be considered in this study. The following sub-sections describe the research hypothesis testing and model fit:

- **Research Hypothesis Testing**

This study has formulated 28 hypotheses that require testing to see if they support the model constructs. According to Hair et al. (2010), “*testing the hypotheses aims to determine which predictors (independent variables) provide a meaningful contribution to the explanation of the dependent variables*”. In this study, the hypotheses paths were developed to test the relationships between dependent and independent constructs in the research model based on their influence. The cloud data governance office (CDGO), preparation requirements (PR), cloud data governance functions (CDF), contextual alignment (CA), contextual integration (CI), sustain requirements (SR) and monitor requirements (MR) are the exogenous (independent) constructs, whereas contractual context (CC) and deploy context (DPC) were specified as the endogenous (dependent) constructs. The procedure for assessing the model's structure included a p-value and the standardised path coefficients, to explore which hypothesised relationships were supported. The p-value was used to weigh the strength of the evidence (Suhr, 2006); thus, the p-value helps the researcher to determine the significance of the hypothesis results. The p-value is a number between 0 and 1; for a result to be statistically significant, the p-value must be less than or equal to alpha ($p < 0.05$). Moreover, for the hypothesised relationships to be supported, the standardised path coefficients are required to be significant at the $p < 0.05$ level, and should be at least 0.20 to be considered meaningful (Chin, 1998). To consider whether the hypothesised relationships are supported, the standardised path coefficients should be at least 0.20 and ideally above 0.30, and significant at the $p < 0.05$ level; they can then be considered meaningful for discussion (Chin, 1998; Ratnam et al., 2014). Therefore, this section presents the results of the hypotheses testing; the path analysis shows that all hypotheses support the model structure. The results show that the standard path coefficients for all hypotheses were greater than 0.20, with p-values < .05. Figure 6.18 shows the paths analysis for the hypotheses, and Table 6.29 shows the hypotheses testing results, which were used to test the relationships between the latent constructs.

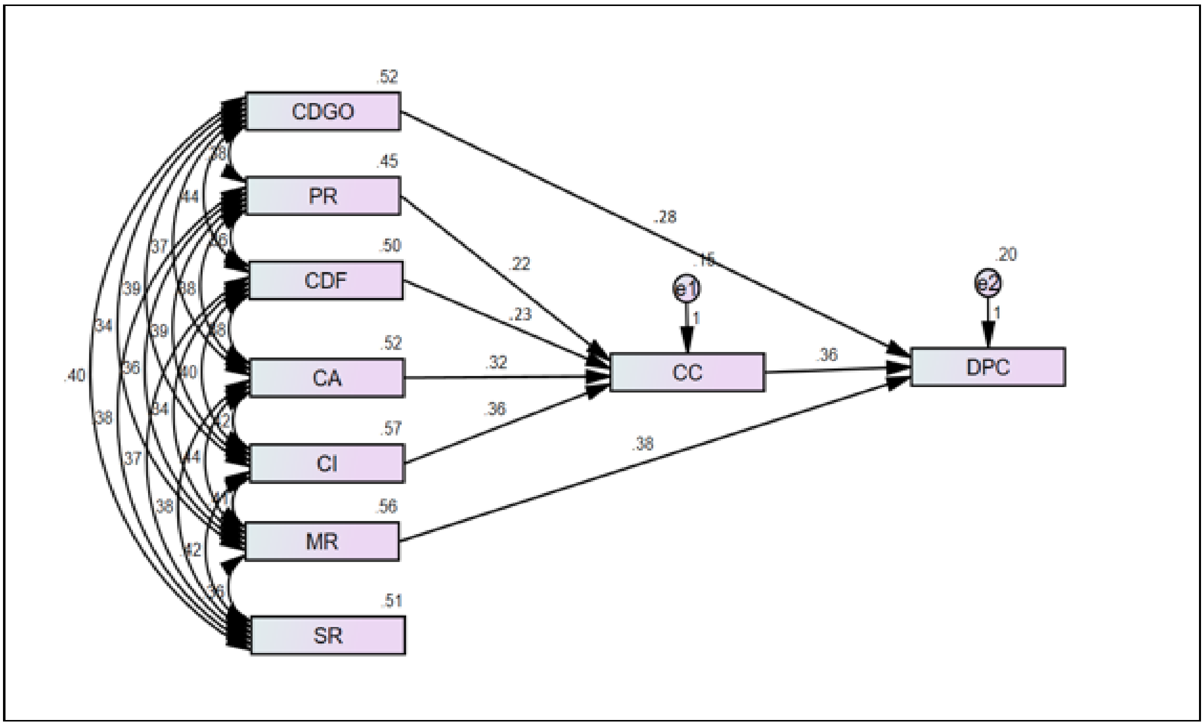

Figure 6.18 The path analysis for the hypotheses

Table 6.29 The hypotheses testing results

Hypotheses No	Hypotheses Path	Standard Path Coefficient (Beta)	Standard Error	t-value	Decision
Ha1	CDGO< --> PR	0.379	0.043	8.829**	Supported
Ha2	CDGO< --> CDF	0.437	0.047	9.318**	Supported
Ha3	CDGO< --> CA	0.374	0.045	8.363**	Supported
Ha4	CDGO< --> CI	0.390	0.047	8.517**	Supported
Ha5	CDGO< --> MR	0.340	0.044	7.666**	Supported
Ha6	CDGO< --> SR	0.395	0.045	8.700**	Supported
Ha7	PR< --> CDF	0.363	0.042	8.678**	Supported
Ha8	PR< --> CA	0.377	0.043	8.800**	Supported
Ha9	PR < --> CI	0.389	0.045	8.704**	Supported
Ha10	PR < --> MR	0.360	0.043	8.362**	Supported
Ha11	PR< --> SR	0.383	0.043	8.907**	Supported
Ha12	CDF< --> CA	0.375	0.044	8.487**	Supported
Ha13	CDF < --> CI	0.396	0.047	8.517**	Supported
Ha14	CDF< --> MR	0.342	0.044	7.794**	Supported
Ha15	CDF< --> SR	0.370	0.044	8.436**	Supported
Ha16	CA < --> CI	0.423	0.048	8.781**	Supported
Ha17	CA< --> MR	0.436	0.048	9.029**	Supported
Ha18	CA< --> SR	0.385	0.045	8.554**	Supported
Ha19	CI< --> MR	0.415	0.049	8.489**	Supported
Ha20	CI< --> SR	0.423	0.048	8.806**	Supported
Ha21	MR< --> SR	0.357	0.045	7.954**	Supported
Hb1	CDGO --> DPC	0.284	0.063	4.507*	Supported
Hb2	PR --> CC	0.220	0.075	2.892*	Supported
Hb3	CDF --> CC	0.231	0.066	3.485***	Supported
Hb4	CA --> CC	0.321	0.069	5.523**	Supported
Hb5	CI --> CC	0.358	0.065	5.523**	Supported
Hb6	CC --> DPC	0.361	0.064	5.612**	Supported
Hb7	MR --> DPC	0.385	0.061	6.282**	Supported

Note: *P<0.01, **P<0.001, ***P<0.05

- **Model Fit**

The model fit is another step to assess the structure model; in the literature, many indices have been used to measure model fit. The goodness-of-fit (GOF) test is considered to be a popular test to measure model fit (Ratnam et al., 2014). The basic index of the GOF test is Chi-square ($\chi 2$) statistics, significance level (p-value) and degree of freedom (df). Furthermore, the goodness-of-fit index (GFI), adjusted goodness-of-fit index (AGFI), incremental-fit index (IFI), Tucker-Lewis index (TLI), Comparative Fit Index (CFI), the Root Mean Square Error of Approximation (RMSEA) and the relative Chi-square ($\chi 2$/df) test were used to evaluate the measurement model (Morris et al., 2011; Merchant et al., 2013; Ratnam et al., 2014; Fan et al., 2016). In this study, the AMOS 24.0 package was used to investigate the GOF indices; AMOS presents more than 20 different GOF measures and the choice of which to report is a matter of argument between methodologists. In the literature, some authors have suggested that the following GOF tests are sufficient to assess the model fit: Chi-square ($\chi 2$), degree of freedom df , $\chi 2$/df, CFI, TLI, IFI, and RMSEA (Hair et al., 2010; Ratnam et al., 2014). Therefore, this study has chosen Chi-square ($\chi 2$), degree of freedom df, $\chi 2$/df, CFI, TLI, IFI, GFI, AGFI and RMSEA to be the GOF test indices. To achieve the model fit and its quality, the indices are tested to determine if they are valid and an acceptable fit, based on their requirements. A small $\chi 2$ value relative to the degrees of freedom (i.e., values lower than 3) indicates a good model fit (Merchant et al., 2013). RMSEA should be < 0.05, which is good, and < 0.08, which is acceptable, and the Comparative Fit Index (CFI) should be greater than 0.95 (CFI > = 0.95, which is acceptable as a close model fit) (Ratnam et al., 2014; Fan et al., 2016). Two other indices are the Goodness-of-Fit Index (GFI), which should be greater than 0.90 (GFI > =0.90), and Adjusted Goodness-of-Fit Index (AGFI), which should also be greater than 0.90 (AGFI > =0.90) (Ratnam et al., 2014; Fan et al., 2016). Additionally, the Incremental-fit index (IFI) and Tucker-Lewis index (TLI) have also been considered in this study; these indices should be greater than 0.90 (IFI > =0.90, TLI> =0.90) (Alshehri, 2012). Thus, the results in this study show that all tests achieved the test requirements. Table 6.30 shows the model fit and quality indices results.

Table 6.30 The framework fit and quality indices

Model fit Indices	Quality Indices	Requirement
Chi-Square (X^2)	16.015	X^2 >df
Digress of Freedom (df)	8	df >0
Probability level	0.042	P<0.05
Chi-Square/ df	2.002	Chi-Square/ df <3
GFI	0.984	GFI >0.90
AGFI	0.910	AGFI >0.90
IFI	0.996	IFI>0.90
TLI	0.981	TLI>0.90
CFI	0.996	CFI>=0.95 is acceptable
RMSEA	0.070	RMSEA <0.08 is acceptable

6.6.7. Discussion

This study has examined and presented ways to implement the strategy framework, which aims to help organisations implement an effective cloud data governance programme. The study is novel in that it identifies major components (constructs) that influence the framework of cloud data governance. The nine proposed cloud data governance constructs – cloud data governance office, preparation requirements, cloud data governance functions, contextual alignment, contextual integration, contractual context, deploy context, sustain requirements and monitor requirements – define the cloud data governance framework. The aim of this study is to test how these constructs positively influence the implementation of the framework for cloud data governance. Based on the data collected (questionnaire, n=206) from different public sector organisations in Saudi Arabia, structural equation modelling (SEM) was carried out through the application of a two-step approach: a measurement model and a structure model. In the first step, the measurement model evaluation was achieved by examining the reliability and validity of the latent constructs. In the second step, the model's structure was investigated by hypothesis testing and by examining the model fit. SPSS version 24.0 was used to analyse the descriptive statistics and construct reliability, and AMOS version 24.0 was the modelling tool. Two methods were used to analyse the latent variables in quantitative studies – Confirmatory Factor Analysis (CFA) and Exploratory Factor Analysis (EFA) (Hox & Bechger, 2007). Confirmatory Factor Analysis is usually applied to test and confirm the model constructs by assessing both the validity and reliability of each construct (Guo et al., 2008). On the other hand, EFA is usually applied if the factors have not been identified, and it helps the researcher to identify the constructs of the developed model (Suhr, 2006).

In order to test the measurement model, this study has applied CFA and EFA by assessing the reliability and validity of each construct in the model (Albright, 2008). In addition, CFA enables the researcher to test whether the measures applied for a particular factor are consistent and measure the same factor (Albright, 2008). The factor loading for each item in the model construct has been measured and the factor loadings for these items were above 0.7, which means that they have been accepted as suitable for factor analysis. With regard to the reliability verification, Cronbach's alpha (α) has been used in this study to measure the internal consistency between construct items. (Tavakol & Dennick, 2011, p.53) reported that "*internal consistency is a commonly used technique to assess the reliability by using Cronbach's alpha*". A total of 31 items measuring nine constructs were assessed for reliability in this study. The results in Table 6.17 showed that the Cronbach's alphas (α) for the model constructs were greater than 0.6. Three items measuring the cloud data governance office had a Cronbach's alpha value of 0.819; four items measuring preparation requirements had a Cronbach's alpha value of 0.790; four items measuring cloud data governance functions had a Cronbach's alpha value of 0.881; eight items measuring contextual alignment had a Cronbach's alpha value of 0.954; two items measuring contextual integration had a Cronbach's alpha value of 0.830; two items measuring contractual context had a Cronbach's alpha value of 0.767; two items measuring deploy context had a Cronbach's alpha value of 0.697; four items measuring sustain requirements had a Cronbach's alpha value of 0.809; and two items measuring monitor requirements had a Cronbach's alpha value of 0.906.

In order to assess the validity, EFA and an examination of the correlation coefficients for all items of each construct were used in this study. In addition, the convergent and discriminant validities of the measurement constructs were also assessed using CFA. The EFA was conducted using the statistical package SPSS 24.0; all constructs of the research model were analysed one by one, and the validation process and results have been discussed in detail. The correlation coefficients matrix was calculated for all items used in measuring the research model constructs. The results revealed that the correlation coefficients between items were greater than 0.3, which indicates that they were suitable for factor analysis(Alshehri, 2012). The KMO has been examined for each construct; the KMO statistical value for these constructs was greater than 0.50, and other constructs were equal to the minimum acceptable level of 0.50, which means that they were suitable for factor analysis (Taherdoost et al., 2014). Furthermore, convergent and discriminant validity were assessed and examined by CFA. In terms of the convergent validity, the AVE and the CR were used to measure the convergent validity of the constructs (Farrell, 2010). The construct has convergent validity if the CR is 0.7 or above and the AVE is 0.5 or above (Shyu et al., 2013). The results revealed that all the constructs in the research model had an AVE between 0.616 and 0.913. In addition, all the constructs in the research model had a CR between 0.868 and 0.961; that is to say, the construct reliability for the internal structural fit of the latent variables was good. On the other hand, a comparison of the absolute value of the square root of the AVE by a construct and the correlations between the constructs have been used to assess discriminant validity (Guo et al., 2008). The results showed that all square roots of the AVE were higher than the correlations between constructs, and that definitely confirms adequate discriminant validity.

The second step to assessing the research model was testing the structural model by testing the hypothesis and model fit. Regarding hypothesis testing, 28 hypotheses have been formulated in this study, based on the model constructs, which require testing to make sure that the relationships between the model constructs support the framework aim. The hypotheses paths were developed to test the relationships between dependent and independent constructs in the research model based on their influence. Based on path analysis, the results show that all hypotheses support the model structure. The results show that the standard path coefficients for all hypotheses were greater than 0.20, with p-values < .05. Therefore, the results for the hypotheses path analysis have achieved an acceptable range in terms of standard path coefficient and p-value. The next step was the model fit; in this step, the model fit has been measured by the GOF test. The results show that model fit has achieved an acceptable range in many indices. The results were: $\chi 2$ = 16.015, df = 8, $\chi 2$/df = 2.002, P=0.042, GFI = 0.984, AGFI=0.910, TLI = 0.981, CFI = 0.996, IFI = 0.996, RMSEA = 0.070. Thus, based on the results mentioned above, this model became the best option and was chosen as the final research model for this study.

6.7. Chapter Summary

This chapter discusses and highlights the process to validate and evaluate the proposed framework for cloud data governance that was presented in Chapter Three. Having developed the cloud data governance framework, there is a need to test and evaluate its validity before it can be more widely disseminated. The validation process aims to determine whether the research findings used for developing the framework are sound and to establish whether these findings are reliable. In addition, a focus group was held to validate the cloud data governance framework through a case study in Saudi Arabia. The focus group focused on the validation of the cloud data governance framework; the participants involved in the focus group session were classified into two groups: experts from different government organisations and cloud providers in Saudi Arabia. The validation in this study was performed by selecting popular criteria that had been used in the literature to validate frameworks. In addition, the focus group recommendations and results were considered to change and improve the framework.

In addition, this chapter highlights the process to evaluate the proposed framework: SEM was used to evaluate and assess the research model and to test the research hypotheses based on the questionnaire's findings. The analysis procedures comprised an assessment of the measurement model and the structural model. With regard to measurement, the reliability and validity of the model constructs have been considered based on their items; also, the EFA and CFA techniques were employed to assess reliability and validity. In terms of reliability, that was measured by Cronbach's alpha for each individual construct; the results of the analysis show that the majority of the constructs achieved an excellent and high reliability of more than 0.7, except one construct that achieved a high moderate reliability of more than 0.6. Following this, EFA was conducted for all individual constructs to explore the validity of the whole framework, and the CFA technique was used to uncover and confirm the convergent and discriminant validity. In this chapter, the measurement of the structural model has also been presented; this measurement was based on hypotheses path analysis and model fit. With regard to path analysis, the results show that all hypotheses support the model structure: the standard path coefficients for all hypotheses were greater than 0.20, with p-values $< .05$. In terms of model fit, the results show that framework fit has achieved the acceptable range in many indices. The following chapter will present the maturity model and assessment matrix validation, and the tool designed to evaluate cloud data governance in some public sector organisations using a case study in Saudi Arabia.

Chapter 7. Evaluation of the Cloud Data Governance Maturity Model and Assessment Matrix

7.1. Introduction

The maturity model was proposed and explained in Chapter Four. It aims to guide organisations to assess the current state of their cloud data governance programme, and help them to plan for new goals based on new requirements. The maturity model was developed based on the proposed strategy framework presented in Chapter Three, in order to define the maturity model dimensions and levels. Additionally, a cloud data governance assessment matrix was proposed as a tool to facilitate the assessment task. The cloud data governance assessment matrix aims to identify the strengths and weaknesses of cloud data governance, and to provide guidelines to improve the cloud data governance process in the organisation. Having developed the cloud data governance maturity model and assessment matrix, there is a need to test and evaluate their validity before they can be more widely disseminated. For this purpose, a focus group was organising for the specified case study of Saudi Arabia. The participants involved in this session were classified into three groups: experts from different government organisations, cloud providers and academics. The focus group recommendations were considered in order to adjust the proposed maturity model and assessment matrix. The results of each of the validation procedures are discussed below.

7.2. Focus Group to Evaluate the Maturity Model and Assessment Matrix

The focus group session focused on the evaluation of the cloud data governance maturity model and assessment matrix. This focus group considered many objectives to achieve its aim:

- Conduct one focus group involving participants from government organisations, the telecommunication and information technology industry (cloud providers) and academia in Saudi Arabia.
- Distribute the questionnaire to evaluate the proposed maturity model and assessment matrix to:
    - Evaluate their completeness.
    - Evaluate their consistency.
    - Evaluate their practicality.

  - Evaluate their usefulness.
  - Evaluate their verifiability.
  - Evaluate the strengths and weaknesses of the assessment matrix.
  - Obtain suggestions from the participants to improve the cloud data governance maturity model and assessment matrix.
- Perform content analysis of the collected data.
- Provide a report on the collated content analysis and detail suitable content and format for evaluating the proposed maturity model and assessment matrix.

7.2.1. Focus Group Description

This section highlights and describes the focus group session, as follows:

- ***Focus Group Session***

This focus group is called the cloud data governance maturity model and assessment matrix focus group; its discussion was based on the given guidelines (see Appendix D). The focus group included:

1. Presentation in which the background of the research was discussed, including the problem, aim and objectives, and the desired outcomes of the research.
2. Presentation of the proposed maturity model and assessment matrix and explanation of the maturity model and assessment matrix development and implementation.
3. Open discussions to gather the participants' experience to validate the proposed maturity model and assessment matrix.
4. Closed questions with a five-point Likert scale to obtain feedback from the focus group participants.
5. Gathering feedback through the use of open-ended questions and open discussion to obtain feedback from the focus group participants to improve and update the proposed maturity model and assessment matrix.

- **Deliverables**

A deliverable in this context is any unique and verifiable result of a focus group discussion that enables a change and improvement to occur to complete the maturity model level, dimensions, name of the level and content of the assessment matrix. The deliverables within this stage permitted improvements and updates to the proposed maturity model and assessment matrix. These improvements were driven by the recommendations and results of the evaluation, provided by the focus group.

7.3. Assessment Criteria

Throughout the literature, some research models and framework developments have focused upon creating evaluation and validation criteria, also called success criteria or quality aspects. Therefore, this section examines methods of selecting the appropriate criteria for use within the evaluation of the maturity model and its assessment matrix. Beecham et al. (2005) identified seven criteria that were used to evaluate the R-CMM maturity model and to examine the strengths and weaknesses of the model. These criteria are: adherence to CMM characteristics, limit scope, consistency, understandability, ease of use, being tailorable and verifiable. Niazi and colleagues (2008) proposed an RE maturity measurement framework in order to assess the strengths and weaknesses of the RE practices within the model based on two success criteria (Niazi et al., 2008). These criteria are user satisfaction and ease of use. These two criteria were adapted from Davis' Technology Acceptance Model (Davis, 1989). Boehm & Valerdi (2008) identified a list of criteria that according to them would be most helpful in evaluating the utility of a software cost model for practical estimation purposes. These criteria are: definition, fidelity, objectivity, constructiveness, detail, stability, scope, ease of use, prospectiveness and parsimony; these criteria were presented in the form of questions. (Solemon, 2013) proposed five criteria to evaluate the RE process improvement model and it make it more concrete. These criteria are: completeness, consistency, practicality, usefulness and verifiability. Generally, the criteria listed above can be redefined and adopted for evaluating the cloud data governance maturity model and assessment matrix, in order to improve them and make them more concrete. After analysing all the proposed criteria in the literature, five criteria were selected for evaluating the proposed maturity model and six criteria were selected for evaluating the proposed assessment matrix; each criterion includes sub-criteria. These criteria will be assessed by a quantitative research method using a Likert-scale frequency. A qualitative research method will also be considered in this assessment, based on the participants' suggestions.

7.4. Participants' Profiles

The focus group comprised 10 participants, and these participants have been coded with the names P1 to P10. The participants were divided into three types: government organisations, cloud providers and academics in Saudi Arabia. Six participants were from government organisations, 2 were from cloud providers, and 2 were from academia. The participants from the government organisations were representatives from the Ministry of Interior, Ministry of Finance, Directorate General for Passports, Prince Mohammad bin Abdulaziz Hospital and the Saudi Vision 2030 office. The participants from the cloud providers were representatives from the biggest cloud provider companies in Saudi Arabia: Saudi Telecom Company (STC) and Etihad Etisalat Company (Mobily).

Academic experts were representatives from the Prince Sattam bin Abdulaziz University and the Technical & Vocational Training Corporation (TVTC). The participants in this focus group were internally homogenous with respect to education and recent experience with cloud computing, building self-assessment models and matrices, and aspects of governance. To gather feedback from a mix of participants in different organisations, the focus group session was conducted with all of the participants at the same time. Table 7.1 shows the participants' demographic details.

Table 7.1 The demographic characteristics of the participants

Participant group	Participant code	Position	Experience in current job	Cloud experience	Self-assessment model and matrix	Governance experience
Government organisation	P1	IT Manager	11 years	2-5 Years	2-5 Years	1-2 Years
	P2	CIO	5-10 Years	5-10 years	1-2 Years	2-5 Years
	P3	IT Manager	5-10 years	2-5 Years	2-5 Years	1-2 Years
	P4	Data centre administrator	years >10	1-2 Years	1-2 Years	<1 year
	P5	IT Manager	years >10	5-10 years	5-10 years	5-10 years
	P6	IT Manager	years >10	1-2 Years	2-5 Years	2-5 Years
Cloud provider	P7	Data centre administrator	years >10	1-2 Years	1-2 Years	<1 year
	P8	Cloud Manager	5-10 years	2-5 Years	1-2 Years	5-10 years
Academia	P9	Researcher	years >10	5-10 years	5-10 years	2-5 years
	P10	Researcher	5-10 Years	2-5 Years	1-2 Years	2-6 Years

7.5. Cloud Data Governance Maturity Model Evaluation

This study selected five main criteria to evaluate the cloud data governance maturity model; each contains sub-criteria. These criteria are as follows: completeness, consistency, practicality, usefulness and verifiability. This study presents the criteria assessment results based on the quantitative and qualitative feedback. A Likert scale (agree-disagree scale) was used for this purpose where the respondents specified their level of agreement or disagreement on a symmetric agree-disagree scale for a series of statements. Figure 7.1 illustration the cloud data governance maturity model evaluation process.

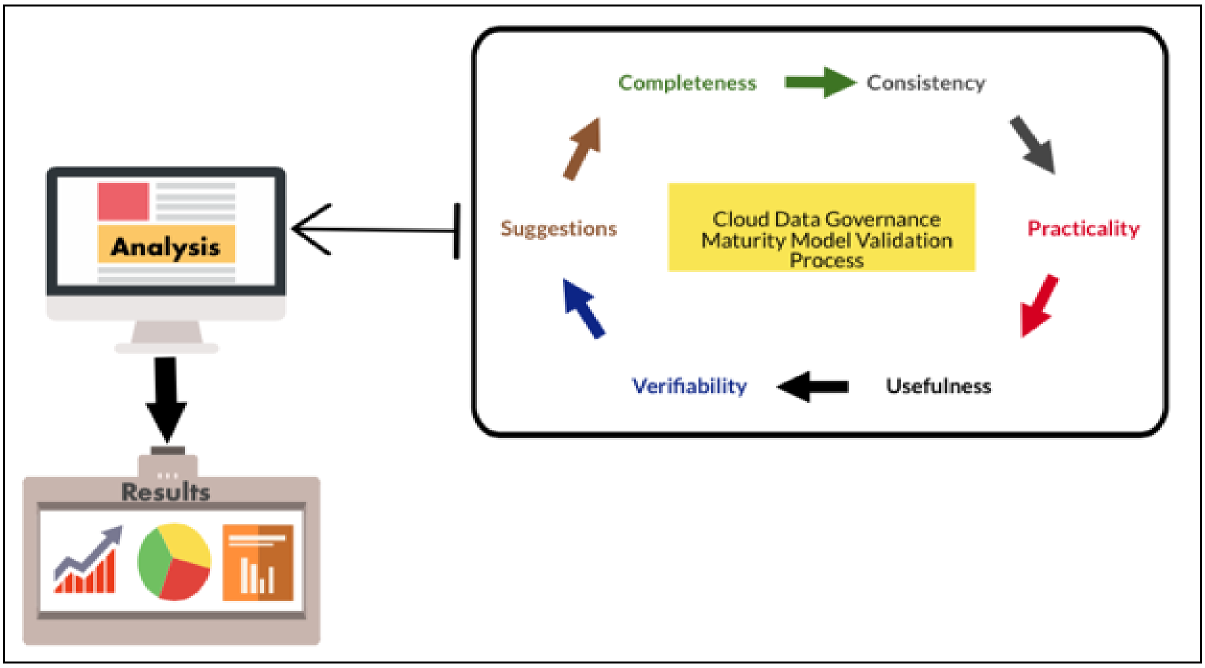

Figure 7.1 The cloud data governance maturity model evaluation process

The results for each criterion are presented below:

7.5.1. Completeness

The completeness criterion evaluated the mean value for three sub-criteria: scope, definitions and perceived completeness. The evaluation of the completeness criteria was accomplished through five statements. The results show a general agreement among the participants for all given statements with mean => 4.00. Figure 7.2 presents the respondents' feedback in order to evaluate the completeness of the maturity model.

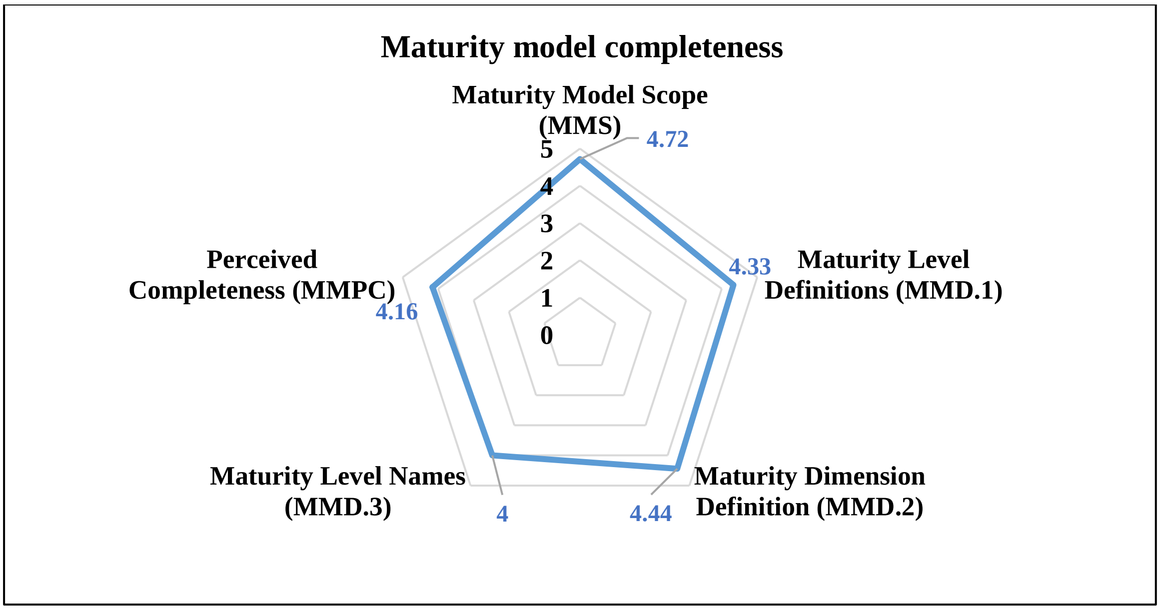

Figure 7.2 The respondents' feedback for maturity model completeness

7.5.2. Consistency

This criterion aims to evaluate the consistency level of abstraction, granularity and detail given within the maturity model. Internal consistency has been used to evaluate the consistency level of the maturity model. One statement has been used to investigate the respondents' level of agreement regarding the internal consistency of the maturity model, which is: "*There is a consistent level of abstraction, granularity, and detail given within the cloud data governance maturity model*". The results show a general agreement among the participants for given statement with mean = 4.66.

7.5.3. Practicality

This criterion aims to evaluate the practicality of implementing the cloud data governance maturity model, based on five sub-criteria: ease of use, ease of learning, understandability, practical utility and being tailorable. The evaluation of the practicality criteria is accomplished through five statements. The results show a general agreement among participants for all given statements with mean => 4.22. Figure 7.3 presents the respondents' feedback in order to evaluate the practicality of the maturity model.

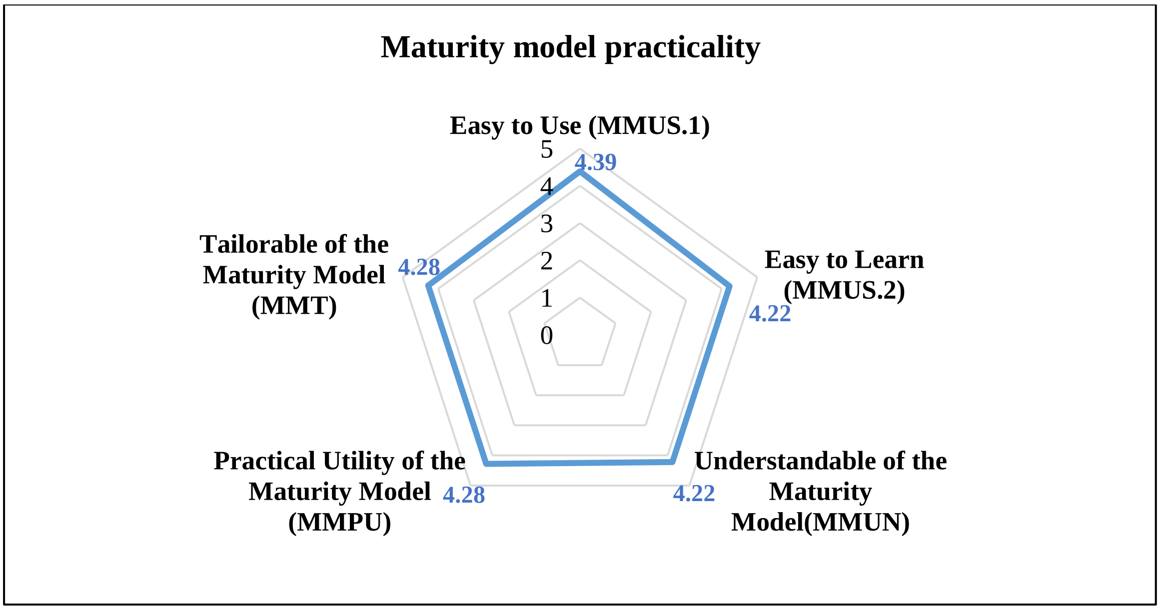

Figure 7.3 The respondent's feedback on the maturity model's practicality

7.5.4. Usefulness

This criterion aims to evaluate the usefulness of the maturity model for assessing and improving the cloud data governance processes in the organisation. It is based on two sub-criteria: perceived benefits and constructiveness. Thus, the evaluation of the usefulness criteria is accomplished through two statements. The results show a general agreement among participants for all given statements with mean => 4.50. Figure 7.4 presents the respondents' feedback in order to validate the usefulness of the maturity model.

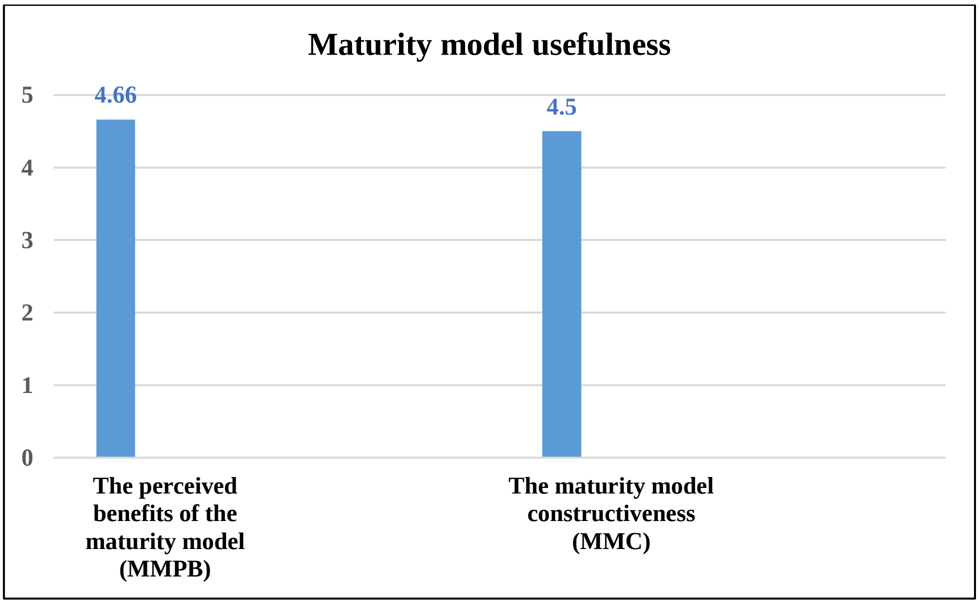

Figure 7.4 The respondents' feedback on the maturity model's usefulness

7.5.5. Verifiability

This criterion aims to evaluate the verifiability of the maturity model based on three sub-criteria: feasible test coverage, stability and verifiability. The evaluation of the verifiability criteria is accomplished through three statements. The results show a general agreement among participants for all given statements with mean => 4.0. Figure 7.5 presents the respondents' feedback in order to evaluate the verifiability of the maturity model.

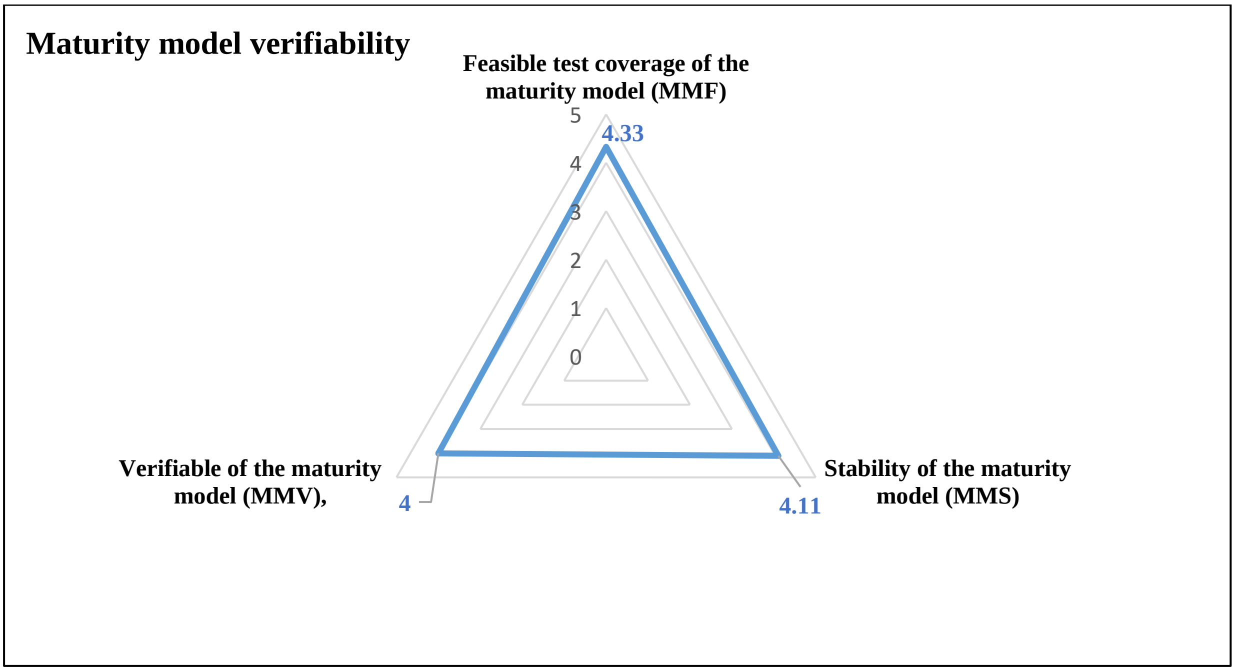

Figure 7.5 The respondent's feedback of the maturity model verifiability.

7.5.6. Overall Summary for the Evaluation of the Proposed Maturity Model

Table 7.2 shows the results summary regarding the participant groups' answers to the five criteria (completeness, consistency, practicality, usefulness and verifiability) in terms of the cloud data governance maturity model evaluation. The results show slight consistency among participants for all criteria for evaluation with mean ranging between 4 and 5.

Table 7.2 The participant groups' feedback on the maturity model based on each criterion

Sub-criteria	Completeness: Maturity model scope (MMS)	Completeness: Maturity model definition (MMD.1)	Completeness: Maturity model definition (MMD.2)	Completeness: Maturity model definition (MMD.3)	Completeness: Perceived completeness of the maturity model (MMPC)	Completeness: **Mean for Each Group**	Consistency: Internal consistency of the maturity model	Consistency: **Mean for Each Group**	Practicality: Usability of the maturity model (MMUS.1)	Practicality: Usability of the maturity model (MMUS.2)	Practicality: Understandable of the maturity model(MMUN)	Practicality: Practical utility of the maturity model (MMPU)	Practicality: Tailorable of the maturity model (MMT)	Practicality: **Mean for Each Group**	Usefulness: The perceived benefits of the maturity model (MMPB)	Usefulness: The maturity model constructiveness (MMC)	Usefulness: **Mean for Each Group**	Verifiability: Feasible test coverage of the maturity model (MMF)	Verifiability: Stability of the maturity model (MMS)	Verifiability: The verifiable of the maturity model (MMF)	Verifiability: **Mean for Each Group**
Government Organisations	4.66	4.50	4.33	4.50	4.83	4.56	4.50	4.50	4.66	4.16	4.66	3.83	3.83	4.23	5.00	4.50	4.75	4.00	4.33	4.50	4.28
Cloud Providers	5.00	4.50	4.50	4.00	5.00	4.60	5.00	5.00	4.00	4.00	4.00	4.50	4.50	4.20	4.50	4.50	4.50	4.50	4.00	4.00	4.17
Academy	4.50	4.00	4.50	3.50	4.00	4.10	4.50	4.50	4.50	4.50	4.00	4.50	4.50	4.40	4.50	4.50	4.50	4.50	4.00	3.50	4.00
Mean	4.72	4.33	4.44	4.00	4.61	4.42	4.66	4.66	4.39	4.22	4.22	4.28	4.28	4.28	4.66	4.50	4.58	4.33	4.11	4.00	4.15

Figure 7.6 shows that all the participant groups indicated their agreement with the evaluation criteria to support the cloud data governance maturity model evaluation.

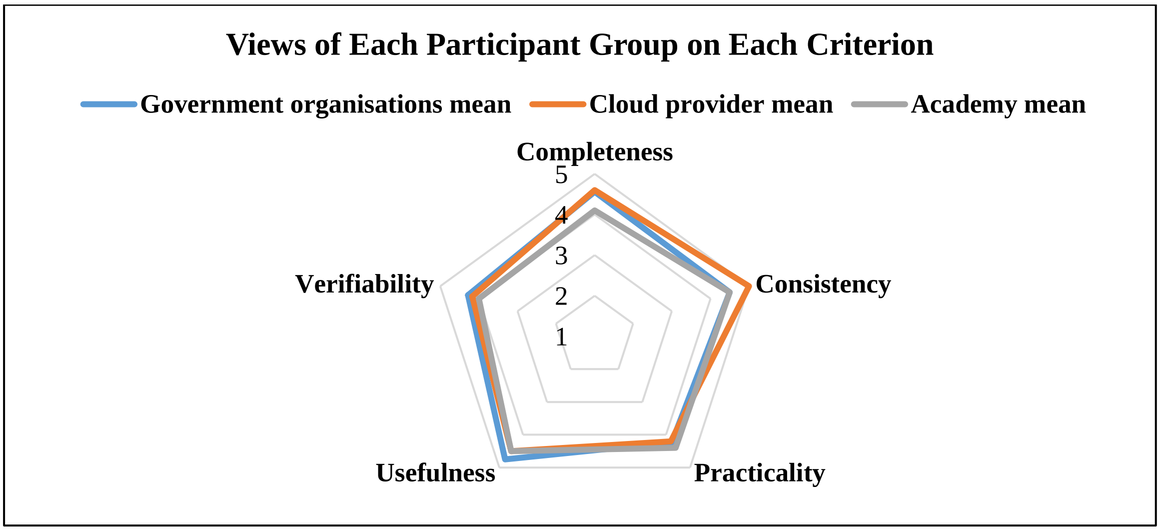

Figure 7.6 Participant groups' feedback to each criteria of the evaluation

7.5.7. Participants' Recommendations on Proposed Cloud Data Governance Maturity Model

As shown in the previous sections, the overall feedback from the focus group on the proposed cloud data governance maturity model was very positive, meeting all of the assessment criteria and being based on strong foundations. Recommendations to improve the cloud data governance maturity model were as follows:

- The majority of the participants suggested changing the level five name from "*converged*" to another relevant word related to the level's meaning, because the word converged may cause confusion with a network infrastructure keyword, and they suggested changing it to "*comprehensive*" or "*optimising*".
- Two participants suggested that within the maturity model diagram, each main dimension of the cloud data governance should also display its sub-dimensions.

As discussed in this section, the qualitative feedback indicated that the focus group participants suggested improving the design of the proposed maturity model. The first suggestion was accepted and the original diagram was amended to change the level five name from "converged" to "optimising". However, as the sub-dimensions were already displayed within the framework diagram and represented within the assessment matrix, displaying them in the maturity model would reduce its clarity. Therefore, the second suggestion was not accepted. The improved design of the cloud data governance maturity model is presented in Figure 7.7.

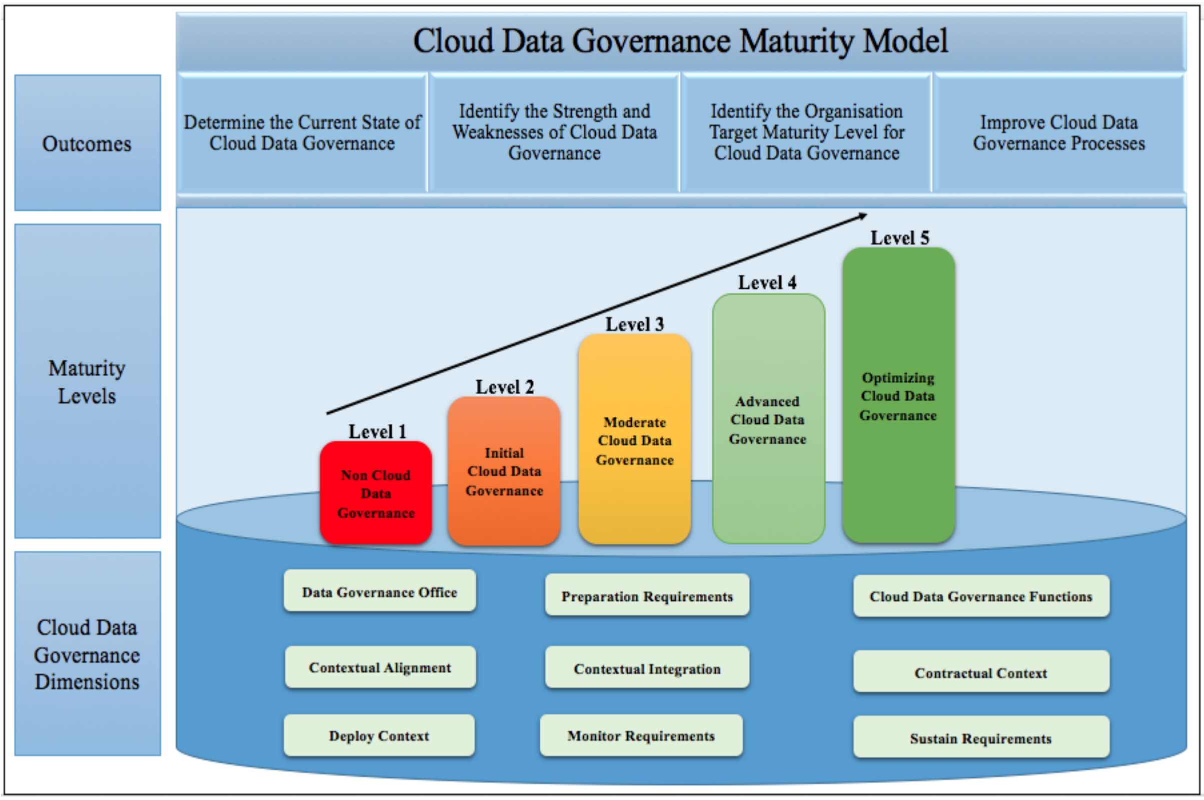

Figure 7.7 Amended maturity model after participants' feedback

7.6. Cloud Data Governance Assessment Matrix Evaluation

Six criteria were used to evaluate the proposed cloud data governance assessment matrix. These criteria are as follows: completeness, consistency, practicality, usefulness, verifiability, and strengths and weaknesses. This section presents the criteria assessment results based on the quantitative and qualitative feedback. Again, a Likert scale (agree-disagree scale) has been used to evaluate the assessment criteria; respondents specify their level of agreement or disagreement on a symmetric agree-disagree scale for a series of statements. Figure 7.8 illustration the cloud data governance assessment matrix evaluation process.

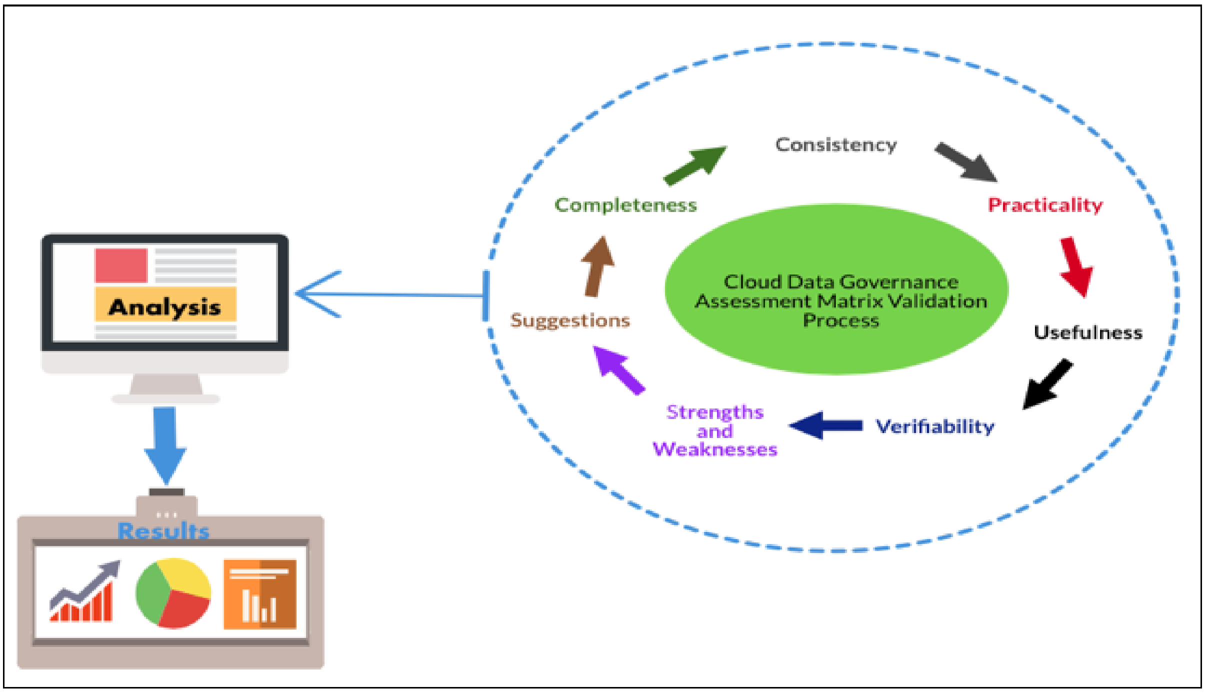

Figure 7.8 The cloud data governance assessment matrix evaluation process

The results for each criterion are presented below.

7.6.1. Completeness

The completeness criterion evaluated the mean value for three sub-criteria: scope, definitions and perceived completeness. The evaluation of the completeness criteria was accomplished through four statements. The results show a general agreement among participants for all given statements with mean => 4.27. Figure 7.9 presents the respondents' feedback to evaluate the assessment matrix's completeness.

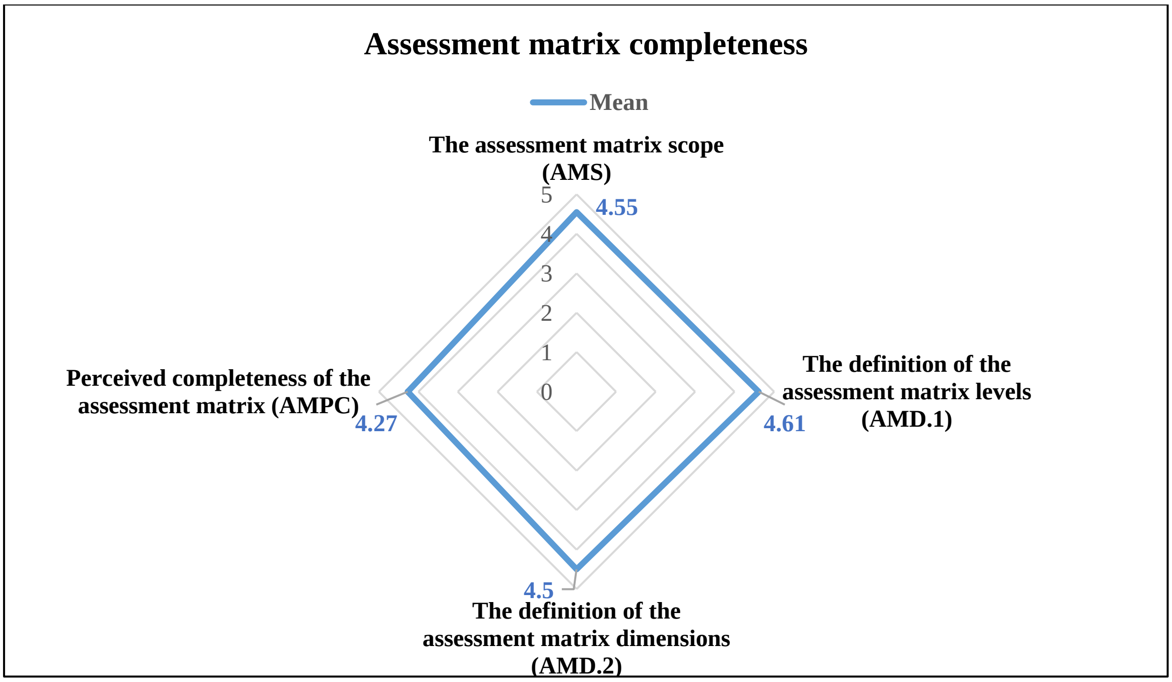

Figure 7.9 The respondents’ feedback for assessment matrix completeness

7.6.2. Consistency

This criterion aims to evaluate the consistency level of abstraction, granularity and detail given within the assessment matrix. Internal consistency has been used to evaluate the consistency level of the assessment matrix. One statement has been used to investigate the respondents’ level of agreement regarding internal consistency of the assessment matrix, which is: “*There is a consistent level of abstraction, granularity and detail given within the cloud data governance assessment matrix*”. The results show a general agreement among participants for given statement with mean = 4.16.

7.6.3. Practicality

This criterion aims to evaluate the practicality of implementing the cloud data governance assessment matrix, based on five sub-criteria: ease of use, ease of learning, understandability, practical utility and being tailorable. The evaluation of the practicality criteria is accomplished through five statements. The results show a general agreement among participants for all given statements with mean => 4.44. Figure 7.10 presents the respondents’ feedback in order to evaluate the practicality of the assessment matrix.

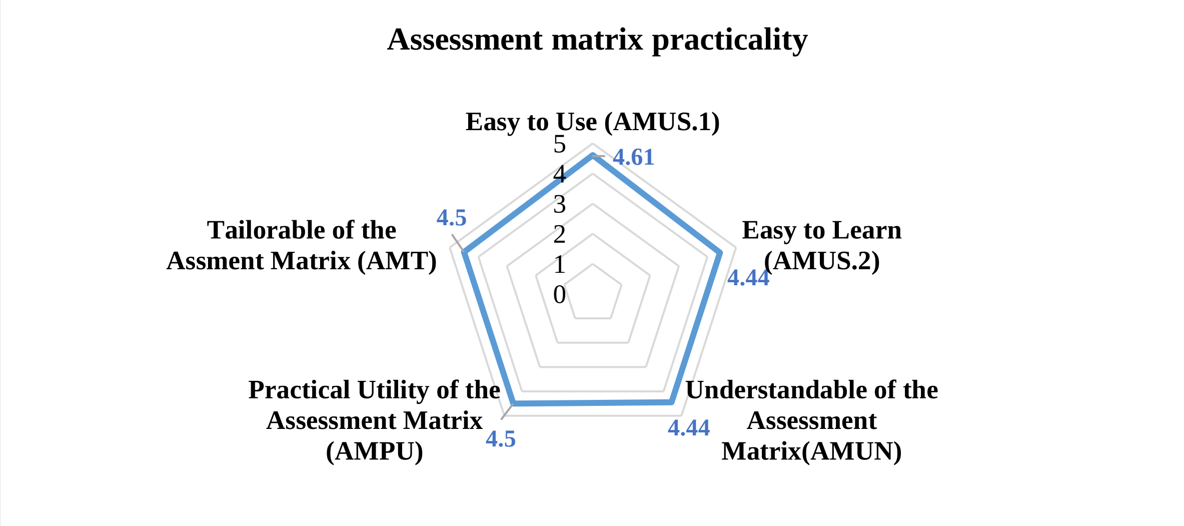

Figure 7.10 The respondents' feedback on the assessment matrix's practicality.

7.6.4. Usefulness

This criterion aims to evaluate the usefulness of the assessment matrix for assessing and improving the cloud data governance processes in the organisation. It is based on two sub-criteria: perceived benefits and constructiveness. Thus, the evaluation of the usefulness criteria is accomplished through two statements. The results show a general agreement among participants for all given statements with mean => 4.66. Figure 7.11 presents the respondents' feedback in order to evaluate the usefulness of the assessment matrix.

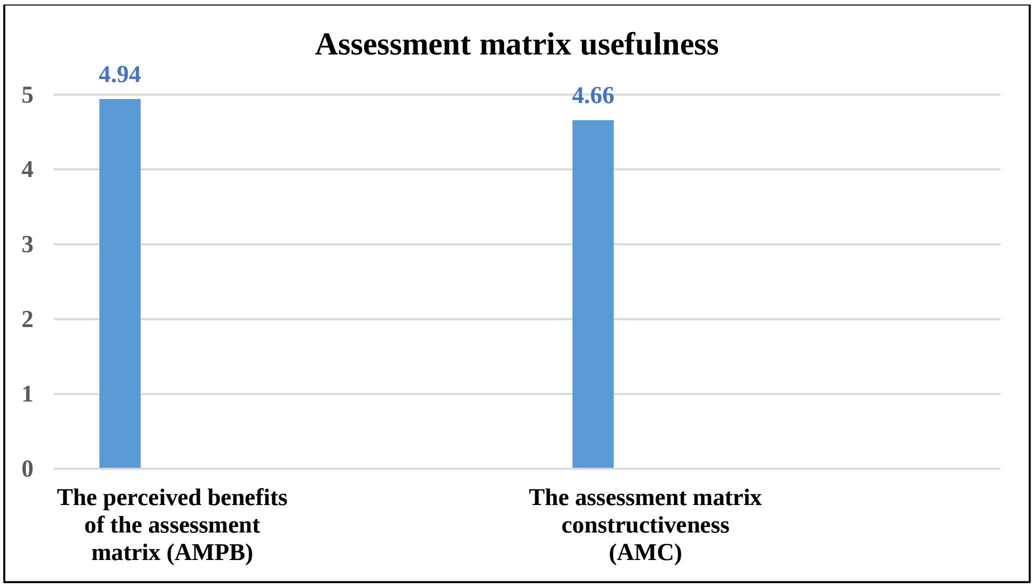

Figure 7.11 The respondents' feedback on the usefulness of the assessment matrix

7.6.5. Verifiability

This criterion aims to evaluate the verifiability of the assessment matrix based on three sub-criteria: feasible test coverage, stability and verifiability. The evaluation of the verifiability criteria is accomplished through three statements. The results show a general agreement among participants for all given statements with mean => 4.16. Figure 7.12 presents the respondents' feedback in order to evaluate the verifiability of the assessment matrix.

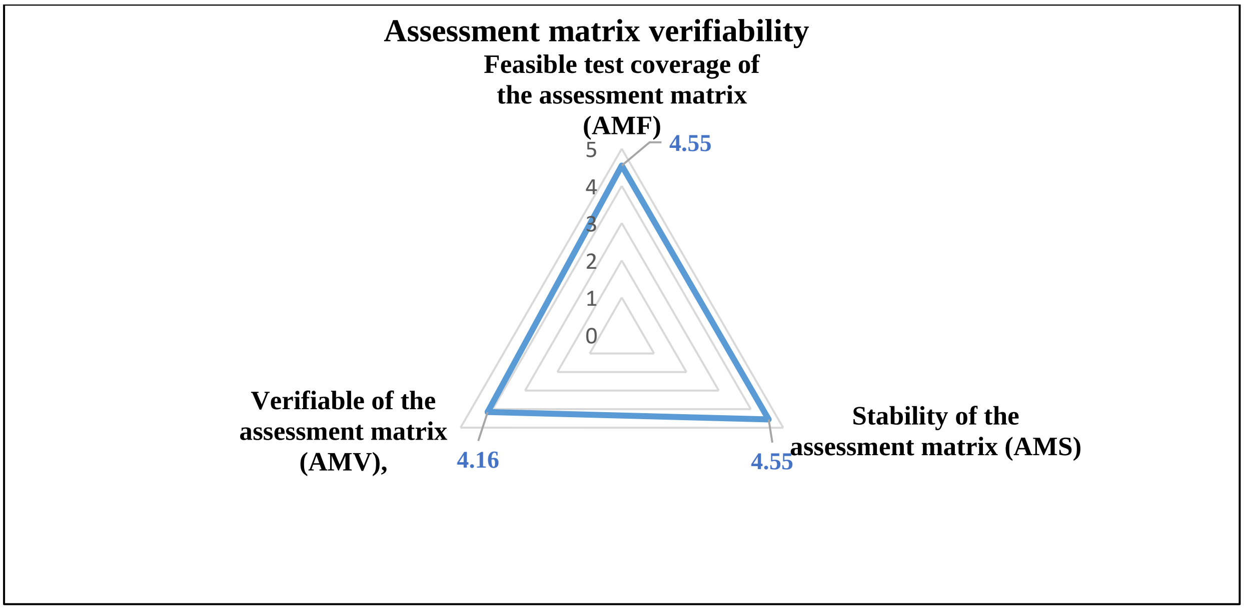

Figure 7.12 The respondents' result in order to validate the verifiability of the assessment matrix

7.6.6. Strengths and Weaknesses

This criterion aims to evaluate the strengths and weaknesses of the assessment matrix based on two sub-criteria: individual level and individual dimension in assessment matrix. A Likert scale of agreement from 5 (strongly agree) to 1 (strongly disagree) was used to indicate whether the participants agreed or disagreed with each statement to rate the strengths and weaknesses of the assessment matrix.

a) Individual Level in Assessment Matrix

This criterion aims to evaluate the strengths and weaknesses of the assessment matrix levels' contents to measure the constructs of cloud data governance. Five statements were used to assess the strengths and weaknesses of the assessment matrix levels' contents, and these statements were coded using LS.n. Figure 7.13 shows the results for the strengths and weaknesses of the individual levels in the assessment matrix.

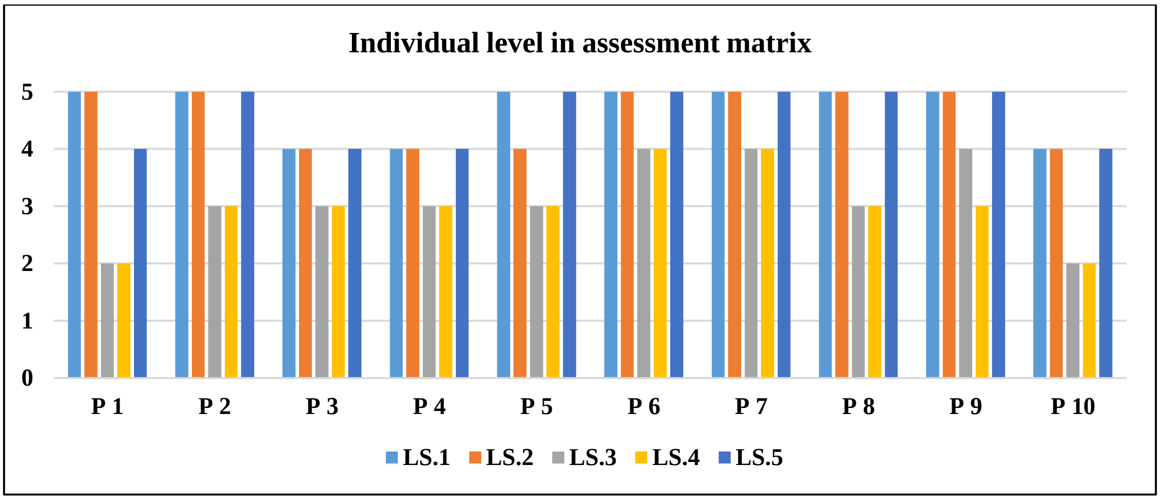

Figure 7.13 The results for the strengths and weaknesses of the individual levels in the assessment matrix

Figure 7.13 shows the participants' feedback on the statement regarding the evaluation of the strengths and weaknesses of the assessment matrix levels to measure the constructs of cloud data governance. The results show that all participants agreed with these statements except two statements which were (LS.3 and LS.4), with mean => 4.60. LS.3 and LS.4 statements were used to evaluate the strengths and weaknesses of the content of levels 3 and 4. The results show that most of the participants reported a neutral response with mean => 3.00. Regarding the first statement (LS.1), which was "*Level 1 in the assessment matrix provides strong content to measure the constructs of the cloud data governance maturity model*", the results show that most of the participants strongly agreed (mean= 4.70). The second statement (LS.2) was "*Level 2 in the assessment matrix provides strong content to measure the constructs of the cloud data governance maturity model*", and the results also show that most of the participants selected strongly agree (mean = 4.60). With regard to the third statement (LS.3), which was "*Level 3 in the assessment matrix provides strong content to measure the constructs of the cloud data governance maturity model*", the results show that most of the participants gave the neutral response (mean= 3.10). For the fourth statement (LS.4), which was "*Level 4 in the assessment matrix provides strong content to measure the constructs of the cloud data governance maturity model*", the results also show that most of the participants reported themselves as neutral (mean= 3.00). Finally, for the fifth statement (LS.5), which was "*Level 5 in the assessment matrix provides strong content to measure the constructs of the cloud data governance maturity model*", the results show that most of the participants selected strongly agree (mean = 4.60).

b) Individual Dimension in Assessment Matrix

This criterion aims to evaluate the strengths and weaknesses of the assessment matrix dimensions' contents to measure the constructs of cloud data governance. Nine statements were used to assess the strengths and weaknesses of the assessment matrix contents to measure the constructs of the cloud data governance framework. These statements were coded with DS.n. Figure 7.14 shows the results for the strengths and weaknesses of the individual dimensions in the assessment matrix.

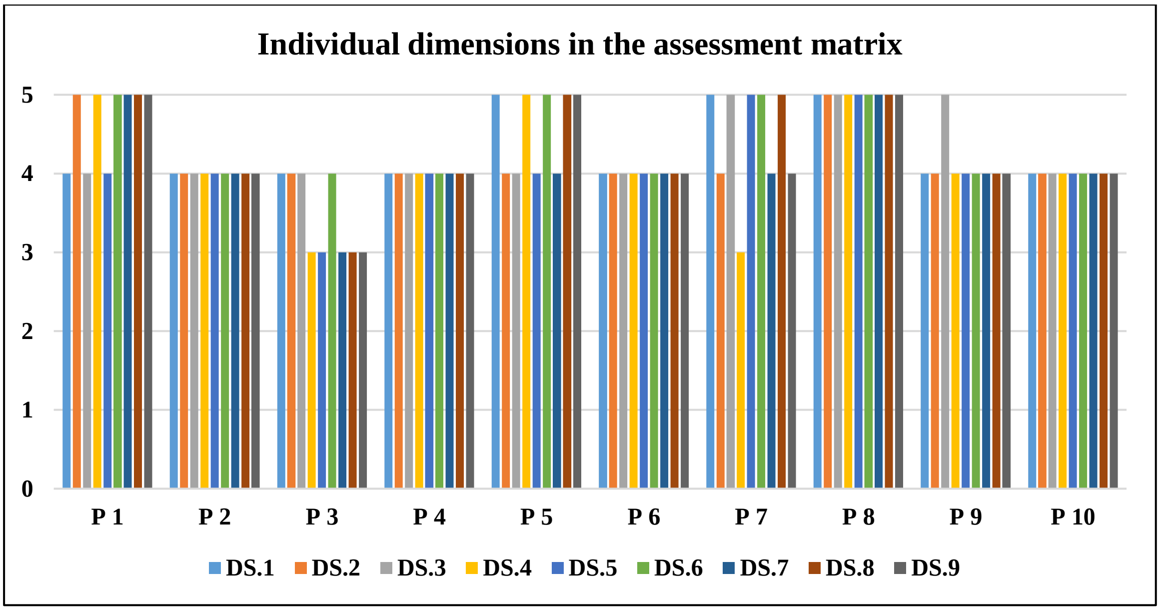

Figure 7.14 The results for the strength and weaknesses of the individual dimensions in the assessment matrix

Figure 7.14 shows the participants' answers to the statements regarding the evaluation of the strengths and weaknesses of the assessment matrix dimension to measure the constructs of cloud data governance. The results show that most of the participants agreed with these statements with mean => 4.10. Regarding the first statement (DS.1), which was "*the assessment matrix provides strong content to measure the cloud data governance office construct in the cloud data governance framework for each maturity level*", the results show that most of the participants agreed with this statement (mean = 4.30). The second statement (DS.2), which was "*the assessment matrix provides strong content to measure the preparation requirements construct in the cloud data governance framework for each maturity level*", the results show that most of the participants agreed with this statement (mean = 4.20). With regards to the third statement (DS.3), which was "*the assessment matrix provides strong content to measure the cloud data governance functions construct in the* *cloud data governance framework for each maturity level*", the results also show that most of the participants agreed with this statement (mean = 4.30).

For the fourth statement (DS.4), which was "*the assessment matrix provides strong content to measure the contextual alignment construct in the cloud data governance framework for each maturity level*", the results also show that most of the participants agreed with this statement (mean = 4.10). Regarding the fifth statement (DS.5), which was "*the assessment matrix provides strong content to measure the contextual integration construct in the cloud data governance framework for each maturity level*", the results show that most of the participants agreed with this statement (mean = 4.10). For the sixth statement (DS.6), which was "*the assessment matrix provides strong content to measure the contractual context construct in the cloud data governance framework for each maturity level*", the results show that most of the participants agreed with this statement (mean = 4.40).

For the seventh statement (DS.7), which was "*the assessment matrix provides strong content to measure the deploy context construct in the cloud data governance framework for each maturity level*", the results show that most of the participants agreed with this statement (mean = 4.10). Regarding the eighth statement (DS.8), which was "*the assessment matrix provides strong content to measure the sustain requirements construct in the cloud data governance framework for each maturity level*", the results show that most of the participants agreed with this statement (mean = 4.30). Finally, for the last statement (DS.9), which was "*the assessment matrix provides strong content to measure the monitor requirements construct in the cloud data governance framework for each maturity level*", the results show that most of the participants agreed with this statement (mean = 4.20).

7.6.7. Overall Summary for the Evaluation of the Cloud Data Governance Assessment Matrix

Table 7.3 shows the results summary regarding the participant groups' answers to the five criteria (completeness, consistency, practicality, usefulness, and verifiability) in terms of the cloud data governance maturity model evaluation. The results show slight consistency among participants for all criteria for validation with mean ranging between 4 and 5.

Table 7.3 The participants' feedback on the assessment matrix based on each criterion

Criterion	Sub-criteria	Government Organisations	Cloud Providers	Academy	Mean for each criterion
Completeness	Assessment matrix scope (AMS)	4.66	4.50	4.50	4.55
	Assessment matrix definition (AMD.1)	4.33	5.00	4.50	4.61
	Assessment matrix definition (AMD.2)	4.00	5.00	4.50	4.50
	Perceived completeness of the assessment matrix (AMPC)	3.83	4.50	4.50	4.27
	Mean for Each Group	4.21	4.75	4.50	4.48
Consistency	Internal consistency of the assessment matrix	4.00	4.50	4.00	4.16
	Mean for Each Group	4.00	4.50	4.00	4.16
Practicality	Usability of the assessment matrix (AMU.1)	4.83	4.50	4.50	4.61
	Usability of the assessment matrix (AMU.2)	4.33	4.50	4.50	4.44
	Understandable of the assessment matrix (AMUN)	4.33	4.50	4.50	4.44
	The practical utility of the assessment matrix (AMPU)	4.50	4.50	4.50	4.50
	Tailorable of the assessment matrix (AMT)	4.50	5.00	4.00	4.50
	Mean for Each Group	4.50	4.60	4.40	4.50
Usefulness	Perceived benefits of the assessment matrix (AMPB)	4.83	5.00	5.00	4.94
	The assessment matrix constructiveness (AMC)	4.50	4.50	5.00	4.66
	Mean for Each Group	4.67	4.75	5.00	4.80
Verifiability	Feasible test coverage of the maturity model (MMF)	4.66	4.50	4.50	4.55
	Stability of the maturity model (MMS)	4.66	4.50	4.50	4.55
	The verifiable of the maturity model (MMF)	4.00	4.50	4.00	4.16
	Mean for Each Group	4.44	4.50	4.33	4.42

Figure 7.15 shows that all the participant groups indicated their agreement with the evaluation criteria to support the cloud data governance assessment matrix evaluation.

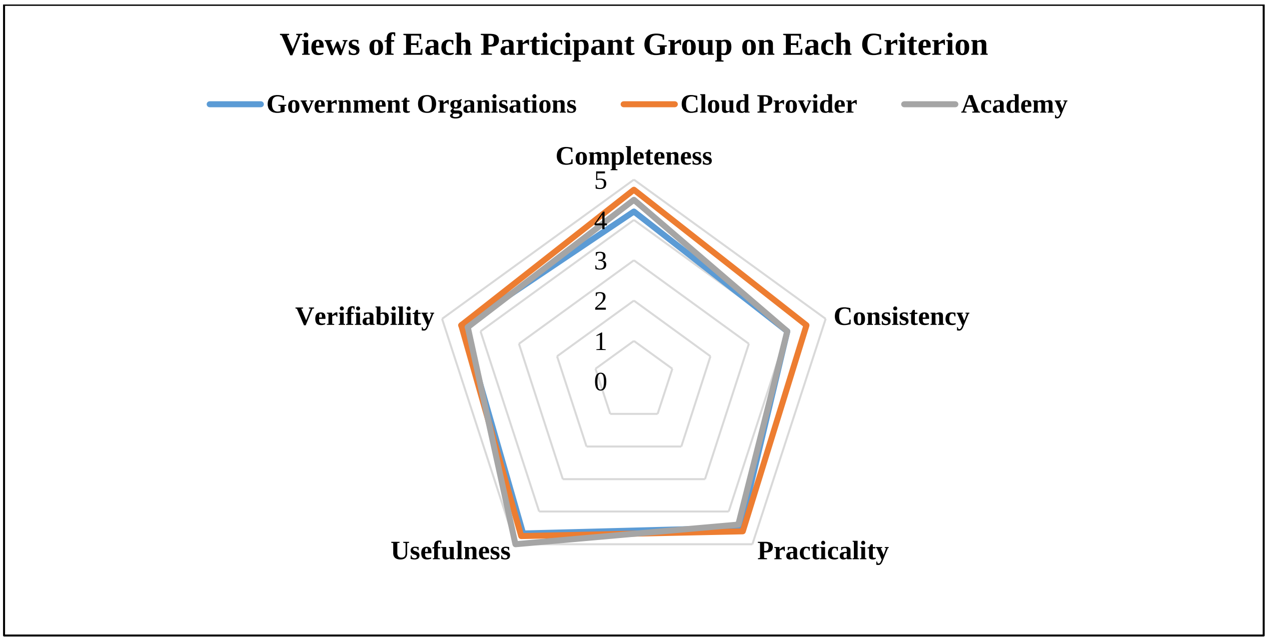

Figure 7.15 The participant groups' feedback on the assessment matrix based on each criterion

7.6.8. Participants' Recommendations to Improve the Proposed Assessment Matrix

As shown in the previous sections, the overall feedback from the focus group on the proposed cloud data governance assessment matrix was very positive, meeting all of the assessment criteria and being based on strong foundations. Additionally, a number of recommendations were suggested in the participants' feedback, he main recommendations were:

1. Clarify incomplete and complete – to clarify this, there were a number of recommendations from the participants as follows:
   - Some of the participants suggested changing the word "*incomplete*" for each dimension in level 3 to "*achieve some requirements*" or "*representing less than 60%*".
   - Some of the participants suggested adding the number of items for each dimension in the assessment matrix to improve it and to change the word "*incomplete*" in level 3 to be "*satisfy n-1 items from n*".
   - Some of the participants suggested adding the number of items for each dimension in the assessment matrix to improve it and to change the word "*complete*" in level 4 to be "*satisfy all (n) items from n*".
2. Developing an application tool in order to assess the state of cloud data governance in organisations in a real environment, to prove that it is working perfectly.

The suggestions above were taken into consideration in this research. In order to the first suggestion it was clarified in chapter Four, and the second suggestion also consider in this research by developing tool to practically test the research findings in a real case scenario and it presents in next section.

7.7. Practical Evaluation of the Research Findings

As part of the evaluation, it was important to practically test the research findings in a real case scenario as was suggested by the participants in the focus group. Therefore, two case scenarios were used to examine the practicality of using the cloud data governance framework in a real-life environment. The case scenario considered two public sector organisations in Saudi Arabia, which were adopting some cloud computing services. These organisations belong to military and the healthcare sectors, respectively. To do this, a tool was designed and developed that helps decision makers to assess the cloud data governance in their organisations, based on the proposed cloud data governance framework, maturity model and assessment matrix. This proposed tool was designed for testing purposes, however, its potential can be considerable, and it can be used to: i) support decision makers in their decision making related to cloud data governance implementation; ii) inform decision makers about the current level of cloud data governance in their organisations; iii) inform decision makers about the strengths and weaknesses of each dimension of cloud data governance; and iv) allow decision makers to improve cloud data governance implementation by identifying their target level. This tool is hereafter called the maturity assessment & recommendation system of cloud data governance (MARS-CDG).

7.7.1. Presentation of the MARS-CDG Tool

The proposed tool was implemented using Python as a programming language, with Python Libraries Flask, Jinja2, and SQLAlchemy. SQLite was used as a database engine in the tool development. Furthermore, the design of user-friendly interfaces was considered in this study to enhance the usability of the tool, but this was not the main focus. The main screenshots of the tool are presented below for illustration. These screenshots provide details of the step-by-step process to use the proposed tool utilities. The map of the MARS-CDG tool is as follows:

1. Create account and fill in user information, including first name, last name, organisation's name, username and password.

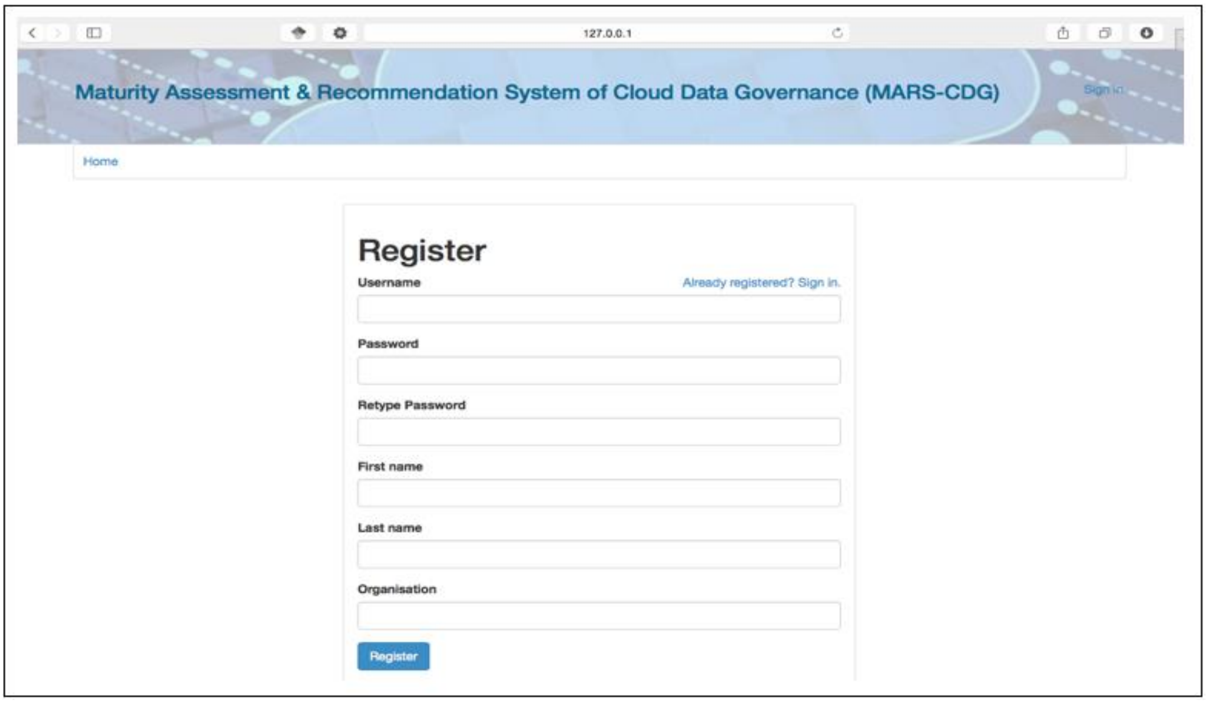

Figure 7.16 The registration form

2. User sign in to access the MARS-CDG tool.

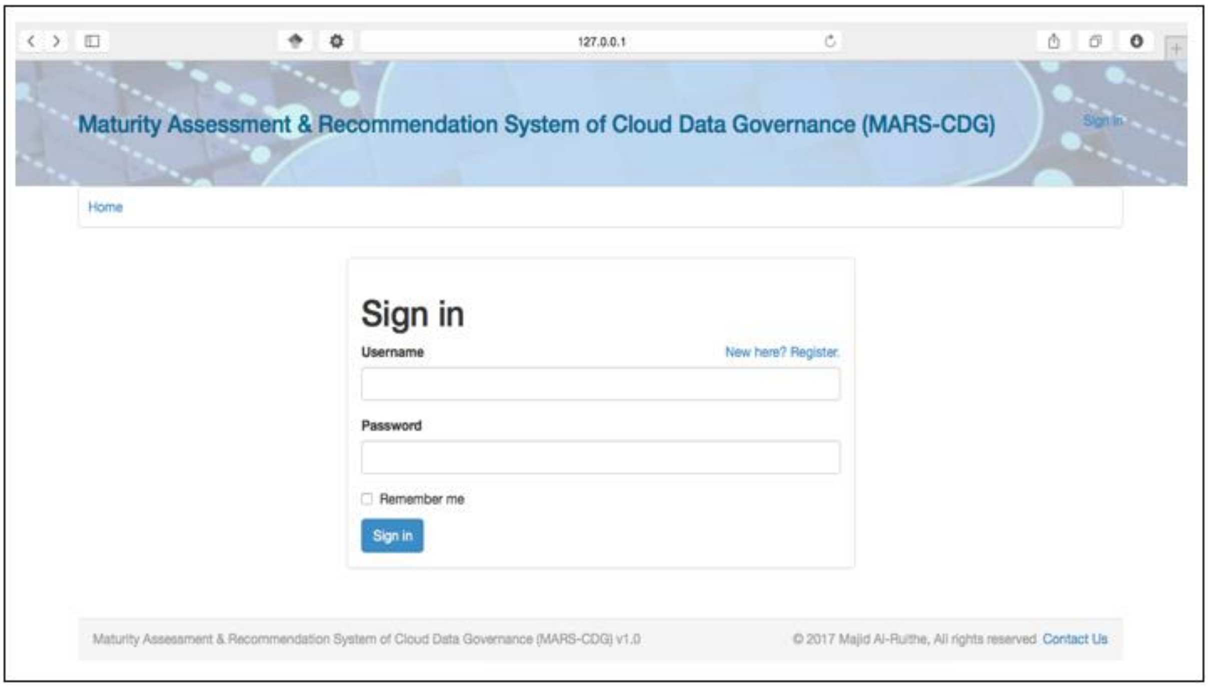

Figure 7.17 The sign in form

3. Access the home page, which includes an overview of the MARS-CDG tool.

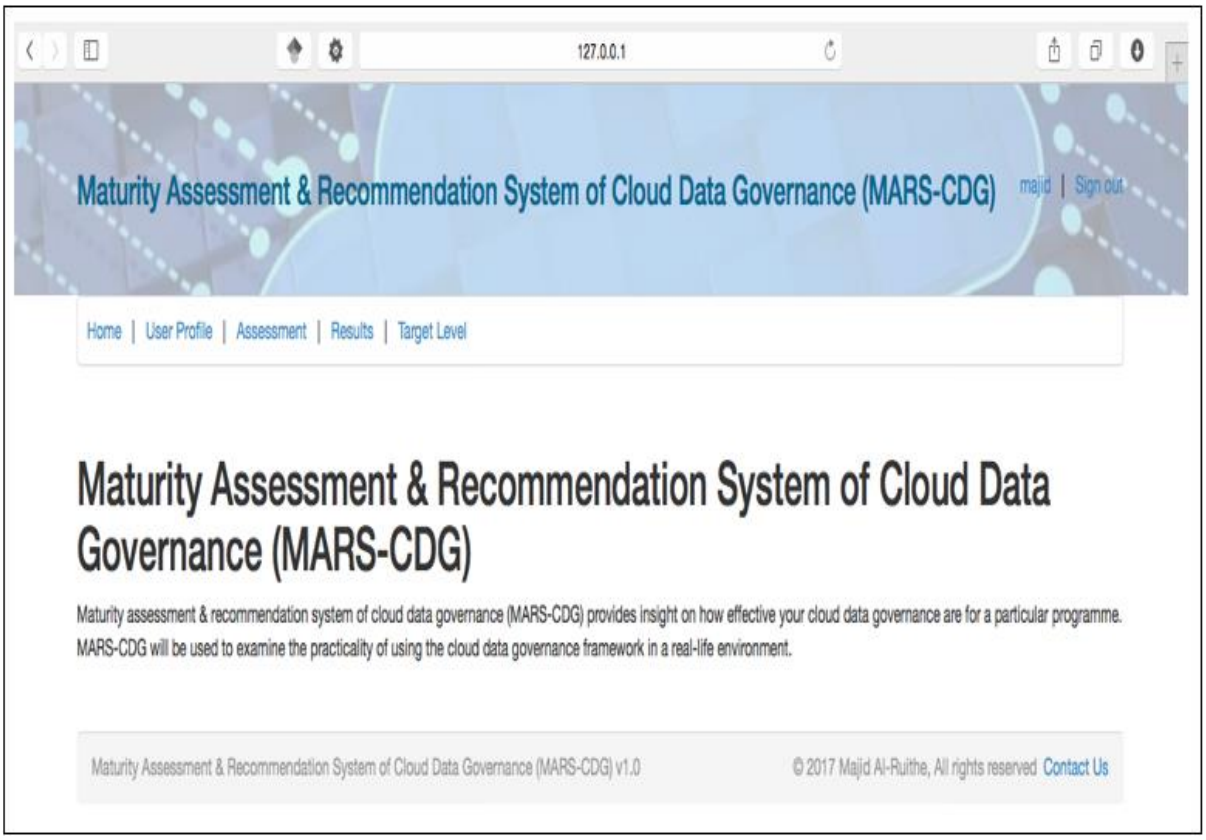

Figure 7.18 The home page

4. Access the user profile form, which allows a user to change his username/password.

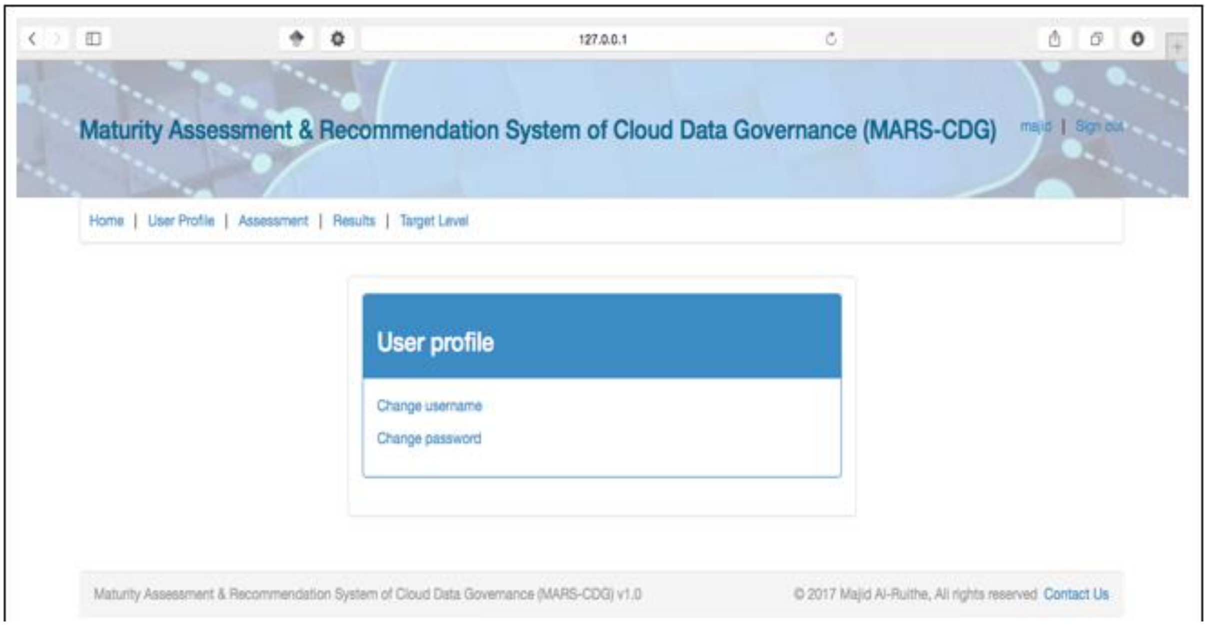

Figure 7.19 The user profile form

5. Access to the initial page to guide the user on how to use the MARS-CDG tool to start the assessment

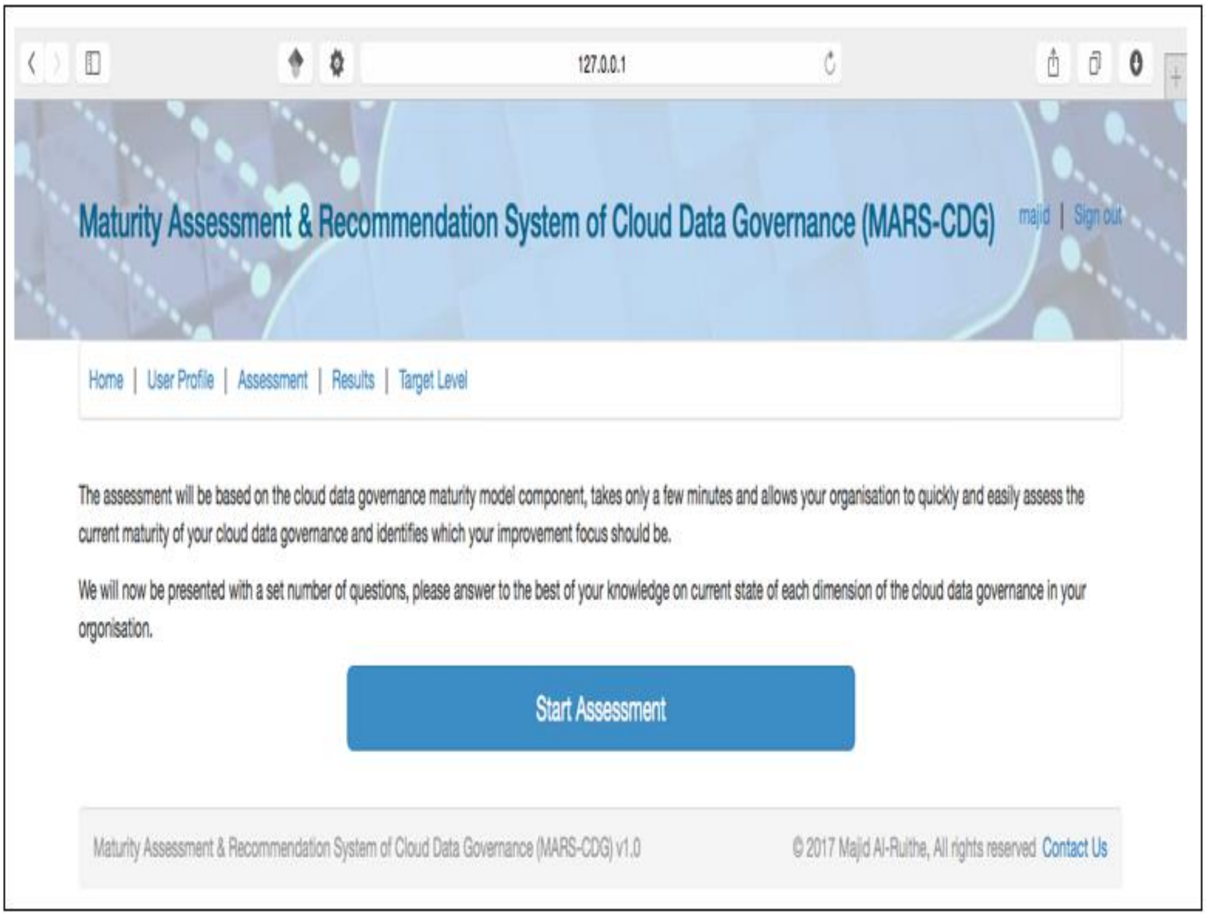

Figure 7.20 The initial page of the cloud data governance assessment

6. Start the assessment process.

Figure 7.21 The example of the assessment process

7. Present the results of the cloud data governance assessment, the maturity level for each dimension and the overall maturity level for cloud data governance in the organisation presented in this page.

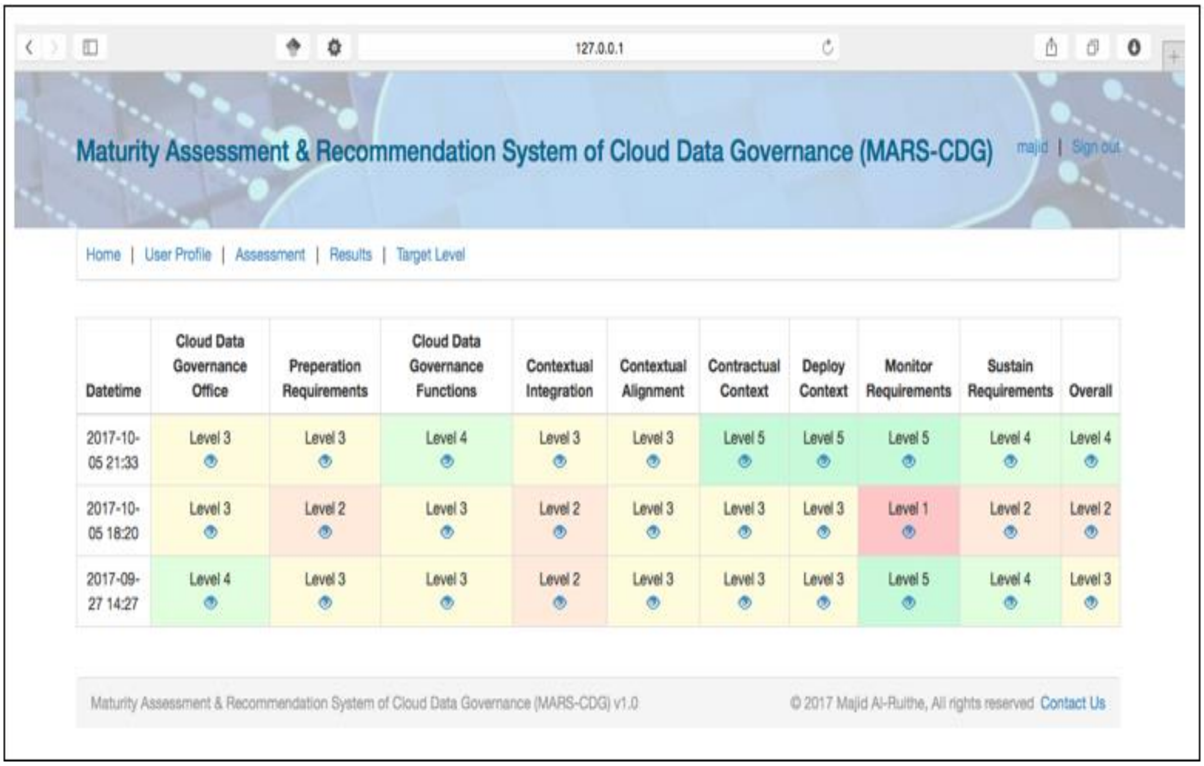

Figure 7.22 The results page of the cloud data governance assessment

8. Present the assessment results for the cloud data governance dimension. This page includes: assessment details, weakness/strength results, and cart bar/radar chart to present the level for each sub-dimension in the main dimension of cloud data governance.

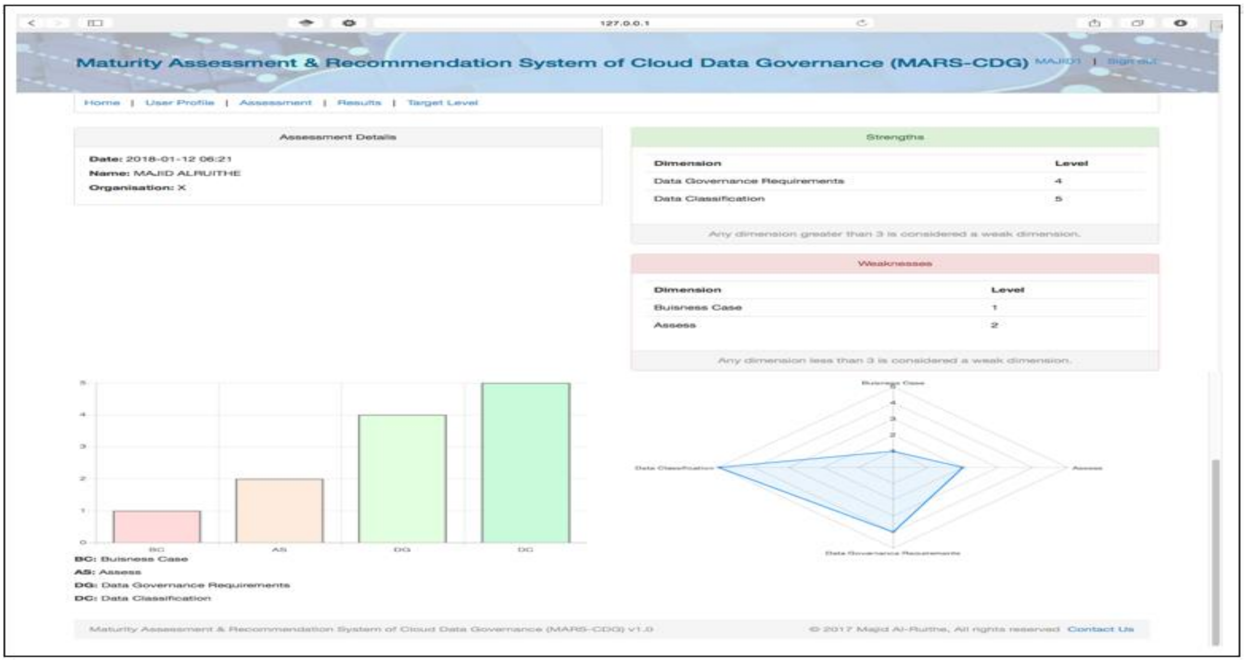

Figure 7.23 The example of the assessment results for cloud data governance dimension

9. The user calculates the target level based on the results of the last assessment.

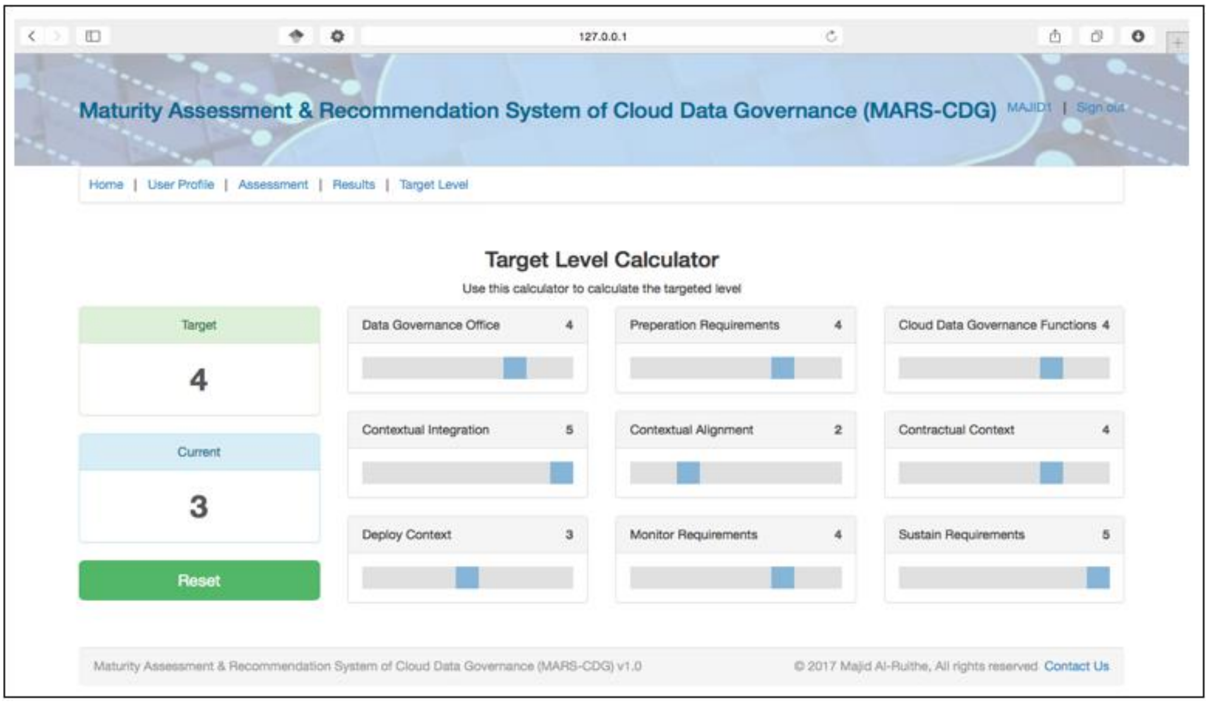

Figure 7.24 The target level page

7.7.2. Decision Algorithm for Maturity Level

In order to decide on the maturity level of a cloud data governance programme in an organisation, it needs to be calculated by a decision algorithm. Each dimension of cloud data governance needs to be measured by this algorithm, based on the state of any one dimension in the organisation. This information is given by the users in their responses to given requirements defined in the proposed assessment matrix. The steps of the decision algorithm procedures are shown in the flowchart depicted in Figure 7.25, and explained below.

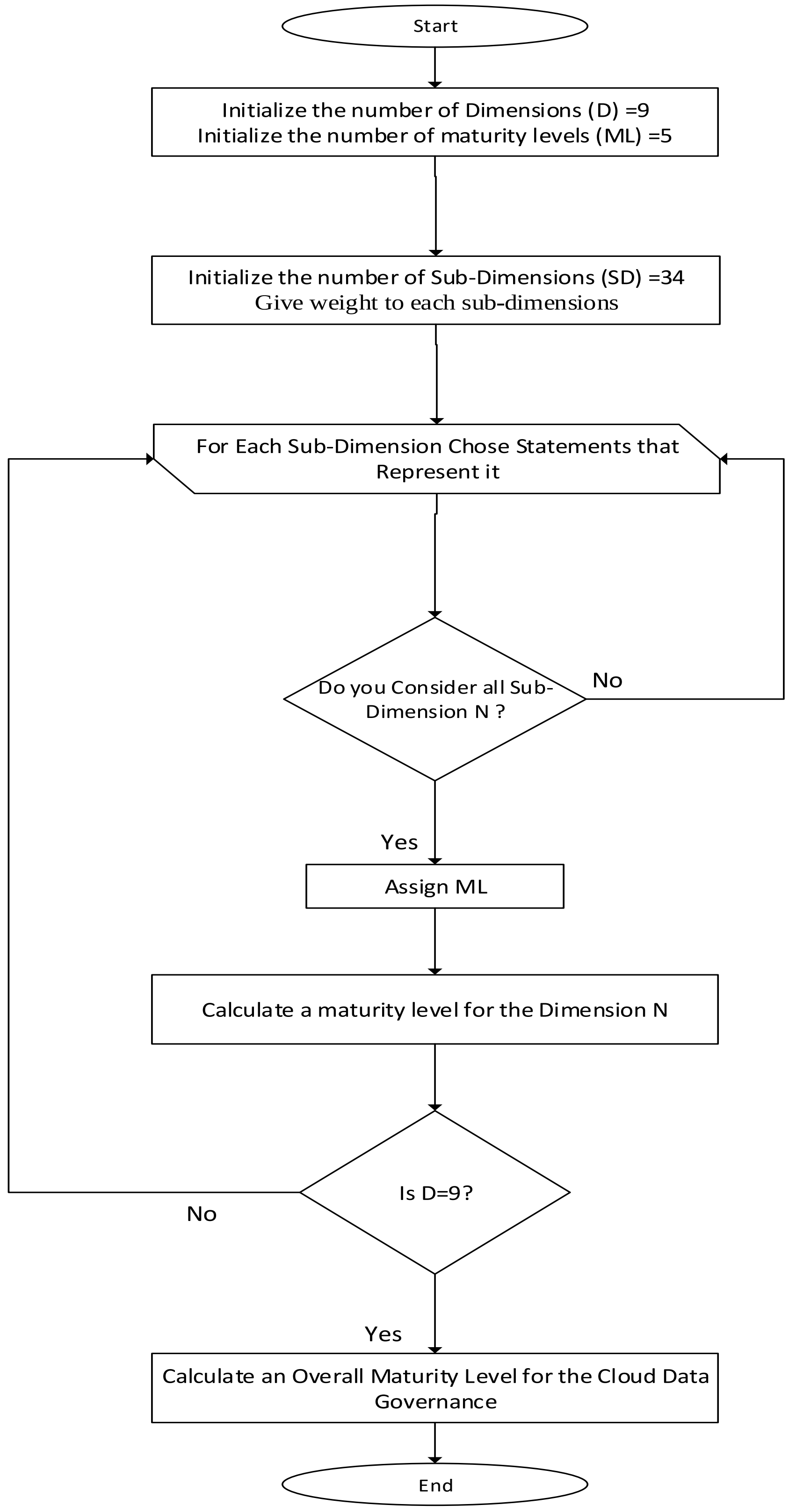

Figure 7.25 The decision algorithm for maturity level flowchart

Step 1: Defining the core dimensions and maturity levels.

In this step, the nine core dimensions that are used to assess the cloud data governance in the organisation are defined. These dimensions have been mentioned in Chapter Four, and they are coded by *(D)* in this algorithm. Additionally, five maturity levels described in Chapter Four are defined in this step; these levels are used to assess these dimensions, and are coded by *(ML)* in the proposed algorithm.

Step 2: Defining the sub-dimensions for all core dimensions.

In this step, the sub-dimensions that are used to assess the core dimensions for cloud data governance are defined. These sub-dimensions were described in Chapter Four and are coded by *(SD)* in the proposed algorithm.

Step 3: Giving a weight to each sub-dimension.

All defined core dimensions are assumed to be equally important. Therefore, the maturity level of these core dimensions is based on their relevant sub-dimensions, which are calculated based on the weight assigned to each sub-dimension. In a similar way, within each core dimension a weight average is assigned to the sub-dimension. To calculate the sub-dimension weight, the following formula is used:

$$\textbf{Sub} - \textbf{dimension weight} = \frac{\mathbf{1}}{\boldsymbol{SDN}} \qquad \text{Equation 7.1}$$

In this formula, *SDN* is the number of sub-dimensions in any one dimension.

Step 4: Survey and measure the maturity level for each sub-dimension.

In order to measure the cloud data governance maturity, all sub-dimensions are measured and assessed based on the multiple statements.

Step 5: Calculate the maturity level for each sub-dimension.

After measuring each sub-dimension of cloud data governance, the maturity level for each sub-dimension will be assigned based on their selected statement(s).

Step 6: Calculate the maturity level for each core dimension.

After measuring all the sub-dimensions of the core dimension, the maturity level for each core dimension will be calculated based on the average of the weighted maturity of all its sub-dimensions. To calculate the maturity level for each dimension in cloud data governance, the following formula is used:

$$\textbf{The Maturity Level} = \frac{\sum_{i=1}^{n} \textbf{Maturity Level (i)} * \textbf{Weight (i)}}{\sum_{i=1}^{n} 5 * \textbf{Weight (i)}} * \ \mathbf{5} \qquad \text{Equation 7.2}$$

In this formula, *n* is the number of sub-dimensions and *5* indicates the number of maturity levels.

Step 7: Calculate the overall maturity level.

After calculating the maturity level for each dimension, the overall maturity level will be calculated. The overall maturity level is the average of the weighted maturity of all the dimensions. To calculate the overall maturity level for the cloud data governance in the organisation, the following formula is used:

$$\textbf{The Overall Maturity Level} = \frac{\sum_{i=1}^{n} \textbf{Maturity Level (i)}}{\mathbf{N}} \qquad \text{Equation 7.3}$$

In this formula, *N* is the number of dimensions.

The steps in the decision algorithm for the maturity level calculation are illustrated below.

Algorithm 1: Algorithm for maturity level decision

Input: D, where D= Set of Dimension

: ML, where ML= Set of Maturity Level

: SD, where SD= Set of Sub-Dimension

: S, where S= Set of statement to determine ML for each Sub-Dimension

Output: Decision Cloud Data Governance Maturity Level

Require: D$\neq \phi$, *Numb_* D= 9

:N$\neq \phi$, *Numb_* ML= 5

:SD$\neq \phi$, *Numb_* SD =34

: :S$\neq \phi$, *Numb_* S =5

1: Initialise parameters D, ML,SD, S, W

2: Numb_ D= 9

3: Initialise SD for D

4: Numb_ SD for D1=3

Numb_ SD for D2=4

Numb_ SD for D3=4

Numb_ SD for D4=8

Numb_ SD for D5=2

Numb_ SD for D6=2

Numb_ SD for D7=3

Numb_ SD for D8=3

Numb_ SD for D9=5

Initialise S to ML in each SD

Numb_ S =5

Apply statements for SD to assess D then

$$\mathrm{W} = \frac{1}{SDN}$$

If Numb_ SD = 34 then do

$$\mathrm{ML} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{ML}\ (\mathrm{i})\ *\ \mathrm{W}\ (\mathrm{i})}{\sum_{\mathrm{i}=1}^{\mathrm{n}} 5 * \mathrm{W}\ (\mathrm{i})} *\ 5$$

Assign ML for SD

Else if Numb_ SD not met do

Return apply statements for SD to find consideration

Repeat until *Numb*_ SD=34

While *Numb*_ SD=34 then

End if

End if

End While

$$\mathrm{ML} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{ML}\ (\mathrm{i})}{\mathrm{N}}$$

Assign ML for cloud data governance

End

The subsequent sections present two real case scenarios when the proposed tool was used to assess the maturity level of two real organisations in Saudi Arabia.

7.7.3. Case Scenario One: Organisation A

The first case scenario comprises an organisation that is part of the military sector with around 5000 employees. According to the questionnaire results, organisation A has been adopting some cloud computing services, and it is planning to expand these in the near future.

- **Analysis of the Current Level of Cloud Data Governance in Organisation A using MARS-CDG Tool**

To assess the current state of the cloud data governance implementation, the IT manager at organisation A was requested to address all of the statements represented by all the defined sub-dimensions, depending on which maturity level was calculated. Table 7.4 shows the dimension levels and the overall level of cloud data governance in organisation A.

Table 7.4 The overall level of cloud data governance in organisation A

Cloud Data Governance Dimensions	Maturity Level	Overall Level
Cloud Data Governance Office	Level 2	***Level 2***
Preparation Requirements	Level 2	
Cloud Data Governance Functions	Level 2	
Contextual Integration	Level 2	
Contextual Alignment	Level 2	
Contractual Context	Level 1	
Deploy Context	Level 1	
Monitor Requirements	Level 1	
Sustain Requirements	Level 1	

Table 7.4 shows the maturity level of each dimension of cloud data governance in the organisation A. The results show that overall, the cloud data governance implementation in this organisation was at level 2, which is weak and informal, and requires some serious attention. It was interesting for this organisation to recognise the importance of data governance for its cloud provision; there was some evidence of this already as their IT team seem to deal with some aspects of data governance, but they do so in an ad-hoc way. Figure 7.26 shows the current state of cloud data governance implementation in organisation A, based on their assessment.

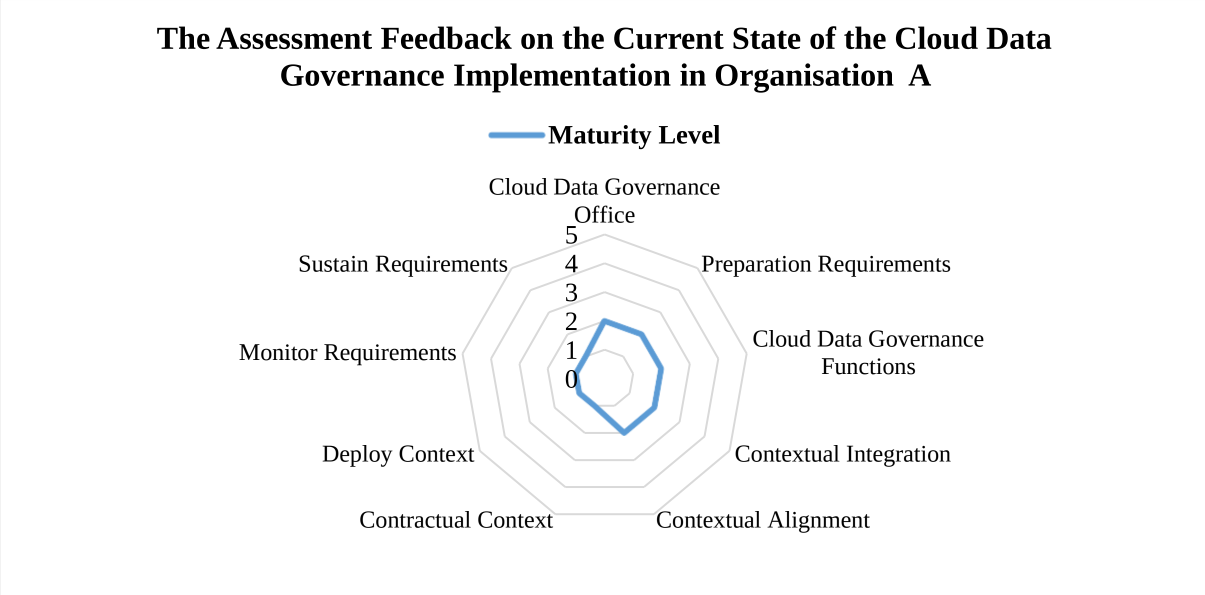

Figure 7.26 The current state of cloud data governance implementation in organisation A

- **Analysis of the Target Level of Cloud Data Governance in Organisation A using MARS-CDG Tool**

The same IT manager was asked to determine the near-future target level for cloud data governance in the organisation, using the target utility of the tool. Table 7.5 shows the planned target levels and the overall target level of the cloud data governance in organisation A, as specified by the IT manager.

Table 7.5 The target level of cloud data governance in organisation A

Cloud Data Governance Dimensions	Maturity Target Level	Overall Target Level
Cloud Data Governance Office	Level 3	***Level 3***
Preparation Requirements	Level 5	
Cloud Data Governance Functions	Level 3	
Contextual Integration	Level 4	
Contextual Alignment	Level 3	
Contractual Context	Level 3	
Deploy Context	Level 3	
Monitor Requirements	Level 3	
Sustain Requirements	Level 2	

The results show that the target level of cloud data governance implementation in this organisation was level 3. Figure 7.27 shows a comparison between the current level of cloud data governance in organisation A and its target level.

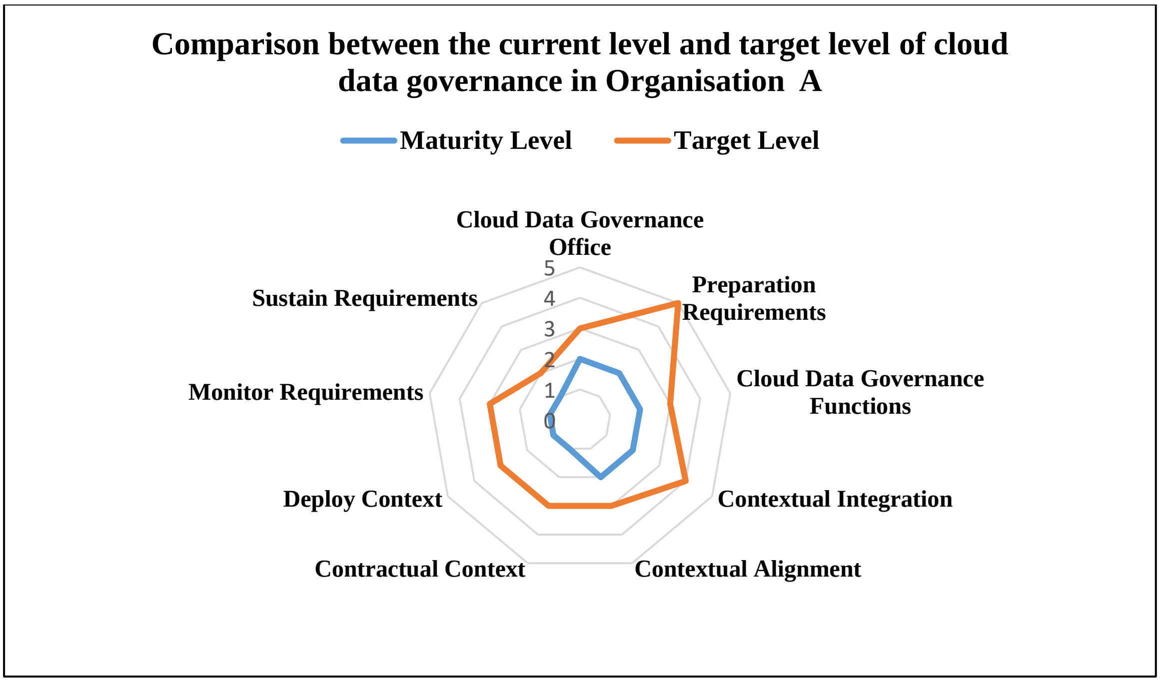

Figure 7.27 The comparison between the current level of cloud data governance and its target level in organisation A

7.7.4. Case Scenario Two: Organisation B

The second case scenario comprises an organisation that is part of the healthcare sector with around 2300 employees. According to the questionnaire results, organisation B has been adopting some cloud computing services, and it is planning to expand these in the near future. The IT department team is responsible for managing the organisation's data, and the network and information security section is part of the IT department. The network and information security section is doing some technical and practical work regarding information security policies. In this study, the head of the network and information security section was involved in this evaluation. In the interview session, the participant reported that the organisation does not have a formal strategy in place to implement data governance in general or for cloud computing in particular. With regard to benchmarking, measuring and assessing data governance implementation in the organisation, the participant reported that they use KPIs to measure the implementation of information security aspects. In addition, the participant also reported that the organisation does not consider the cloud data governance programme in its budget. Finally, the head of network and information security in this organisation used the web tool to evaluate the cloud data governance initiatives of organisation B. The results are as follows:

- **Analysis the Current Level of the Cloud Data Governance in Organisation B using MARS-CDG Tool**

To assess the current state of the cloud data governance implementation, the head of network and information security at organisation B was requested to address all the statements represented by all the defined sub-dimensions, depending on which maturity level was calculated. Table 7.6 shows the dimension levels and the overall level of cloud data governance in organisation B.

Table 7.6 The overall level of cloud data governance in organisation B

Cloud Data Governance Dimensions	Maturity Level	Overall Level
Cloud Data Governance Office	Level 2	***Level 2***
Preparation Requirements	Level 2	
Cloud Data Governance Functions	Level 2	
Contextual Integration	Level 2	
Contextual Alignment	Level 2	
Contractual Context	Level 1	
Deploy Context	Level 2	
Monitor Requirements	Level 1	
Sustain Requirements	Level 1	

Table 7.6 shows the maturity level of each dimension of cloud data governance in organisation B. The results show that the cloud data governance implementation in this organisation was at level 2, which is weak and informal, and requires some serious attention. It was interesting for this organisation to recognise the importance of data governance for their cloud provision; there was already some evidence of this as their network and information security team seem to deal with some aspects of data governance, but do so in an ad-hoc way. Figure 7.28 shows the current state of cloud data governance implementation in organisation B, based on their assessment.

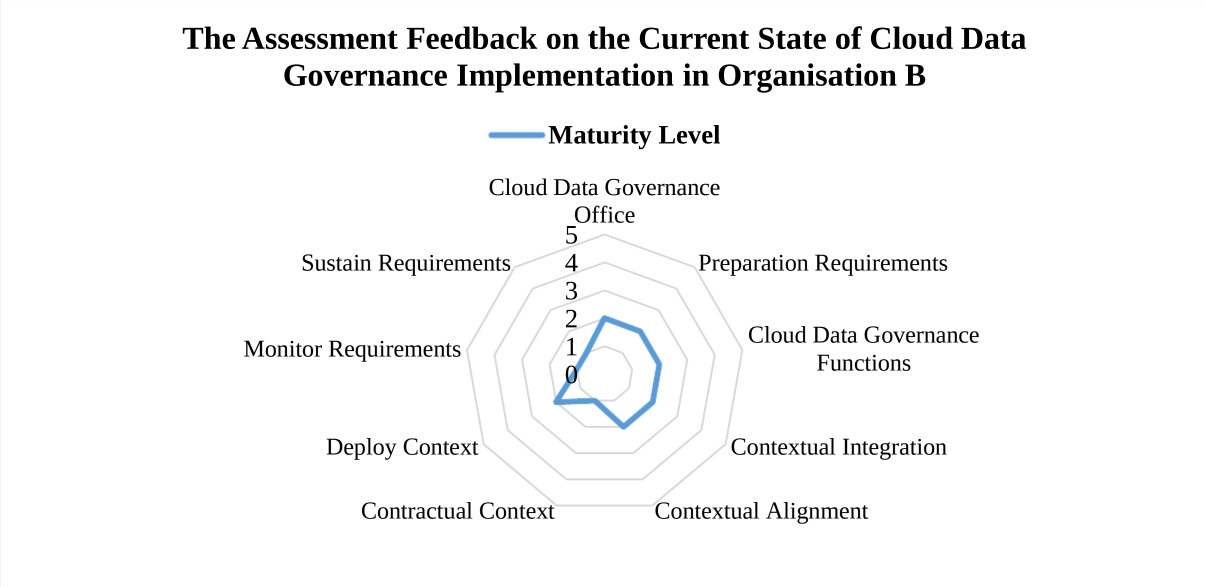

Figure 7.28 The current state of cloud data governance implementation in organisation B

- **Analysis of the Target Level of Cloud Data Governance in Organisation B using MARS-CDG Tool**

The same head of network and information security manager was asked to determine the near-future target level of cloud data governance in the organisation, using the target utility of the tool. Table 7.7 shows the planned target levels and the overall target level of the cloud data governance in organisation B, as specified by the head of network and information security manager.

Table 7.7 The target level of cloud data governance in organisation B

Cloud Data Governance Dimensions	Maturity Target Level	Overall Target Level
Cloud Data Governance Office	Level 4	***Level 3***
Preparation Requirements	Level 5	
Cloud Data Governance Functions	Level 4	
Contextual Integration	Level 3	
Contextual Alignment	Level 3	
Contractual Context	Level 4	
Deploy Context	Level 3	
Monitor Requirements	Level 3	
Sustain Requirements	Level 3	

The results show that the target level of cloud data governance implementation in this organisation was level 3. Figure 7.29 shows the comparison between the current level of cloud data governance in organisation B and its target level.

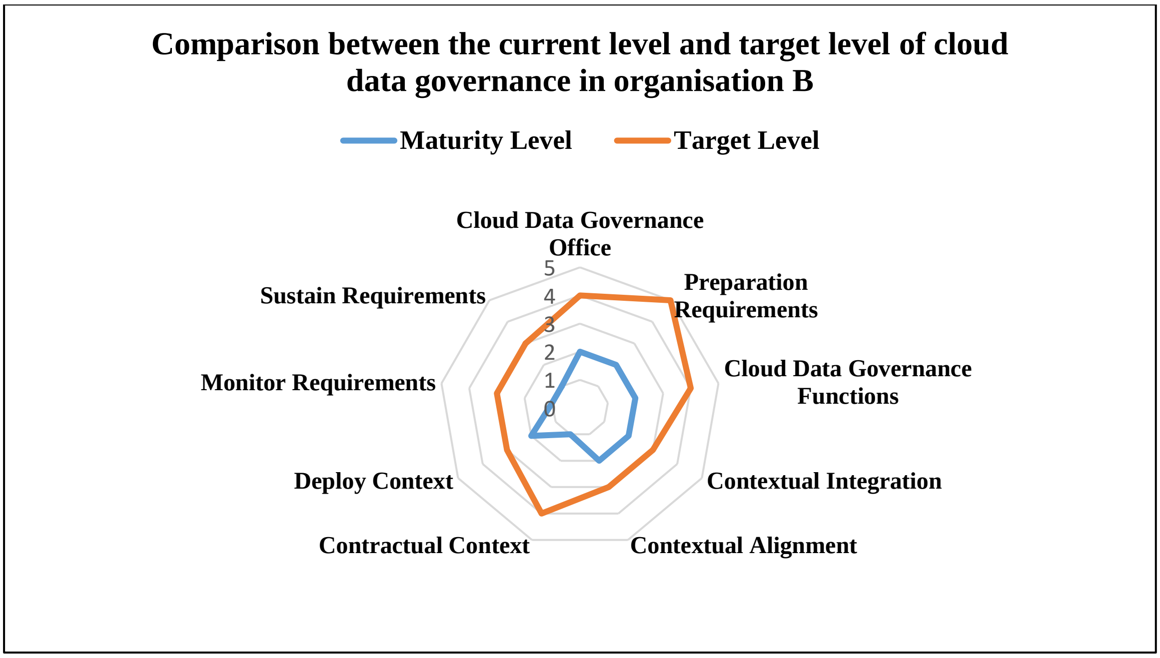

Figure 7.29 The comparison between the current level of cloud data governance in organisation B and its target level

7.8. Chapter Summary

This chapter has discussed the results of the cloud data governance maturity model and the assessment matrix validation through a focus group approach. The findings from the focus group were highlighted as being in support of the proposed concept and structure of the proposed maturity model and assessment matrix. Comments made during the validation process have been considered and captured by amending the original diagram of the maturity model. The assessment matrix contents have also been modified based on the participants' feedback. Additionally, the MARS-CDG tool was developed to evaluate the state of cloud data governance implementation in organisations. Two case scenarios were used to examine the practicality of using the proposed cloud data governance framework, maturity model and assessment matrix in a real-life environment. The next chapter presents the research conclusion and recommendations of this thesis.

Chapter 8. Research Conclusions and Recommendations

8.1. Introduction

This Chapter presents a summary of the research process and findings of this thesis, by first a research overview; second, a summary of research findings and contribution to knowledge, fellow by research limitations and finally, recommendations for future research directions.

8.2. Research Overview

In today's cloud computing is one of the most popular technological trends. Despite the numerous benefits of cloud computing, it is still not widely adopted by public sectors in many countries, due to a number of many issues and challenges. Central to these concerns is the loss of control on data, security and privacy of data, data quality and assurance, data stewardship, which are all attributes data governance. Therefore, in this thesis, the Cloud computing model is discussed as a highly disruptive technology, which requires extremely rigorous data governance strategy and programme, which can be more complex but necessary. However, in the literature there are very few studies reported on data governance for cloud services, despite its significance importance.

The purpose of this research was to develop a strategy framework that could be used to design, deploy and sustain an effective cloud data governance programme; it also aimed to advance research in this field, which will contribute to the wider Information Systems' research community and practitioners, with a particular focus on the Saudi Public Sector. To fulfil the research objectives, listed in Chapter One, a mixed research methodology was adopted, varying between Quantitative and Qualitative methods, involving the analysis of relevant literature using a Systematic approach, Questionnaires, Focus Groups and Case Studies. These combined with the adopted underpinning theoretical basis and tools, have all supported a rigorous research process that resulted in solid findings, meeting all the thesis' objectives. The next section presents a summary of the research findings and contribution to knowledge. There are three fundamental directions that underpin this research and its contributions

1. Thesis aims at addressing the cloud data governance challenge for the Saudi Public Sector, however, since this an unprecedented work, and there is no one size that fits all, it is important first to develop a Strategy Framework for cloud data governance in

order to understand the core phases and components and for enabling the implementation of effective cloud data governance programme.

2. In order to support organisations implement their cloud data governance programme, based on the developed Strategy Framework, there is a need for tools that enable them to assess their current state and define their targets. A Maturity Model was proposed together with an assessment matrix.
3. The above were all developed based Systematic Literature Reviews and underpinning theories and concepts, mainly involving the Analytic Theory and the Critical Success Factors (CSFs); thus, the results could be generalized, however, this Thesis aims at addressing the cloud data governance challenge for the Saudi Public Sector, there is a need to validate and/or evaluate the developed Framework, Maturity Model and Assessment Matrix by the concerned beneficiaries of this thesis.

8.3. Summary of the Research Contributions and Findings

This research has produced a number of findings and contributions to knowledge; the major findings and contributions to knowledge in this thesis include the following:

1. Identifying the research gaps and the significance of the defined scope of the research. By addressing the research gap in the literature a critical evaluation of the state of the art of data governance in non-cloud and, more specifically, in cloud computing was considered. The outcomes have led the researcher in this thesis to propose novel contributions in the area of data governance and more specifically of cloud data governance. The impact of the results from the study could be significant for the research community and practitioners in different countries. This is justified by the lack of research and development and practice on cloud data governance.

2. A critical evaluation of the state of the art of data governance in non-cloud and, more specifically, in cloud computing, including the identification of Critical Success Factors (CSFs) and Barriers to implementing effective cloud data governance programme in organisations. A systematic literature review guideline has been undertaken in this research to understand the state of the art of data governance for non-cloud and cloud computing environments. The findings showed that the research on data governance in general and on its implementation in the cloud in particular is

still in its early stages and more research efforts are required. The findings confirmed that currently there is no single approach to the implementation of data governance programmes in all organisations, the findings were presented in Chapter Two. The impact of the results from the study could be significant for organisations in different countries and more specifically in KSA. This is justified by the lack (almost no previous related work) of research and development and practice on data governance for cloud computing. The Critical Success Factors (CSFs) and Barriers to implementing effective cloud data governance programme in organisations were identified and classified based on in the literature findings, and they were presented in Chapter Two. Furthermore, based on the results findings in Chapter Two, a Cloud Data Governance Taxonomy and Key Dimensions were developed in Chapter Three to support a framework development.

3. Developed a Strategy Framework to understand how to Design, Deploy and Sustain an effective cloud data governance programme. To fill the gap identified in this study, which was related to the lack of a strategy framework to understand how to Design, Deploy and Sustain an effective cloud data governance programme. A novel strategy framework was developed in this research and it was presented in Chapter Three. The framework was developed based on an analytic theory and critical success factors concept. The novel framework can help decision makers to understand the important processes required to develop a cloud data governance programme, and help the public sector organisations to avoid loss of governance and control of their data in the cloud provider's environment. In addition, the framework was developed based on the five phases; each phase contains important factors to achieve it. The first phase in this framework helps the cloud consumers to understand the data governance situation in their organisations; the second phase helps the cloud consumers to design data governance activities; the third phase assists the cloud consumers and providers to understand how to implement a cloud data governance programme; the fourth phase supports the cloud consumer and other relevant actors such as the cloud auditor to evaluate and monitor the cloud data governance programme performance; and the fifth phase helps the cloud consumer and provider to improve and sustain cloud data governance programme.

4. Developed a cloud data governance Maturity Model. To fill the gap identified in this study that was related to the lack of a maturity model for cloud data governance. A cloud data governance maturity model was developed in this research, and it was presented in Chapter Four. A cloud data governance maturity model was developed based on dimensions of the cloud data governance framework in Chapter Three, and maturity levels. These levels range from one to five, where one is a lack of maturity and five is fully mature. In addition, this model will contribute to help organisations understand their current position for cloud data governance implementation and identify their future path. This contribution will be achieved by classifying components of the cloud data governance framework dimensions based on the five maturity levels.

5. Developed a cloud data governance Assessment Matrix. Developed a cloud data governance Assessment Matrix. A cloud data governance assessment matrix was developed in this research, and it was presented in Chapter Four. In this research, the cloud data governance assessment matrix is developed to support the cloud data governance maturity model developed as part of this thesis. The assessment matrix was developed to help organisations to identify their current state of cloud data governance, and it helps the organisation to identify its target to achieve good cloud data governance outcomes. The cloud data governance assessment matrix also aims to allow the organisation to understand the strength and weakness of its cloud data governance, and provide guidelines to improve its cloud data governance. Therefore, this research adopted this mechanism, which was used to determine the best and worst practices, and then to determine the characteristics of all the levels in between. Furthermore, the assessment matrix was constructed with five levels and nine core categories (dimensions) were added as cross-reference categories for the five levels. In addition, four prefix terms were used to formulate the text descriptions for each level in the assessment matrix in order to determine the difference between the levels: Does not exist, Informal, Semi-formal and Formal.

6. Developed and tested a Tool to facilitate the assessment activity. Developed and tested a Tool to facilitate the assessment activity. A tool was developed in chapter Seven to conducting practical evaluation of the assessment matrix. The tool was implemented using Python as a programming language, with Python Libraries Flask,

Jinja2, and SQLAlchemy. Furthermore, SQLite was used as a database engine in the tool development. This tool is hereafter called the maturity assessment & recommendation system of cloud data governance (MARS-CDG). It aims to help the decision makers to assess the maturity of the cloud data governance in the organisations, and to support the organisations using the cloud data governance framework to build their cloud data governance programme. The tool is a valuable tool for providing quick results for decision makers to take the right decision to improve their cloud data governance programme. In addition, the tool in this research was developed to be more practical by allowing the organisations to assess their cloud data governance programme based on their situation, and it presents the overall current state of the cloud data governance, and current state of each dimension and sub-dimensions for the cloud data governance. The strengths and weaknesses of each dimension and sub-dimension of the cloud data governance are also reported by this tool. Furthermore, this tool also allows the organisations to identify the overall target for the cloud data governance and for each dimension based on their requirements.

7. Validated and evaluated the research outcomes (1-6 above) for the Case Study of this Thesis. This research was used a case study in Saudi Arabia to investigating the state of cloud computing adoption and cloud data governance implementation in the public sector organisations in Saudi Arabia, and to validate and evaluate the proposed framework, maturity model and assessment matrix for the cloud data governance. The steps to validate and evaluate the research outcomes as summarised below:
    - Regarding investigating the state of cloud computing adoption and cloud data governance implementation, the questionnaire method was used to investigate the current state of cloud computing and cloud data governance in public sector organisations in Saudi Arabia. In addition, the critical success factors (CSFs) and barriers to implementing cloud data governance identified from the literature were considered in this survey to understand their situation in Saudi Arabia. the findings were presented in Chapter Five.
    - In order to validate and evaluate the proposed framework in Chapter Three, a focus group approach was adopted to validate the proposed framework, the focus group comprised for our case study involved ten (10) participants from government organisations and cloud providers. The findings showed that there

is an agreement between participants on the importance of the proposed framework to develop the cloud data governance programme. In addition, they contributed to this research by adding important recommendation to improve and change the proposed framework, and these recommendations and changes were made to the framework, the validation findings were presented in chapter Six. On the other hand, the framework was evaluated by the Structural Equation Modelling (SEM) technique, the evaluation findings were presented in chapter Six. A SEM was used to evaluate and assess the research framework and to test the research hypotheses based on the questionnaire findings. The findings confirmed that all hypotheses support the framework structure and it has achieved an acceptable.

- Regarding to evaluate the proposed maturity model and an assessment matrix in Chapter Four, a focus group approach was adopted to evaluate the proposed maturity model and an assessment matrix based on some criteria, the focus group comprised for our case study involved ten (10) participants from government organisations, cloud providers, and academia. The findings showed that there is an agreement between participants on the importance of the proposed maturity model and an assessment matrix to assess the cloud data governance programme. In addition, they contributed to this research by adding important recommendation to improve and change the proposed maturity model and an assessment matrix, and these recommendations and changes were made to the maturity model and assessment matrix, the evaluation findings were presented in chapter Seven. On the other hand, maturity assessment & recommendation system of cloud data governance (MARS-CDG) was used to examine the practicality of using the cloud data governance framework in a real-life environment based on two case scenarios were used. The case scenario considered two public sector organisations in Saudi Arabia, which were adopting some cloud computing services. These organisations belong to healthcare and the military sectors, respectively. The findings showed that the cloud data governance implementation in these case scenarios is still in its early stages and more efforts are required, the findings were presented in chapter Seven.

8.4. Research Limitations

Although the Thesis has fulfilled all research objectives, the author recognises some limitations, which could be addressed in future work.

Considering, this research is the first study to tackle cloud data governance at this scale. Although the lack of prior studies has been an advantage in developing a highly novel research, it can also be considered as a limitation. The research findings could be further enriched with a richer literature. A richer literature can mean more established methods, theories, models and frameworks, etc., which would have supported the research directions for this thesis. The lack of literature also means the absence of a relevant research community, the interaction with whom would have been very useful the development of this thesis. On the other hand, the lack of prior studies, has given the Author the opportunity to establish some important foundations in the field of cloud data governance with invaluable contribution to knowledge.

Another limitation is related to the research methodology, particularly, for the validation part of the thesis. This is a known limitation in all research projects, which employ Focus Groups and questionnaires, which is related to the bias in the participants's responses and the sample population. In this thesis, the sample population was adequate for the scale of the project and involved balanced representations from most important Saudi public sector's organisations, as cloud consumers; private sector as cloud providers and from academia. However, a bigger population size with a bigger or full representation of the relevant stakeholders would always strengthen the research findings. Another issue was the related to the participants' contribution to the study, which is linked with the lack of the prior studies; that is their lack of knowledge in the field, despite their senior positions as IT Managers and Directors. To minimise inaccuracy in data analysis at the same time minimise any possible influence on the responses, the Author supplied the participants with the right background that explains the context of investigation. The limitation of the lack of knowledge have also taken the participants outside their comfort zone, which was valuable for the research analysis. The other limitation of this study is related to the time and resource constraints: this study had to be completed within a reasonable timeframe allocated for PhD research. If more time was allocated for the empirical work, the level of detail obtained, particularly from the case study, would have been greater and of a wider scope.

8.5. Recommendations for Further Research

Cloud data governance is a comparatively new phenomenon and this research serves as a starting point for further research into this area, and many opportunities and interest areas have been discovered and are worth future study. These are as follows:

1. Extend the validation of the research findings, in this thesis, to all public sector orgsanisations in Saudi Arabia as well as the Private Sector.
2. Investigate how to embed the research findings of this thesis in the Saudi Vision 2030 for digital transformation.
3. Investigate cloud data governance for different case studies of different countries, which will allow opportunities for comparison between these countries, and adoption of best practices.
4. Further research could focus on a real case of implementation of a cloud data governance programme derived from the proposed strategy framework. This will require the development of adequate tools to help in the process.
5. Exploit the research findings of this thesis in developing new Standards for cloud data governance, which can be implemented in organisations and be auditable.
6. Each phase or component of the developed Framework, in this thesis, could be a standalone research project, which allows for depth, e.g. Cloud data governance programme for security.
7. The proposed tool for assessment (MARS-CDG) has a huge potential, that it can be extended to be an intelligent and automated recommendation system for customised cloud data governance programmes, based on an organisation specific requirements.
8. Investigate the inclusion of data governance, as a standard requirement in Service Level Agreements (SLAs), and develop means to monitor any violations.
9. The convergence of the Internet of Things (IoT) with the cloud has been a subject of research interest. Evidence suggests that such a convergence carries huge potential, albeit with some challenges, too. There is a consensus that privacy, security and governance are key concerns. One central issue is the lack of mature governance and security standards for data within IoT & cloud converged environment. This opens doors to important research opportunities to tackle the challenge of cloud data governance as part of an IoT ecosystem.

References

(HIMSS), the H.I. and M.S.S. (2015). *A ROADMAP TO EFFECTIVE DATA GOVERNANCE : How to Navigate Five Common Obstacles*. [Online]. Available from: http://www.himss.org/roadmap-effective-data-governance-how-navigate-five-common-obstacles.

Abu-Tapanjeh, A.M. (2009). Corporate governance from the Islamic perspective: A comparative analysis with OECD principles. *Critical Perspectives on Accounting*. 20 (5). p.pp. 556–567.

Abu Musa, A. (2009). Exploring COBIT Processes for ITG in Saudi Organizations An empirical Study. *The International Journal of Digital Accounting Research*. 9 (1). p.pp. 99–126.

Adelman, S. (2008). Without a Data Governance Strategy. *DM Review*. [Online]. 18 (1). p.p. 32. Available from: citeulike-article-id:6015242%5Cnhttp://proquest.umi.com/pqdweb?index=17&#38%5Cndid=1437995401&#38%5CnSrchMode=1&#38%5Cnsid=1&#38%5CnFmt=3&#38%5CnVInst=PROD&#38%5CnVType=PQD&#38%5CnRQT=309&#38%5CnVName=PQD&#38%5CnTS=1256648869&#38%5CnclientId=23406.

Adler, S. (2007). *The IBM Data Governance Council Maturity Model : Building a roadmap for effective data governance*. [Online]. Available from: https://www-935.ibm.com/services/uk/cio/pdf/leverage_wp_data_gov_council_maturity_model.pdf.

Akin, O.C. (2014). The Impact and Challenges of Cloud Computing Adoption on Public Universities in Southwestern Nigeria. *IJACSA) International Journal of Advanced Computer Science and Applications*. 5 (8). p.pp. 13–19.

Al-shehry, A.M. (2009). *Transformation towards e-government in The Kingdom of Saudi Arabia: technological and organisational perspectives*. [Online]. De Montfort University. Available from: http://hdl.handle.net/2086/2418.

Albright, J.J. (2008). *Confirmatory Factor Analysis using Amos ,*. [Online]. USA. Available from: http://www.iub.edu/~statmath/stat/all/cfa/cfa2008.pdf.

Alexandria, V. (2014). *Despite Data Governance Efforts, Eighty-Nine Percent of Federal IT Professionals Are Apprehensive About Migrating IT Services to the Cloud*. [Online]. 2014. Available from: http://www.businesswire.com/news/home/20140909005167/en/Data-Governance-Efforts-Eighty-Nine-Percent-Federal-Professionals#.VeV27Jrovcc. [Accessed: 12 July 2016].

Alhammadi, A. (2013). *A Knowledge Management Migration Model and a Framework to Support Cloud Computing Migration*.

Alharbi, F., Atkins, A. & Stanier, C. (2016). Understanding the determinants of Cloud Computing adoption in Saudi healthcare organisations. *Complex & Intelligent Systems*. [Online]. p.pp. 1–17. Available from: http://link.springer.com/10.1007/s40747-016-0021-9.

Alhassan, I., Sammon, D. & Daly, M. (2016). Data governance activities: an analysis of the literature. *Journal of Decision Systems*. [Online]. 25 (S1). p.pp. 64–75. Available from: http://dx.doi.org/10.1080/12460125.2016.1187397.

Alkhater, N., Wills, G. & Walters, R. (2014). Factors Influencing an Organisation's Intention to Adopt Cloud Computing in Saudi Arabia. In: *IEEE 6th International Conference on Cloud Computing Technology and Science*. [Online]. 2014, pp. 1040–1044. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7037803.

Allen, C., Des Jardins, T.R., Heider, A., Lyman, K.A., McWilliams, L., Rein, A.L., Schachter, A.A., Singh, R., Sorondo, B., Topper, J. & Turske, S.A. (2014). Data governance and data sharing agreements for community-wide health information exchange: lessons from the beacon communities. *EGEMS (Washington, DC)*. [Online]. 2 (1). p.p. 1057. Available from: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=4371395&tool=pmcentrez&rendertype=abstract.

Almarabeh, T., Majdalawi, Y.K. & Mohammad, H. (2016). Cloud Computing of E-Government. *Communications and Network*. 8 (February). p.pp. 1–8.

Alsanea, M. (2015). *Factors Affecting the Adoption of Cloud Computing in Saudi Arabia?s Government Sector Theises*. Goldsmiths, University of London.

Alshehri, M.A. (2012). *Using the UTAUT Model to Determine Factors Affecting Acceptance and Use of E-government Services in the Kingdom of Saudi Arabia*. Griffith University.

Amberg, M., Fischl, F. & Wiener, M. (2005). *Background of critical success factor research*. [Online]. Available from: http://www.international-outsourcing.de/CSF-Tool/docs/WorkingPaper_BackgroundCSF_Ambergetal._FINAL.pdf.

Apostu, A., Puican, F., Ularu, G., Suciu, G. & Todoran, G. (2013). Study on Advantages and Disadvantages of Cloud Computing - the Advantages of Telemetry Applications in the Cloud. *Recent Advances in Applied Computer Science and Digital Services*. p.pp. 118–123.

Arturo, C. & Alvarez, M. (2011). *Cloud Computing : Concerns and challenges for its adoption in SMEs and large companies in Japan*. Ritsumeikan Asia-Pacific University.

Ataya, G. (2013). Information Security , Risk Governance and Management Frameworks . An Overview of COBIT 5. In: *SIN '13: Proceedings of the 6th International Conference on Security of Information and Networks*. 2013, pp. 3–5.

Australian Institute of Health and Welfare (2014). *AIHW data governance framework 2014 (AIHW)*. [Online]. Available from: http://www.aihw.gov.au/WorkArea/DownloadAsset.aspx?id=60129548881.

Badger, L., Grance, T., Patt Corner, R. & Voas, J. (2011). Cloud Computing Synopsis and Recommendations. *NIST Special Publication*. [Online]. 800 p.p. 84. Available from: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf.

Badrakhan, B.B. (2010). Drive Toward Data Governance. *Ewweb*. (August 2010). p.pp. 35–38.

Barnes, E., Howells, E.P., Marshall, K., Bullock, A., Cowpe, J. & Thomas, H. (2012). Development of the Maturity Matrix Dentistry (MMD): a primary care dental team development tool. *Bdj*. [Online]. 212 (12). p.pp. 583–587. Available from: http://www.nature.com/doifinder/10.1038/sj.bdj.2012.523.

Bauer, J.M. (2005). Internet Governance: Theory and First Principles. *Preliminary draft, August*. [Online]. 31 (March). p.pp. 1–20. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.113.519&rep=rep1&type=pdf.

Beck, C.T. (1994). Reliability and validity issues in phenomenological research. *Western journal of nursing research*. [Online]. 16 (3). p.pp. 254-62–7. Available from: http://www.ncbi.nlm.nih.gov/pubmed/8036802.

Becker, Jörg, Ralf Knackstedt, and D.-W.I.J.P. (2009). Developing Maturity Models for IT Management – A Procedure Model and its Application. *Business & Information Systems Engineering*. (1.3). p.pp. 213–222.

Becker, J.D., Bailey, E. & Proceedings, A. (2014). IT Controls and Governance in Cloud Computing. In: *AMCIS Proceedings forthcoming*. 2014, pp. 1–20.

Beecham, S., Hall, T., Britton, C., Cottee, M. & Rainer, A. (2005). Using an expert panel to validate a requirements process improvement model. *Journal of Systems and Software*.

76 (3). p.pp. 251–275.
Begg, C. & Caira, T. (2012). Exploring the SME Quandary : Data Governance in Practise in the Small to Medium-Sized Enterprise Sector. *The Electronic Journal Information Systems Evaluation*. 15 (1). p.pp. 3–13.
Benfeldt, O. (2017). *A Comprehensive Review of Data Governance Literature*.
Bhansali, N. (2014). *Data Governance: Creating Value from Information Assets*. Auerbach Publications.
Blommerde, T. & Lynch, P. (2016). A Maturity Matrix for Assessing Service Innovation Capability. In: *rish Academy of Management Conference*. 2016, pp. 1–27.
Boehm, B.W. & Valerdi, R. (2008). Achievements and Challenges in COCOMO Based Software Resource Estimation. *IEEE Software*. [Online]. 25 (5). p.pp. 74–83. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4602679.
Buffenoir, E. & Bourdon, I. (2012). *Reconciling complex organizations and data management: the Panopticon paradigm*. [Online]. (October). p.p. 19. Available from: http://arxiv.org/abs/1210.6800.
Bulla, C.M., Bhojannavar, S.S. & Danawade, V.M. (2013). Cloud Computing : Research Activities and Challenges. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*. 2 (5). p.pp. 206–2014.
Bumpus, W. (2010). NIST Cloud Computing Standards Roadmap. *NIST Special Publication*. 35. p.pp. 1–3.
Burgess, T. (2001). *Guide to the Design of Questionnaires*. 1st Ed. [Online]. LEEDS. Available from: http://www.cavehill.uwi.edu/cermes/socmonpub/workshop_trainin_ resources/recommended_reading/questionnaire design and analysis/burgess_2001_survey_design.pdf.
Burney, A. (2008). Inductive and Deductive Research Approach. *Research Approach*. (March). p.p. 22.
Caralli, R., Knight, M. & Montgomery, A. (2012). *Maturity models 101: a primer for applying maturity models to smart grid security, resilience, and interoperability*. [Online]. USA. Available from: http://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_58920.pdf.
Catteddu, D., Felici, M., Hogben, G., Holcroft, A., Kosta, E., Leenes, R., Millard, C., Niezen, M., Nuñez, D., Papanikolaou, N., Pearson, S. & Pradelles, D. (2013). Towards a Model of Accountability for Cloud Computing Services Proposed Definitions of Accountability in the Cloud. In: *In Proceedings of the DIMACS/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC).* 2013, p. 10.
Catteddu, D. & Hogben, G. (2009). *The European Network and Information Security Agency (ENISA) is an EU agency created to advance This work takes place in the context of ENISA ' s Emerging and Future Risk programme . C ONTACT DETAILS : This report has been edited by*. [Online]. Available from: http://www.springerlink.com/index/R357K80TP72R7121.pdf.
Chao, L. (2012). Cloud Computing for Teaching and Learning. *Design*. [Online]. p.pp. 78–94. Available from: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-4666-0957-0.
Chawngsangpuii, R. & Das, R.K. (2014). A CHALLENGE FOR SECURITY AND SERVICE LEVEL AGREEMENT IN CLOUD COMPUTINGE. *IJRET: International Journal of Research in Engineering and Technology*. 3 (11). p.pp. 2319–2322.
Cheong, L. & Chang, V. (2007a). The Need for Data Governance: A Case Study. *ACIS 2007 Proceedings*. [Online]. (February). Available from: http://aisel.aisnet.org/acis2007/100.
Cheong, L.K. & Chang, V. (2007b). The Need for Data Governance : A Case Study. In: *ACIS*

2007 Proceedings. 2007, pp. 999–1008.
Chin, W.W. (1998). Issues and Opinion on Structural Equation Modeling. *Management Information Systems Quarterly*. 22 (1). p.pp. 1–13.
Cloud Security Alliance (2012). *Cloud Data Governance Research Sponsorship*. [Online]. Available from: https://downloads.cloudsecurityalliance.org/membership/sponsorship/CDG_Sponsorship.pdf.
Cloud Security Alliance (2015). *Cloud Data Governance Working Group*. [Online]. 2015. Available from: https://cloudsecurityalliance.org/group/cloud-data-governance/. [Accessed: 21 May 2015].
Cochran, M. & Witman, P.D. (2011a). GOVERNANCE AND SERVICE LEVEL AGREEMENT ISSUES IN A CLOUD COMPUTING ENVIRONMENT COMPUTING ENVIRONMENT. *Journal of Information Technology Management ISSN*. XXII (2). p.pp. 41–55.
Cochran, M. & Witman, P.D. (2011b). Journal of Information Technology Management A Publication of the Association of Management GOVERNANCE AND SERVICE LEVEL AGREEMENT ISSUES IN A CLOUD COMPUTING ENVIRONMENT. *Journal of Information Technology Management ISSN*. XXII (2). p.pp. 41–55.
Crowston, K. & Qin, J. (2010). A Capability Maturity Model for Scientific Data Management. *American Society for Information Science and Technology*. [Online]. 1 (July). p.pp. 1–10. Available from: http://crowston.syr.edu/system/files/CMM for DM to share.pdf.
Dahlberg, T. & Nokkala, T. (2015). a Framework for the Corporate Governance of Data - Theoretical Background and Empirical Evidence. *Business, Management & Education / Verslas, Vadyba ir Studijos*. [Online]. 13 (1). p.pp. 25–45. Available from: 10.3846/bme.2015.254%5Cnhttp://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=108616811&site=bsi-live.
Davidson, R.M. (2004). Chapter Three : Research Methodology. *City University of Hong Kong*. [Online]. p.pp. 1–20. Available from: http://www.is.cityu.edu.hk/staff/isrobert/phd/ch3.pdf.
Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information. *Information Technolog MIS Quarterly*. [Online]. 13 (3). p.p. 319–340. Available from: http://scholar.google.com/scholar?hl=en&q=davis+perceived+usefulness+perceived+ease+of+use&btnG=Search&as_sdt=2000&as_ylo=&as_vis=0#0%5Cnhttp://www.jstor.org/stable/249008.
Davis, J.R. (2011). Information Governance as a Holistic Approach to Managing and Leveraging Information Prepared for IBM Corporation. *International Journal of Information Management*. 31.
Debreceny, R.S. & Gray, G.L. (2013). IT Governance and Process Maturity: A Multinational Field Study. *Journal of Information Systems*. [Online]. 27 (1). p.pp. 157–188. Available from: http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=88181971&site=ehost-live&scope=site.
DeNardis, L. (2010). *The emerging field of Internet governance*.
Dogo, E.M., Salami, A. & Salman, S.I. (2013). Feasibility Analysis of Critical Factors Affecting Cloud Computing in Nigeria. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*. 2 (4). p.pp. 276–287.
Donaldson, A. & Walker, P. (2004). Information governance - A view from the NHS. *International Journal of Medical Informatics*. 73 (3). p.pp. 281–284.

Eckerson, W. (2011). *Creating an Enterprise Data Strategy*. [Online]. Available from: Creating an Enterprise Data Strategy.

Edelenbos, J. & Klijn, E.H. (2006). Managing stakeholder involvement in decision making: A comparative analysis of six interactive processes in the Netherlands. *Journal of Public Administration Research and Theory*. 16 (3). p.pp. 417–446.

Eugene, G. (2013). Cloud Computing Models. *MIT Engineering Systems Division*. (January).

Fan, Y., Chen, J., Shirkey, G., John, R., Wu, S.R., Park, H. & Shao, C. (2016). Applications of structural equation modeling (SEM) in ecological studies: an updated review. *Ecological Processes*. [Online]. 5 (1). p.pp. 5–19. Available from: http://ecologicalprocesses.springeropen.com/articles/10.1186/s13717-016-0063-3.

Farrell, A.M. (2010). Insufficient discriminant validity: A comment on Bove, Pervan, Beatty, and Shiu (2009). *Journal of Business Research*. 63 (3). p.pp. 324–327.

Fath-allah, A., Cheikhi, L., Al-qutaish, R.E. & Idri, A. (2014). E-Government Maturity Models: A Comparative Study. *International Journal of Software Engineering & Applications (IJSEA), May 2014*. 5 (3). p.pp. 71–91.

Felici, M., Koulouris, T. & Pearson, S. (2013). Accountability for Data Governance in Cloud Ecosystems. *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*. [Online]. p.pp. 327–332. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6735445.

Fernandes, D. a B., Soares, L.F.B., Gomes, J. V., Freire, M.M. & Inácio, P.R.M. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security*. 13. p.pp. 113–170.

Fernández, A. & Llorens, F. (2009). An IT Governance Framework for Universities in Spain. In: *EUNIS 2009 Conference*. 2009, pp. 1–13.

Fleissner, B.B., Jasti, K., Ales, J. & Thomas, R. (2014). *The Importance of Data Governance in Healthcare*. [Online]. Available from: http://encorehealthresources.com/wp-content/uploads/2014/10/The-Importance-of-Data-Governance_FINAL-Oct-2014.pdf.

Fletcher, R.H., Fletcher, S.W., Jiménez, V., Díaz De Salas, S., Mendoza, V., Porras, C., Eisenhardt, K.M., Flyvbjerg, B., Yin, R.K., Study, C., Tellis, W., Gerring, J., Zainal, Z., Dooley, L.M. & Noor, K.B.M. (2007). Case study as a research method. *Academy of Management Review*. [Online]. 5 (2). p.pp. 301–316. Available from: http://www.gslis.utexas.edu/~ssoy/usesusers/l391d1b.htm%5Cnhttp://www.sbs.ox.ac.uk/centres/bt/directory/Documents/CaseStudy4 2HBQR11PRINT.pdf%5Cnhttp://books.google.com/books?id=FzawIAdilHkC&pgis=1%5Cnhttp://scielo.iics.una.py/pdf/riics/v8n1/v8n1a09.pdf.

Fornell, C. & Larcker, D.F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*. [Online]. 18 (1). p.p. 39. Available from: http://www.jstor.org/stable/3151312?origin=crossref.

Forster, N.S. & Rockart, J.F. (1989). Critical succes factors: An annotated bibliography. *MIT Sloan Rev*. 191 (1). p.pp. 3041–3089.

Fox, J., Murray, C. & Warm, A. (2003). Conducting research using web-based questionnaires: practical, methodological, and ethical considerations. *International Journal of Social Research Methodology*. 6 (2). p.pp. 167–180.

Freitas, H., Oliveira, M., Jenkins, M. & Popjoy, O. (1998). The Focus Group, A Qualitative Research Method. *Isrc*. (10298). p.pp. 1–22.

Frick, N. (2012). Identification of Design Elements for a Maturity Model for Interorganizational Integration: a Comparative Analysis. In: *Proceedings of the 25th Bled eConference, eDependability, eProcesses and eServices for the Future*. [Online]. 2012, pp. 185–196. Available from: papers3://publication/uuid/3E9C1488-A4E1-44FC-

AB0F-99AD7DEE746E.
Fruehauf, J., Al-Khalifa, F. & Coniker, J. (2015). Using the Bolman and Deals four frames in developing data governance strategy. *Issues in Information Systems*. 16 (2). p.pp. 161–167.
Fu, X., Wojak, A., Neagu, D., Ridley, M. & Kim, T. (2011). Data governance in predictive toxicology: A review. *Journal of Cheminformatics*. [Online]. 3 (1). p.p. 24. Available from: http://www.jcheminf.com/content/3/1/24.
Galán, A. et al. (2017). Maturity Matrix Assessment: evaluation of energy efficiency strategies in Brussels historic residential stock. *Energy Procedia*. [Online]. 111 (1). p.pp. 407–416. Available from: http://dx.doi.org/10.1016/j.egypro.2017.03.202.
Gates, L.P. (2010). Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework. *Software Engineering Institute*. 11 (November). p.p. 67.
General Authority for Statistics, K. (2017). *Population and Vital Statistics*. [Online]. 2017. Available from: https://www.stats.gov.sa. [Accessed: 13 September 2017].
Gheorghe, M. (2011). Risk Management in IT Governance Framework. *Seria Management*. 14 (2). p.pp. 545–552.
Gicheru, E. (2013). The Psychology of Unmarried Men in Nairobi : A Case Study of Three Bachelors Over Forty. *African Journal of History and Culture*. 5 (6). p.pp. 126–137.
Goldkuhl, G. (2004). Meanings of Pragmatism : Ways to conduct information systems research. In: *International Business*. [Online]. 2004, pp. 17–18. Available from: http://www.vits.org/publikationer/dokument/457.pdf.
Goyal, R. & Sidhu, N. (2014). *Third Party Auditor : An Integrity Checking Technique for Client Data Security in Cloud Computing*. 5 (3). p.pp. 4526–4530.
Goyal, S. (2014). Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. *International Journal of Computer Network and Information Security*. [Online]. 6 (February). p.pp. 20–29. Available from: http://www.mecs-press.org/ijcnis/ijcnis-v6-n3/v6n3-3.html.
Gregor, S. (2002). *A Theory of Theories in Information Systems*. Canberra.
Gregor, S. (2006). The nature of theory in Information Systems. *MIS Quarterly: Management Information Systems*. [Online]. 30 (3). p.pp. 611–642. Available from: http://heim.ifi.uio.no/~petterog/Kurs/INF5220/NatureofTheoryMISQ.pdf%5Cnhttp://www.scopus.com/inward/record.url?eid=2-s2.0-33846102423&partnerID=40&md5=e999cc9b09812ffe3192acf4b90d3e96.
Groß, S. & Schill, A. (2012). Towards user centric data governance and control in the cloud. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 7039 LNCS. p.pp. 132–144.
Guillory, K. (2008). *The 4 Reasons Data Governance Fails*. [Online]. Available from: http://www.noah-consulting.com/experience/papers/4 Reasons Data Governance Fails - Guillory.pdf.
Guo, B., Aveyard, P., Fielding, A. & Sutton, S. (2008). Testing the convergent and discriminant validity of the Decisional Balance Scale of the Transtheoretical Model using the Multi-Trait Multi-Method approach. *Psychology of addictive behaviors : journal of the Society of Psychologists in Addictive Behaviors*. 22 (2). p.pp. 288–294.
Hair, J.F., Black, W.C., Babin, B.J. & Anderson, R.E. (2010). *Multivariate Data Analysis*. Seventh Ed. USA: Upper Saddle River, NJ: Prentice hall.
Hallikas, J. (2015). *Data governance and automated marketing - a case study of expected benefits of organizing data governance in an ICT company*.
Hamel, F. & Herz, T. (2013). IT evaluation in business groups: a maturity model. In: *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. [Online].

2013, pp. 1410–1417. Available from: http://dl.acm.org/citation.cfm?id=2480627.
Harkness, J. a & Schoua-Glusberg, A. (1998). Questionnaires in Translation. *ZUMA-Nachrichten Spezial*. [Online]. (1). p.pp. 87–126. Available from: http://isites.harvard.edu/fs/docs/icb.topic506406.files/znspez3_04_Harkness_Glusberg.pdf.
Helgesson, Y.Y.L., H??st, M. & Weyns, K. (2012). A review of methods for evaluation of maturity models for process improvement. *Journal of software: Evolution and Process*. 24 (4). p.pp. 436–454.
Henseler, J., Ringle, C.M. & Sarstedt, M. (2014). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*. 43 (1). p.pp. 115–135.
Héroux, S. & Fortin, A. (2016). The influence of IT governance, IT competence and IT-business alignment on innovation. *Canadian Academic Accounting Association*. p.pp. 1–36.
De Hert, P. & Papakonstantinou, V. (2013). Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? *I/S: A Journal of Law and Policy for the Information Society*. 9:2. p.pp. 272–324.
Hilton, A. (2006). *Enron and World Finance: A Case Study in Ethics*. [Online]. Available from: http://search.proquest.com/docview/231729629?accountid=14549%5Cnhttp://hl5yy6xn2p.search.serialssolutions.com/?genre=article&sid=ProQ:&atitle=Enron+and+World+Finance:+A+Case+Study+in+Ethics&title=Financial+World&issn=14656078&date=2006-04-01&volume=&issue.
Hox, J.J. & Bechger, T.M. (2007). An introduction to Structural Equation Modeling. *A Multidisciplinary Journal*. 16 (3). p.pp. 556–560.
Hoying, M. (2011). *Data Governance at Stanford: A Data Governance Overview*. [Online]. Stanford, California. Available from: https://web.stanford.edu/dept/pres-provost/cgi-bin/dg/wordpress/wp-content/uploads/2011/11/DG-News002.pdf.
Hsu, W.L. (2012). Conceptual Framework of Cloud Computing Governance Model – An Education Perspective. *IEEE Technology and Engineering Education*. 7 (2). p.pp. 12–16.
Huang, J. & Nicol, D.M. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*. [Online]. 2. p.p. 9. Available from: http://www.journalofcloudcomputing.com/content/2/1/9.
Hunter, L. (2015). *Tools for Cloud Accountability: A4Cloud Tutorial*. [Online]. 2015. Available from: http://www.a4cloud.eu/node/362. [Accessed: 4 November 2015].
Huth, A. & Cebule, J. (2014). *The Basics of Cloud Computing*. [Online]. USA. Available from: http://www.sciencedirect.com/science/article/pii/B9780124059320000074.
Ibm (2007). *The IBM data governance blueprint : Leveraging best practices and proven technologies*. (May).
Imhanwa, S., Greenhill, A. & Owrak, A. (2013). Designing Data Governance Structure: An Organizational Perspective. *GSTF Journal on Computing*. 2 (4). p.pp. 1–10.
ISACA.org (2016). *ISACA*. [Online]. 2016. Available from: https://www.isaca.org/Pages/default.aspx. [Accessed: 23 March 2016].
Jansen, W. & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. *Nist Special Publication*. [Online]. 144. p.pp. 800–144. Available from: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.
Järvinen, P. (2008). On developing and evaluating of the literature review On developing and evaluating of the literature review. *The 31st Information Systems Research Seminar in*

Scandinavia Workshop 3. [Online]. Available from: http://www.cs.uta.fi/reports/dsarja/D-2008-10.pdf.

Javier Salido (2010). Data Governance for Privacy, Confidentiality and Compliance: A Holistic Approach. *ISACA JOURNAL*. 6. p.pp. 1–7.

Joint, A. & Baker, E. (2011). Knowing the past to understand the present. *Computer Law and Security Review*. [Online]. 27 (4). p.pp. 407–415. Available from: http://dx.doi.org/10.1016/j.clsr.2011.05.002.

Jones, S., Irani, Z., Sivarajah, U. & Love, P.E.D. (2017). Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. *Information Systems Frontiers*. p.pp. 1–24.

Joy Medved, SSBB,IQCP, A. (2014). *Data Governance: The Four Critical Success Factors*. [Online]. San Diego,CA USA. Available from: http://www.slideshare.net/Dataversity/enterprise-data-world-data-governance-the-four-critical-success-factors-42859742.

Kamioka, T., Luo, X. & Tapanainen, T. (2017). An Empirical Investigation of Data Governance: the Role of Accountabilities. In: *the 20th Pacific Asia Conference on Information Systems (PACIS)*. 2017, pp. 1–12.

Kennedy et al. (2005). VERIFICATION AND VALIDATION OF SCIENTIFIC AND ECONOMIC MODELS. In: *Agent 2005 Conference Proceedings. Chicago, IL, October 2005*. 2005, pp. 1–15.

Khajeh-Hosseini, A., Sommerville, I. & Sriram, I. (2010). Research Challenges for Enterprise Cloud Computing. *arXiv preprint arXiv*. [Online]. 1001 (3257). p.pp. 1–11. Available from: http://arxiv.org/abs/1001.3257.

Khalil, I., Khreishah, A. & Azeem, M. (2014). Cloud Computing Security: A Survey. *Computers*. [Online]. 3. p.pp. 1–35. Available from: http://www.mdpi.com/2073-431X/3/1/1/.

Kim, S.-H. & Lee, I.-Y. (2015). Study on User Authority Management for Safe Data Protection in Cloud Computing Environments. *Symmetry*. [Online]. 7 (1). p.pp. 269–283. Available from: http://www.mdpi.com/2073-8994/7/1/269/.

Kitchenham, B. & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. *Engineering*. 2 (1). p.pp. 1–44.

Kizlik, B. (2012). *Measurement , Assessment , and Evaluation in Education*. [Online]. Available from: http://www.adprima.com/measurement.htm.

Ko, R.K.L., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q. & Lee, B.S. (2011). TrustCloud: A framework for accountability and trust in cloud computing. *Proceedings - 2011 IEEE World Congress on Services, SERVICES 2011*. p.pp. 584–588.

Kolberg, M. & Magill, E.H. (2002). A pragmatic approach to service interaction filtering between call control services. *Computer Networks*. 38 (5). p.pp. 591–602.

Koltay, T. (2016). Data governance, data literacy and the management of data quality. *IFLA Journal*. [Online]. 42 (4). p.pp. 303–312. Available from: http://ifl.sagepub.com/cgi/doi/10.1177/0340035216672238.

Kooper, M.N., Maes, R. & Lindgreen, E.E.O.R. (2011). On the governance of information: Introducing a new concept of governance to support the management of information. *International Journal of Information Management*. [Online]. 31 (3). p.pp. 195–200. Available from: http://linkinghub.elsevier.com/retrieve/pii/S0268401210000708.

Kshetri, N. (2012). Cloud computing in developing economies. *IEEE Computer*. [Online]. 43 (1). p.pp. 47–55. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2015387.

Kunzinger, F., Corporation, H., Haines, P., Consulting, N., Schneider, S. & Solutions, V. (2010). *Delivering a Data Governance Strategy that Meets Business Objectives*.

[Online]. Available from: http://www.noah-consulting.com/experience/papers/Delivering DG Strategy.pdf.
Kurdi, R.F. (2013). *An Investigation of Readiness Assessments For E-government Information System and Cloud Computing Using Saudi Arabia as a Case Study*. (November).
Ladley, J. (2012). *Data Governance Program*. 1st Ed. R. Day (ed.). New York: Elsevier Inc.
Lee, S.U., Zhu, L., Jeffery, R. & Group, A.P. (2017). Data Governance for Platform Ecosystems : Critical Factors and the State of Practice. *arXiv preprint*. (arXiv:1705.03509).
Loshin, D. (2010). *Operationalizing Data Governance through Data Policy Management*. [Online]. Available from: http://dataqualitybook.com/kii-content/OperationalizingDataGovernance.pdf.
Loshion, D. (2007). *Data Governance for Master Data Management*. [Online]. USA. Available from: https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/data-governance-for-MDM-and-beyond-105979.pdf.
Lui, F. (2011). *NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and*. [Online]. Available from: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:NIST+Cloud+Computing+Reference+Architecture+Recommendations+of+the+National+Institute+of+Standards+and#1.
Maaref, M.S. (2012). *Cloud computing in Africa - Situation and perspectives*. [Online]. Africa. Available from: http://www.itu.int/ITU-D/treg/publications/Cloud_Computing_Afrique-e.pdf.
Mack, N., Woodsong, C., MacQueen, K., Guest, G. & Namey, E. (2011). *Qualitative Research Methods:A Data Collector's Field Guide*. 1st Ed. [Online]. North Carolina, USA. Available from: http://www.fhi360.org/NR/rdonlyres/etl7vogszehu5s4stpzb3tyqlpp7rojv4waq37elpbyei3tgmc4ty6dunbccfzxtaj2rvbaubzmz4f/overview1.pdf.
Macnair, I. (2010). *Fundamentals of Strategic Management*.
Maes, K., Van Grembergen, W. & De Haes, S. (2014). Identifying Multiple Dimensions of a Business Case : A Systematic Literature Review. *The Electronic Journal Information Systems Evaluation*. 17 (1). p.pp. 47–59.
Maier, A.M., Moultrie, J. & Clarkson, P.J. (2012). Assessing organizational capabilities. *Reviewing and Guiding the Development of Maturity Grids*. [Online]. 59 (1). p.pp. 138–159. Available from: https://www.wiso-net.de/document/ECON__687937566.
Mary, B., Mccarthy, P. & Hill, S. (2011). *Cloud Adoption Points to IT Risk and Data Governance Challenges*. [Online]. USA. Available from: https://www.in.kpmg.com/SecureData/ACI/Files/cloudadoptiondaaprilmay2011.pdf.
Matthews, P. & Muntés-Mulero, V. (2013). *Data Management and Risk Modelling in Cloud Computing Maintenance*. [Online]. UK. Available from: http://www.ca.com/us/~/media/Files/About Us/CATX/data-management-and-risk-modelling-in-cloud-computing-maintenance.pdf%5Cnhttp://www.ca.com/us/collateral/articles/na/data-management-and-risk-modelling-in-cloud-computing-maintenance.aspx.
Maxwell, J. a (2012). *What Is Realism, and Why Should Qualitative Researchers Care?* Los Angeles: Sage Publications.
MCIT (2014). *Report: Saudi Arabia studies arrangements and controls required for provision of cloud computing services*. [Online]. 2014. Available from: http://www.mcit.gov.sa/En/MediaCenter/Pages/News/News-24112014_779.aspx. [Accessed: 5 August 2016].

Meadows, K. a (2003). So you want to do research? 5: Questionaire design. *British Journal Community Nursing*. 8 (12). p.pp. 562–570.
Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*. [Online]. 145. p.p. 7. Available from: http://www.mendeley.com/research/the-nist-definition-about-cloud-computing/.
Merchant, W.R., Li, J., Karpinski, A.C. & Rumrill, P.D. (2013). A conceptual overview of Structural Equation Modeling (SEM) in rehabilitation research. *Work (Reading, Mass.)*. [Online]. 45 (3). p.pp. 407–415. Available from: http://www.ncbi.nlm.nih.gov/pubmed/23594730.
Merrill, T. & Kang, T. (2014). *Cloud Computing : Is Your Company Weighing Both Benefits & Risks ?* [Online]. USA. Available from: https://pdfs.semanticscholar.org/ba76/5acb4af3307f76b02a2a9a5a645baee8ad56.pdf.
Mhlanga, O., Hattingh, Z. & Moolman, H.J. (2014). The effect of restaurant attributes on customers ' expectations and experiences in formal full service restaurants in Port Elizabeth , South Africa. *African Journal of Hospitality, Tourism and Leisure*. 3 (1). p.pp. 1–12.
Morris, N.J., Elston, R.C. & Stein, C.M. (2011). A framework for structural equation models in general pedigrees. *Human Heredity*. 70 (4). p.pp. 278–286.
Moseley, B.M. (2008). Keys to Data Governance Success : *Information Systems Audit and Control Association*. 3 (1). p.pp. 2–4.
Moultrie, J., Sutcliffe, L. & Maier, A. (2016). A maturity grid assessment tool for environmentally conscious design in the medical device industry. *Journal of Cleaner Production*. [Online]. 122. p.pp. 252–265. Available from: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84959331528&partnerID=40&md5=a96da8444daf33095e97eb42b28ade56.
Mukherjee, K. & Sahoo, G. (2010). Cloud Computing: Future Framework for e-Governance. *International Journal of Computer Applications*. 7 (7). p.pp. 31–34.
Müller, R. & Jugdev, K. (2012). Critical success factors in projects. *International Journal of Managing Projects in Business*. [Online]. 5 (4). p.pp. 757–775. Available from: http://dx.doi.org/10.1108/17538371211269040%5Cnhttp://www.emeraldinsight.com/doi/abs/10.1108/17538371211269040.
Mustimuhw Information Solutions Inc. (2015). *Data Governance Framework: Framework and Associated Tools*. [Online]. Available from: https://static1.squarespace.com/static/558c624de4b0574c94d62a61/t/558c75a5e4b0391692159c81/1435268517023/BCFNDGI-Data-Governance-Framework.pdf.
Nascio (2009). Data Governance Part II : Maturity Models – A Path to Progress. *NASCIO Governance Series*. (859). p.pp. 1–30.
Ndamase, Z. (2014). *The impact of data governance on corporate performance: the case of a petroleum company*. the University of Cape Town (UCT).
Neff, A., Schosser, M., Zelt, S., Uebernickel, F. & Brenner, W. (2013). Explicating performance impacts of it governance and data governance in multi-business organisations. In: *Australasian Conference on Information Systems (ACIS)*. 2013, pp. 1–11.
Niazi, M., Cox, K. & Verner, J. (2008). A measurement framework for assessing the maturity of requirements engineering process. *Software Quality Journal*. 16 (2). p.pp. 213–235.
Niemi, E. (2011). *Designing a Data Governance Framework*.
Noor, T.H. (2016). Usage and technology acceptance of cloud computing in Saudi Arabian Universities. *International Journal of Software Engineering and its Applications*. 10 (9). p.pp. 65–76.

Nwabude, C., Begg, C. & Mcrobbie, G. (2014). Data Governance in Small Businesses – Why Small Business Framework should be Different. In: *3rd International Conference on Business, Management and Governance*. 2014, pp. 101–107.

Oberkampf, W.L. & Trucano, T.G. (2008). Verification and validation benchmarks. *Nuclear Engineering and Design*. 238 (3). p.pp. 716–743.

Office, D.G. (2013). *The State of New Jersey Data Governance Framework Strategic Plan*. [Online]. Available from: https://www.nascio.org/portals/0/awards/nominations2014/2014/2014NJ11-NASCIO 2014 Nomination-Data Governance Office.pdf.

Olaitan, O. (2016). TAXONOMY OF LITERATURE TO JUSTIFY DATA GOVERNANCE AS A PRE- REQUISITE FOR INFORMATION GOVERNANCE. In: *Proceedings of the 28th Annual Conference of the Southern African Institute of Management Scientists*. 2016, pp. 586–605.

Olaitan, O., Herselman, M. & Wayi, N. (2016). Taxonomy of literature to justify data governance as a prerequisite for information governance. In: *Proceedings of the 28th Annual Conference of the Southern African Institute of Management Scientists ISBN:*. [Online]. 2016, pp. 586–605. Available from: http://www.up.ac.za/media/shared/643/ZP_Files/2016/Papers/gm26_full.zp97836.pdf.

Oliveira, T., Thomas, M. & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information and Management*. 51 (5). p.pp. 497–510.

Otto, B. (2011a). A Morphology of the Organisation of Data Governance. In: *ECIS 2011 Proceedings*. 2011, p. 272.

Otto, B. (2011b). Data governance. *Business and Information Systems Engineering*. 3. p.pp. 241–244.

Owuonda, S.O. & Orwa, D. (2016). Cloud Computing Governance Readiness Assessment : Case Study of a local Airline Company. *International Journal of Applied Information Systems (IJAIS)* –. 10 (8). p.pp. 33–42.

Owuonda, S.O., Orwa, D., Al-ruithe, M., Benkhelifa, E. & Hameed, K. (2016). Cloud Computing Governance Readiness Assessment : Case Study of a local Airline Company. *Sustainability*. [Online]. 10 (1). p.p. 95. Available from: http://www.mdpi.com/2071-1050/10/1/95.

Panian, Z. (2010a). Some Practical Experiences in Data Governance. *World Academy of Science, Engineering and Technology*. 62. p.pp. 939–946.

Panian, Z. (2010b). Some Practical Experiences in Data Governance. *World Academy of Science, Engineering and Technology*. p.pp. 939–946.

Pearson, S., Tountopoulos, V., Catteddu, D., Sudholt, M., Molva, R., Reich, C., Fischer-Hubner, S., Millard, C., Lotz, V., Jaatun, M.G., Leenes, R., Rong, C. & Lopez, J. (2012). Accountability for cloud and other future Internet services. *CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science*. p.pp. 629–632.

Pennanen, I. (2014). *Data governance Intelligent way of managing data*. [Online]. Turun ammattikorkeakoulu. Available from: www.detica.com.

Petersen, K., Feldt, R., Mujtaba, S. & Mattsson, M. (2008). Systematic Mapping Studies in Software Engineering. *12Th International Conference on Evaluation and Assessment in Software Engineering*. [Online]. 17. p.p. 10. Available from: http://www.cse.chalmers.se/~feldt/publications/petersen_ease08_sysmap_studies_in_se.pdf.

Pinto, J.K. & Prescott, J.E. (1988). Variations in Critical Success Factors Over the Stages in the Project Life Cycle [electronic version]. *Journal of Management*. [Online]. 14 (1).

p.pp. 5–18. Available from: http://journals.sagepub.com.
Poeppelbuss, J., Simons, A. & Simons, A. (2011). Maturity Models in Information Systems Research : Literature Search and Analysis. *Communications of the Association for Information Systems Volume*. 29 (1). p.pp. 1–30.
Pohlman, M. (2010). *Using the CSA Control Matrix and ISO 27017 controls to facilitate regulatory compliance in the cloud*.
Pokharel, S. (2013). *Oklahoma Interoperability Grant Project Oklahoma Interoperability Grant Data Roadmap*. 2nd Ed. Washington,: US Department of Health and Human Services.
Poor, M. (2011a). *Applying Aspects of Data Governance from the Private Sector to Public Higher Education*. [Online]. Eugene,. Available from: https://scholarsbank.uoregon.edu/xmlui/handle/1794/11400.
Poor, M. (2011b). *Applying Aspects of Data Governance from the Private Sector to Public Higher Education*. [Online]. 1277 (July). p.p. 125. Available from: https://scholarsbank.uoregon.edu/jspui/bitstream/1794/11400/1/Poor-2011.pdf.
Power, D. & Street, W. (2013). *Sponsored by All the Ingredients for Success : Data Governance , Data Quality and Master Data Management*. [Online]. Bury Saint Edmunds. Available from: http://www.oracle.com/us/products/middleware/data-integration/odi-ingredients-for-success-1380930.pdf.
Prasetyo, H.N. & Surendro, K. (2015). Designing a data governance model based on soft system methodology (SSM) in organization. *Journal of Theoretical and Applied Information Technology*. [Online]. 78 (1). p.pp. 46–52. Available from: http://www.scopus.com/inward/record.url?eid=2-s2.0-84938938871&partnerID=tZOtx3y1.
Preittigun, A. & Chantatub, W. (2012). A Comparison between IT Governance Research and Concepts in COBIT 5. *International Journal of Research in Management & Technology*. 2 (6). p.pp. 581–590.
Prinzo, R. (2012). *Developing a Strategy for your Data Governance Initiative*. [Online]. South Carolina. Available from: https://hcexchange.conference-board.org/attachment/Rob-Prinzo---WSR_JunJul12_all-3.pdf.
Rajendran, S. (2013). *Organizational Challenges in Cloud Adoption and Enablers of Cloud Transition Program*. [Online]. Available from: http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf%5Cnhttp://arxiv.org/abs/1203.1979.
Rajvanshi, P., Nagar, V. & Chawla, P. (2013). Data Protection in Cloud Computing. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*. [Online]. 3 (3). p.pp. 149–155. Available from: http://ijitee.org/attachments/File/v3i3/C1122083313.pdf.
Ratnam, K.A., Dominic, P.D.D. & Ramayah, T. (2014). A structural equation modeling approach for the adoption of cloud computing to enhance the Malaysian healthcare sector systems-level quality improvement. *Journal of Medical Systems*. 38 (8). p.pp. 2–14.
Rau, K.G. (2004). Effective Governance of IT: Design Objecitves, Roles, and Relationships. *Information Systems Management*. 21 (4). p.pp. 35–42.
Rausch, N., Corporation, S. a S. & Alexander, M. (2013). *SAS Global Forum 2013 Data Management Best Practices in SAS ® Data Management for Big Data SAS Global Forum 2013 Data Management*. [Online]. Available from: https://www.sas.com/content/dam/SAS/en_ca/doc/other1/best-practices-enterprise-data-governance-106538.pdf.

Rebollo, O., Mellado, D. & Fernández-medina, E. (2014). Empirical Evaluation of a Cloud Computing Information Security Governance Framework. *Information and Software Technology*. [Online]. 58. p.pp. 44–57. Available from: http://dx.doi.org/10.1016/j.infsof.2014.10.003.
Redman, T.C. (2013). Data' s Credibility Problem. *Harvard Business Review*. 91 (12). p.pp. 84–88.
Reeves, M.G. & Bowen, R. (2013). Developing a data governance model in health care. *Healthcare financial management : journal of the Healthcare Financial Management Association*. [Online]. 67 (2). p.pp. 82–6. Available from: http://www.ncbi.nlm.nih.gov/pubmed/23413674.
Rennekamp, R. & Nall, M. (2002). *Using focus groups in program development and evaluation*. [Online]. Kentucky. Available from: http://www.ca.uky.edu/agpsd/Focus.pdf.
Rifaie, M., Alhajj, R. & Ridley, M. (2009). Data governance strategy: A key issue in building enterprise data warehouse. In: *iiWAS2009 - The 11th International Conference on Information Integration and Web-based Applications and Services.ACM*. [Online]. 2009, pp. 587–591. Available from: http://www.scopus.com/inward/record.url?eid=2-s2.0-77954571509&partnerID=40&md5=dff7261ca6b5b8bc3440c9bf1b5ef864.
Rimal, B.P., Jukan, A., Katsaros, D. & Goeleven, Y. (2011). Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. *Journal of Grid Computing*. 9 (1). p.pp. 3–26.
Rivera, S., Loarte, N., Raymundo, C. & Dominguez, F. (2017). Data governance maturity model for micro financial organizations in Peru. In: *ICEIS 2017 - Proceedings of the 19th International Conference on Enterprise Information Systems*. [Online]. 2017, pp. 203–214. Available from: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85023167622&partnerID=40&md5=75dfca25fc7ac9709fbc5c63a5e504ad.
Rose, J. & Guide, P. (2013). *Selecting, Using, and Creating Maturity Models: A Tool for Assurance and Consulting Engagements*. [Online]. USA. Available from: https://www.iia.org.uk/media/358857/selecting__using__and_creating_maturity_models_-__a_tool_for_assurance_and_consulting_engagements.pdf.
Rouse, A.C. & Corbitt, B. (2008). There ' s SEM and ' SEM ': A Critique of the Use of PLS Regression in Information Systems Research. In: *the 19th Australasian Conference on Information Systems*. 2008, pp. 845–855.
Russom, P. (2008). Data Governance strateGies. *Business Intelligence Journal*. [Online]. 13 (2). p.pp. 13–15. Available from: http://dev.meritalk.com/uploads_legacy/whitepapers/tdwi_pathfinder1.pdf.
Rutnam, P. (2013). *Monitoring and Evaluation Strategy*. [Online]. London. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/175300/monitoring-evaluation-strategy.pdf.
Ryu, K., Park, J. & Park, J. (2006). A Data Quality Management Maturity Model. *ETRI Journal*. [Online]. 28 (2). p.pp. 191–204. Available from: http://etrij.etri.re.kr/Cyber/BrowseAbstract.jsp?vol=28&num=2&pg=191.
Saidah, a S. & Abdelbaki, N. (2014a). A new cloud computing governance framework. In: *Proceedings of the 4th International Conference on Cloud Computing and Services Science*. [Online]. 2014, pp. 671–678. Available from: http://www.scopus.com/inward/record.url?eid=2-s2.0-84902352099&partnerID=40&md5=cedce19630e88e4321cd8e9234b59920.
Saidah, a S. & Abdelbaki, N. (2014b). A new cloud computing governance framework. *CLOSER 2014 - Proceedings of the 4th International Conference on Cloud Computing and Services Science*. [Online]. p.pp. 671–678. Available from:

http://www.scopus.com/inward/record.url?eid=2-s2.0-84902352099&partnerID=40&md5=cedce19630e88e4321cd8e9234b59920.
Saleforce.com (2010). *Secure , private , and trustworthy : enterprise cloud computing with Force . com*.
Saleh, M. (2011). Information Security Maturity Model. *International Journal of Computer Science and Security ….* [Online]. 5 (3). p.pp. 316–337. Available from: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Information+Security+Maturity+Model#0.
Salem Basamh, S., Qudaih, H.A. & Adam Suhaimi, M. (2014). E-Government Implementation in the Kingdom of Saudi Arabia: An Exploratory Study on Current Practices, Obstacles & Challenges. *International Journal of Humanities and Social Science*. 4 (2). p.pp. 296–300.
Salido, J., Manager, S.P., Group, T.C., Corporation, M. & Cavit, D. (2010a). A Guide to Data Governance for Privacy , Confidentiality , and Compliance. *Microsoft Trustworthy Computing*. [Online]. Part (January). p.p. 35. Available from: https://privacyassociation.org/media/pdf/knowledge_center/Guide_to_Data_Governance_Part5_Moving_to_Cloud_Computing_whitepaper.pdf.
Salido, J., Manager, S.P., Group, T.C., Corporation, M. & Cavit, D. (2010b). *A Guide to Data Governance for Privacy , Confidentiality , and Compliance*. [Online]. USA. Available from: https://iapp.org/media/pdf/knowledge_center/Guide_to_Data_Governance_Part1_The_Case_for_Data_Governance_whitepaper.pdf.
Sandra Nunn (2009). Driving Compliance through Data Governance. *Journal of AHIMA*. 80 (3). p.pp. 50–51.
Sarsfield, S. (2009). *Data governance imperative*. IT Governance Limited (ed.). cambridgeshaire: IT Governance Publishing.
Saudi Vision 2030 (2017). *Saudi Vision 2030*. [Online]. 2017. Available from: http://vision2030.gov.sa/en. [Accessed: 5 July 2017].
Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research methods for business students*. Fifth Edit. Prentice Hall.
Saunders, M., Lewis, P. & Thornhill, A. (2006). Understanding research philosophies and approaches. *Reserach Methods for Business Students*. p.pp. 127–148.
Schipper, J. (2002). *The Dynamic Architecture Maturity Matrix: Assessment analysis and instrument validation*. Sogeti Netherlands B.V.
Seiner, R.S. (2014). *Non-Invasive data governance*. first. KIK Consulting & Educational (ed.). New york.
Self, R.J. (2014). Governance Strategies for the Cloud , Big Data and other Technologies in Education. In: *IEEE/ACM 7th International Conference on Utility and Cloud Computing Governance*. 2014.
Sengupta, S., Kaulgud, V. & Sharma, V.S. (2011). Cloud Computing Security--Trends and Research Directions. In: *2011 IEEE World Congress on Services*. 2011, pp. 524–531.
Sheridan, C. (2005). *SPSS: Analysis without anguish: Version 12.0 for Windows.* 1st Editio. John Wiley & Sons.
Shimba, F. (2010). *Cloud Computing : Strategies for Cloud Computing Adoption Cloud Computing : Strategies for Cloud Computing Adoption*. [Online]. Dublin Institute of Technology. Available from: http://arrow.dit.ie/cgi/viewcontent.cgi?article=1028&context=scschcomdis.
Shyu, C., Li, Y.-L. & Tang, Y. (2013). Applying Confirmatory Factor Analysis on the Measure for Restaurant Over-service. *The Journal of International Management Studies*. 8 (2). p.pp. 10–16.

Silic, M. & Back, A. (2013). Factors impacting information governance in the mobile device dual-use context. *Records Management Journal*. [Online]. 23 (2). p.pp. 73–89. Available from: http://www.emeraldinsight.com/doi/10.1108/RMJ-11-2012-0033.

Simon, M.K. and Goes, J. (2011). *Developing a Theoretical Framework*. [Online]. Available from: www.dissertationrecipes.com.

Siniscalco, M.T. & Auriat, N. (2005). Questionnaire design: Quantitative research methods in educational planning. *International Institute for Educational Planning*. [Online]. 1 (1). p.pp. 1–85. Available from: http://unesdoc.unesco.org/images/0021/002145/214555e.pdf.

Smitha, K.K., Chitharanjan, K. & Thomas, T. (2012). Cloud based e-governance system : A survey. In: *Procedia Engineering*. 2012, pp. 3816–3823.

Soares, S. (2012). The IBM data governance unified process: driving business value with IBM software and best practices. *ISACA JOURNAL*. 4. p.p. 153.

Software Engineering Institute (2010). *CMMI for Development, Version 1.3*. [Online]. USA. Available from: http://repository.cmu.edu/sei/287/.

Solemon, B. (2013). Evaluation Criteria for Requirements Engineering Process Improvement Models and Frameworks. *Computational Method in Science and Engineering*. p.pp. 15–20.

Solutions, C. (2013). *Data governance in the cloud*. [Online]. Available from: https://www.cloudindustryforum.org/file/46/download?token=NvhsDhXt.

Suhr, D. (2006). *Exploratory or confirmatory factor analysis?* [Online]. Northern Colorado: University of Northern Colorado. Available from: http://140.112.142.232/~PurpleWoo/Literature/!DataAnalysis/FactorAnalysis_SAS.com_200-31.pdf.

Suri, P.K. & Mittal, S. (2012). A Comparative Study of various Computing Processing Environments : A Review. *(IJCSIT) International Journal of Computer Science and Information Technologies,*. 3 (5). p.pp. 5215–5218.

Taherdoost, H., Sahibuddin, S. & Jalaliyoon, N. (2014). Exploratory factor analysis: Concepts and theory. In: *2nd International Conference on Mathematical, Computational and Statistical Sciences*. 2014, pp. 375–382.

Tashkandi, A. & Al-Jabri, I. (2015). Cloud Computing Adoption by Higher Education Institutions in Saudi Arabia: Analysis Based on TOE. In: *2015 International Conference on Cloud Computing (ICCC)*. [Online]. 2015, pp. 1–8. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7149634.

Tavakol, M. & Dennick, R. (2011). Making sense of Cronbach's alpha. *International journal of medical education*. 2. p.pp. 53–55.

Thatcher, R.W. (2010). Validity and Reliability of Quantitative Electroencephalography. *Journal of Neurotherapy*. 14 (2). p.pp. 122–152.

The Data Governance Institute (2015). *Definitions of Data Governance*. [Online]. 2015. Available from: http://www.datagovernance.com/adg_data_governance_definition/. [Accessed: 16 February 2015].

Thomas, G. (2009). How to use the DGI data governance framework to configure your program. *Data Governance Institute*. [Online]. p.p. 17. Available from: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:How+to+use+the+DGI+Data+Governance+Framework+to+configure+your+program#0.

Thomas, G. (2006). *The DGI data governance framework*. [Online]. Orlando, FL (USA). Available from: http://www.datagovernance.com/wp-content/uploads/2014/11/dgi_framework.pdf.

Toney, Shraddha, Kadam, S. (2013). Cloud Information Accountability Frameworks for Data Sharing \nin Cloud. *IOSR Journal of Computer Engineering (IOSR-JCE)*. [Online]. 4

(3). p.pp. 93–96. Available from: http://www.iosrjournals.org/iosr-jce/papers/Vol13-issue2/N01329396.pdf?id=3545.
Tountopoulos, V., Felici, M., Pannetrat, A., Catteddu, D. & Pearson, S. (2014). Interoperability Analysis of Accountable Data Governance in the Cloud. *Cyber Security and Privacy Forum. Springer, Cham,*. 470. p.pp. 77–88.
Traulsen, S. & Tröbs, M. (2011). Implementing Data Governance within a Financial Institution. *41. Jarestagung der Gesellschaft für Informatik*. [Online]. 4 (7). p.p. 192. Available from: http://www.user.tu-berlin.de/komm/CD/paper/050141.pdf.
Trivedi, H. (2013). *Cloud Adoption Model for Governments and Large Enterprises*. [Online]. Available from: http://web.mit.edu/smadnick/www/wp/2013-12.pdf.
Truong, H.L. & Dustdar, S. (2012). A survey on cloud-based sustainability governance systems. *International Journal of Web Information Systems*. [Online]. 8. p.pp. 278–295. Available from: http://www.scopus.com/inward/record.url?eid=2-s2.0-84886401122&partnerID=tZOtx3y1.
Tweneboah-koduah, S. (2014). BARRIERS TO GOVERNMENT CLOUD ADOPTION. *International Journal of Managing Information Technology (IJMIT)*. 6 (3). p.pp. 1–16.
Vats, K., Sharma, S. & Rathee, A. (2012). A Review of Cloud Computing and e-Governance. *International Journal of Advanced Research in Computer Science and Software Engineering*. [Online]. 2 (2). p.p. 5. Available from: http://www.ijarcsse.com/.
Victor, E. (2016). *An Assessment of Data Governance at Kenya Health Professionals Regulatory Authorities*. UNIVERSITY OF NAIROBI.
Weber, A.S. (2011). Cloud Computing in Education in the Middle East and North Africa (Mena) Region : Can Barriers Be Overcome ? In: *The 7th International Scientific Conference eLearning and Software for Education Bucharest April 2829 2011*. 2011, pp. 1–42.
Weber, K., Cheong, L., Otto, B. & Chang, V. (2008). Organising Accountabilities for Data Quality Management-A Data Governance Case Study. *Data Warehousing*. [Online]. p.pp. 347–362. Available from: http://www.alexandria.unisg.ch/export/DL/Robert_Winter/204595.pdf.
Weber, K., Otto, B. & Osterle, H. (2009a). One Size Does Not Fit All — A Contingency Approach to Data Governance. *ACM Journal of Data and Information Quality*. [Online]. 1 (1). p.p. 4:1-4:27. Available from: http://dl.acm.org/citation.cfm?id=1515696.
Weber, K., Otto, B. & Osterle, H. (2009b). One Size Does Not Fit All — A Contingency Approach to Data Governance. *ACM Journal of Data and Information Quality*. 1 (1). p.p. 4:1-4:27.
Weill, P. & Ross, J. (2007). *IT Governance Executive Questionnaire*. USA.
Wende, K. (2007a). A Model for Data Governance – Organising Accountabilities for Data Quality Management. *Corporate Governance*. [Online]. p.pp. 417–425. Available from: http://aisel.aisnet.org/acis2007/80.
Wende, K. (2007b). A Model for Data Governance – Organising Accountabilities for Data Quality Management. In: *Proceedings of 18th Australasian Conference on Information Systems*. [Online]. 2007, pp. 417–425. Available from: http://aisel.aisnet.org/acis2007/80.
Wende, K. (2007c). Data Governance Defining Accountabilities for Data Quality Management. *D'Atri, Alessandro (Hrsg.)*. [Online]. Available from: https://www.alexandria.unisg.ch/publications/Kristin_Wende/214034.
Wende, K. & Otto, B. (2007). A contingency approach to data governance. In: *Proceedings, 12th International Conference on Information Quality (ICIQ-07), Cambridge, USA*. 2007, p. 14.

Wibowo, M.A. & Waluyo, R. (2015). Knowledge management maturity in construction companies. *Procedia Engineering*. [Online]. 125 (1). p.pp. 89–94. Available from: http://dx.doi.org/10.1016/j.proeng.2015.11.014.

Williams, J.J. & Ramaprasad, a. (1996). A taxonomy of critical success factors. *European Journal of Information Systems*. [Online]. 5 (4). p.pp. 250–260. Available from: http://www.scopus.com/inward/record.url?eid=2-s2.0-21444443126&partnerID=tZOtx3y1.

Williams, P.A.H. (2007). Information governance: a model for security in medical practice. *Journal of Digital Forensics, Security and Law*. 2 (1). p.pp. 57–74.

Woldu, L. (2013). *Lewam Woldu Cloud Governance Model and Security Solutions for Cloud Service Providers*. Helsinki Metropolia University of Applied Science.

Wright, D.B. (2006). Causal and associative hypotheses in psychology: Examples from eyewitness testimony research. *Psychology, Public Policy, and Law*. [Online]. 12 (2). p.pp. 190–213. Available from: http://doi.apa.org/getdoi.cfm?doi=10.1037/1076-8971.12.2.190.

Yale; Wendy. (2011). *Is data governance in cloud computing still a mirage or do we have a vision we can trust*. [Online]. USA. Available from: http://vmblog.com/archive/2011/02/10/is-data-governance-in-cloud-computing-still-a-mirage-or-do-we-have-a-vision-we-can-trust.aspx#.WlSfoovA4cg.

Yeasmin, S. & Rahman, K.F. (2012). ’ Triangulation ’ Research Method as the Tool of Social Science Research. *BUP Journal*. 1 (1). p.pp. 154–163.

Appendices

Appendix A: Understanding Cloud Computing Technology

Recently, cloud computing has become one of the most significant debated issues of information technology, and it has motivated research on related technologies by academia and the industry. In 2007, cloud computing was introduced as an important new topic in the technical and academic fields (Stephen, 2007; Lohr, 2007). Cloud computing is also an emerging trend and undergoing serious adoption in both public and private sector organisations. As organisations of all shapes and sizes begin to adapt to cloud computing, this technology is evolving like never before. Industry experts believe that this new technology will continue to grow and develop even further in the coming few years (Apostu et al., 2013). There are differences between cloud computing and traditional computing in many areas. Sriram and Khajeh-Hosseini (2010) reiterated this view by pointing out that cloud computing is a shift from computing as a product to computing as a service that is delivered to consumers over the internet. Rader (2012) states that the main differences between cloud computing and traditional computing are in the areas of what to manage, form of contract, accounting treatment, increments of functionality, development and maintenance tasks, infrastructure tasks, units of measure and cost structure. Cloud computing is composed of various elements from other computational models such as autonomic computing, grid computing and utility computing to form one of the most innovative computational deployment architectures in the world today. Cloud computing can be defined as simply a set of services in information technology that are provided to a customer on demand over a network. Hence, for scientists, clouds promise to be an alternative to supercomputers, clusters and grids (Goyal, 2014). The cloud computing definition mainly used today is the one expressed by the National Institute of Standards and Technology (NIST) (Jansen & Grance, 2011). The NIST defines cloud computing as "*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*".

Cloud computing offers organisations more choices as regards how to run infrastructures, save costs and delegate liabilities to third-party providers. In addition, the cloud can achieve many advantages and disadvantages for organisations when they decide to move their service and data to cloud computing. The main advantages of cloud computing for businesses include: cost efficiency, almost unlimited storage, backup and recovery, automatic software integration, easy access to information, quick deployment, agility, easier scale of services and delivery of new services (Rajan, 2012; Apostu et al., 2013). However, in spite of its many advantages, cloud computing also has its disadvantages. Organisations need to be aware of these aspects before moving their data and services to this technology. The main disadvantages involved in cloud computing are: technical issues, security in the cloud, prone to attack, possible downtime, cost, inflexibility and lack of support (Apostu et al., 2013). Recently, data has become an essential part and the primary asset that enterprises and individuals possess. Yet, despite the advantages of cloud computing, many potential cloud users have yet to join the cloud, because they are worried about putting their sensitive data in the cloud. There are growing concerns about the security, integrity and confidentiality of data stored in the cloud computing environment side infrastructure (Sengupta et al., 2011). Lack of control over sensitive data in the cloud is also a major worry for cloud consumers (Chow et al., 2009). One aspect of control in cloud implementation is transparency. Loss of data governance is also a top risk and concern in cloud computing (Ko et al., 2011). The implications from data control being transferred to a third party are not yet fully understood, and many organisations hold back because the lack of transparency makes it difficult for them to adhere to regulatory compliance. In particular, a cloud user may not receive adequate support if served a subpoena or faced with legal action, cannot have any guarantee whether data was deleted by the provider according to its retention policy, and could face audit difficulty. In addition, there are concerns about the theft of a company's proprietary information by a cloud provider (Chow et al., 2009).

Over all, to encourage users to adopt cloud computing in their organisation, cloud providers have to work with them to address their concerns. This is the major contribution in this study. In general, cloud computing has become an integral part of business and technology models, and has forced organisations to adapt to new technology strategies (Gorelik 2013). Cloud computing architecture is composed of five essential characteristics, four deployment models, three service models and five cloud actors (Mell & Grance, 2011).

- **Essential Characteristics**

Cloud computing has certain characteristics in order to meet expected user requirements and to provide qualitative services. NIST has categorised the essential characteristics of cloud computing as:

6. ***On-demand self-service:*** A consumer can access provision-computing capabilities, such as server time and network storage, as needed automatically without the service provider's intervention.
7. ***Broad network access:*** To profit cloud computing services, the internet works as a backbone for cloud computing. The services are available over the network and accessed through standard mechanisms that promote use by mobile phones, tablets, laptops and workstations.
8. ***Resource pooling:*** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify the location at a higher level of abstraction (e.g., country, state or data centre). Examples of resources include storage, processing, memory and network bandwidth.
9. ***Rapid elasticity:*** Elasticity is the beauty of cloud computing. The users also can access cloud resources in any quantity at any time. The resources can be provisioned without cloud service provider intervention and can be quickly scaled in and scaled

out according to the consumer’s needs to deliver high-quality services in a secure way.

10. ***Measured service:*** Automatically control and optimise resources for the cloud system’s use by leveraging a metering capability. The users can achieve different service quality at different charges to optimise resources at different levels of abstraction suitable to the service (e.g., SaaS, PaaS, IaaS, storage, processing, bandwidth and active user accounts). These can be monitored, controlled and reported, providing transparency for both the provider and consumer of the utilised service.

- ## Cloud Actors

Cloud actors refers to a person or an organisation that participates in a process or a transaction and/or performs tasks in the cloud computing environment. According to the NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud auditor, cloud carrier and cloud broker (Lui 2011). The cloud actors are the following:

1. ***Cloud Consumer:*** A person or organisation that maintains a business relationship with and uses services from cloud providers.
2. ***Cloud Provider:*** A person, organisation or entity responsible for making a service available to interested parties.
3. ***Cloud Auditor:*** A party that can conduct independent assessment of cloud services, information system operation, performance and security of the cloud implementation.
4. ***Cloud Broker:*** An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers.
5. ***Cloud Carrier:*** An intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers.

- ## Service Delivery Model

Cloud providers offer services to cloud consumers through several service delivery models. These models describe how cloud computing services are made available to consumers (Gorelik, 2013). The fundamental cloud service models include:

- **Infrastructure as a Service (IaaS)**

Infrastructure as a Service (IaaS) is the first layer in the cloud computing environment. In this model, the cloud provider delivers the infrastructure to the consumer over the internet. Therefore, the user is able to deploy and run various software over the internet (e.g., system or application software) (Ullah & Xuefeng 2013). The consumers have the ability to provision computing power, storage and networks (Goyal, 2014). They have control over operating systems, deployed applications and storage, and partial control over the network. Nevertheless, they have no control over all the infrastructure resources. This model incorporates a number of unique characteristics. The key characteristic of an IaaS cloud enabling computing resources to scale up and down are elasticity and scalability. The IaaS model also allows customers to rent computing resources and start a new project quickly. However, the main challenge in the IaaS model is security (Bulla et al., 2013). Some IaaS providers are GoGrid, Flexiscale, Joyent and Rackspace.

- **Platform as a Service (PaaS)**

Platform as a service (PaaS) is the middleware model, and it is an alternative to the traditional platform model. It has more benefits because all the infrastructure needed to run applications will be accessed over the internet. PaaS refers to applications created by a development language that is hosted by the cloud service provider in a cloud infrastructure. In this model, the cloud provider not only provides the hardware, it also allows customers or software developers to build their own applications by delivering higher-level services in the form of program development tools, platforms and frameworks, and provides these applications to the end-users (Fernandes et al., 2013). Some popular PaaS providers are GAE, Microsoft's Azure and Force.com.

- **Software as a Service (SaaS)**

Software as a Service (SaaS) is a term that refers to software in the cloud. It is one of the leading service models and is the one most commonly adopted by organisations using the cloud. SaaS is the capability provided to the user to use the cloud provider's applications that are running on a cloud infrastructure (Mell & Grance 2011). The consumer can access these applications and services via networks from various client devices and client interface (e.g., web browser, mobile phone) (Bulla et al. 2013). Consumers do not manage or control the underlying cloud infrastructure including the network, operating systems, servers, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings (Goyal, 2014). This model incorporates a number of unique characteristics. One of these characteristics is that consumers no longer need to install or buy a software product. They can access it directly via the internet from a Software as a Service provider, for example, Google Apps or Microsoft Office 365 (Alam and Shakil, 2015). However, there are two main challenges with the SaaS model: integration applications and data locality:

- ***Integration***: Enterprise resource planning (ERP) is one of the applications that provide services to business area. SaaS providers develop application programming interfaces (APIs) to solve integration problem for companies (Bulla et al., 2013). Thus, APIs also have some limitations because an API requires coding and maintenance for modification and updates to it (Bulla et al., 2013).
- ***Data locality:*** The locality of data is a very important part of the enterprise architecture and the problem is that the customer does not know where the data is being stored, due to compliance and data privacy laws in various countries (Bulla et al., 2013).

In summary, the three primary service delivery models discussed in this study are Software as a Service (SaaS), where the control is limited only to applications the consumer uses, Infrastructure as a Service (IaaS), where the consumer uses and has control over processing power, storage and network components, and Platform as a Service (PaaS), in which the consumer uses and has control over the hosting environment for their applications (see Figure). These service delivery models may have synergies between them and be interdependent. For instance, PaaS is dependent on IaaS because application platforms require a physical infrastructure.

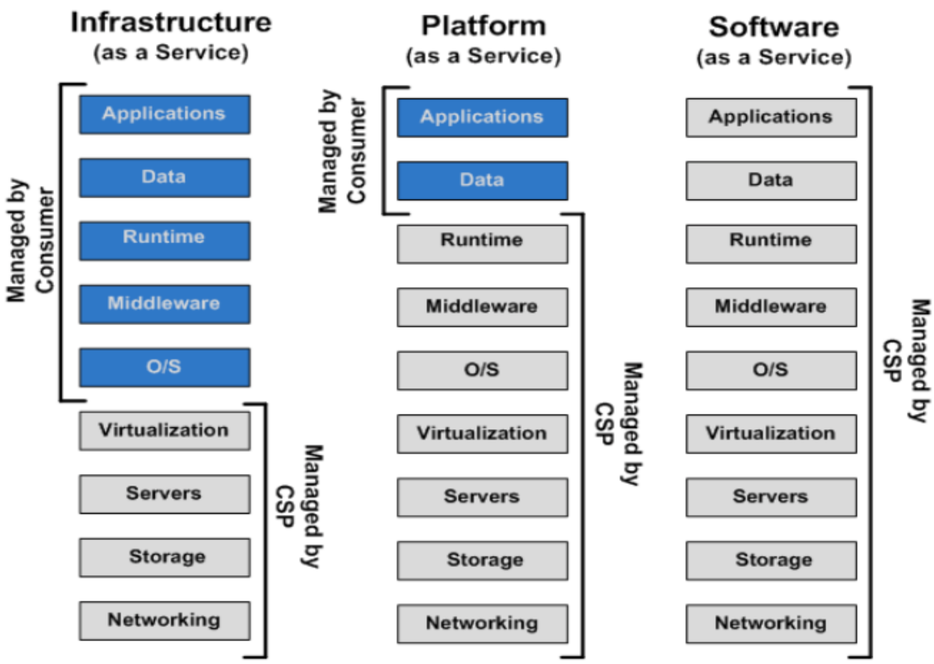

Figure 2.3. Cloud Service Model. Source: Lui (2011).

- **Cloud Deployment Models**

Cloud computing is an emerging technology and organisations of different sizes are thinking about deploying their services in the cloud. Cloud computing deployment models are classified into four types: public, private, hybrid and community (Mell & Grance, 2011). In this study, all the four cloud deployment models are defined, discussed and compared with their benefits and drawbacks, thus providing a clear idea of which model would be most beneficial for specific organisations to adopt.

- **Public Cloud**

The infrastructure of the public cloud is made available to the general public or a large industry group and is owned, managed and operated by an organisation that sells cloud services (Mell & Grance, 2011). This means the public cloud offers applications, storage and other services to the general public by a service provider based on a "pay-as-you-go" model. A public cloud is hosted on the internet and designed to be used by any user with an internet connection to provide a similar range of services and capabilities. This model is considered to be the best model for small and start-up companies because users can scale their use on demand and do not need to purchase new hardware to use the service (Eugene 2013). Microsoft, Amazon, Google and Salesforce.com are the most popular public cloud vendors that offer their services to the general public. There are many advantages of public clouds for cloud consumers, which are data availability and continuous uptime, 24/7 technical support, no wasted resources, and easy and inexpensive setup (Subashini & Kavitha 2011). However, data security, privacy, data location, reliability and data back-up are the most signification challenges for organisations in a public cloud environment (Jansen & Grance 2011). This model also faces some legal issues because the data may not even be in the same country as the cloud consumer; it can be located anywhere in the world.

- **Private Cloud**

The infrastructure of a private cloud is provisioned for exclusive use by a single organisation including multiple users (e.g., business units). It may be owned, managed and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises (Mell & Grance, 2011). This model does not offer services to the general public; it is hosted in an organisation's data centre and provides its services only to users inside that organisation or its partners (Goyal, 2014). Consumers are charged on the basis of per gigabyte usage along with bandwidth transfer fees. Furthermore, data stored in the private cloud can only be shared amongst the organisation's users and third-party sharing depends upon the trust the third party builds with the organisation. The big advantage that the private cloud has over the public cloud is that of data privacy and security. However, the major disadvantage of the private cloud is its higher cost. The number of private clouds increased in 2013 and it requires highly skilled IT technicians to manage them and improve security, control, resiliency, compliance and transparency (Fernandes et al., 2013). Popular examples of private clouds include Amazon Virtual Private Cloud (Amazon VPC), Eucalyptus Cloud Platform, IBM SmartCloud Foundation and Microsoft Private Cloud (Parsi and Laharika, 2013).

- **Hybrid Cloud**

Hybrid clouds are more complex than the other deployment models (private, community or public). A hybrid cloud is a cloud computing environment that is a mixture of two or more other cloud deployment models (public, community and private clouds) which are circumscribed by a secure network and centrally managed (Fernandes et al., 2013). This model is managed by the owner organisation and a third party in both on-site and off-site locations (Goyal, 2014). The hybrid cloud brings together the advantages of public and private clouds and improves the challenges of each one. It has many benefits that reduce capital expenses as part of the organisation's infrastructure, offers the ability to rapidly scale in the public cloud and controls in a private cloud (Goyal 2014). A major advantage of the hybrid cloud model is that an organisation only pays for extra computing resources when they are needed. Hybrid cloud architecture requires both on-premises resources and off-site (remote) server-based cloud infrastructure (Parsi and Laharika, 2013). However, there are risks associated with the security policies spanning the hybrid cloud environment such as issues with how encryption keys are managed in a public cloud compared to a purely private cloud environment (Goyal 2014). Hybrid clouds are usually deployed by organisations that require faster implementation for projects and that are willing to push part of their workload to public clouds for cloud-bursting purposes (Goyal 2014).

- **Community Cloud**

A community cloud falls between private and public cloud environments with respect to the target set of users. It is somewhat similar to a private cloud, but the infrastructure and computational resources are exclusive to two or more organisations that have common privacy, security and regulatory considerations, rather than a single organisation (Goyal 2014). A Community clouds are provisioned for exclusive use by a business community of consumers from organisations that have shared concerns, which are concrete industries such as the public sector, healthcare and media (Marinos & Briscoe 2009). Furthermore, the community cloud is designed for organisations that have shared concerns such as security requirements, mission, policy and compliance considerations (Sen 2013a). It can be managed by the owner’s committee or from another cloud provider, and may be placed at an on-site or off-site location (Fernandes et al., 2013). The community cloud removes the costs of private clouds and the security risks of public clouds. According to Briscoe and Marinos (2009), “*Community cloud computing makes use of the principles of digital ecosystems to provide a paradigm for clouds in the community, offering an alternative architecture for the use cases of cloud computing*”. It is more technically challenging to handle distributed computing issues in the community cloud; these issues include latency, additional security requirements and differential resource management (Briscoe & Marinos 2009). The advantages of the community cloud are that the set-up costs can be cheaper than those for a private cloud because they are divided among all participants. Additionally, management of the community cloud can be outsourced to a cloud provider that will be bound by contract and that has no preference for any of the clients involved (Goyal 2014). However, drawbacks of the community cloud are that the costs are higher than those for the public cloud, and all the community members share the amount of bandwidth and data storage (Goyal 2014). Therefore, all the government organisations in a city or country can share the same cloud (Parsi and Laharika, 2013). Figure shows the cloud computing definition schema.

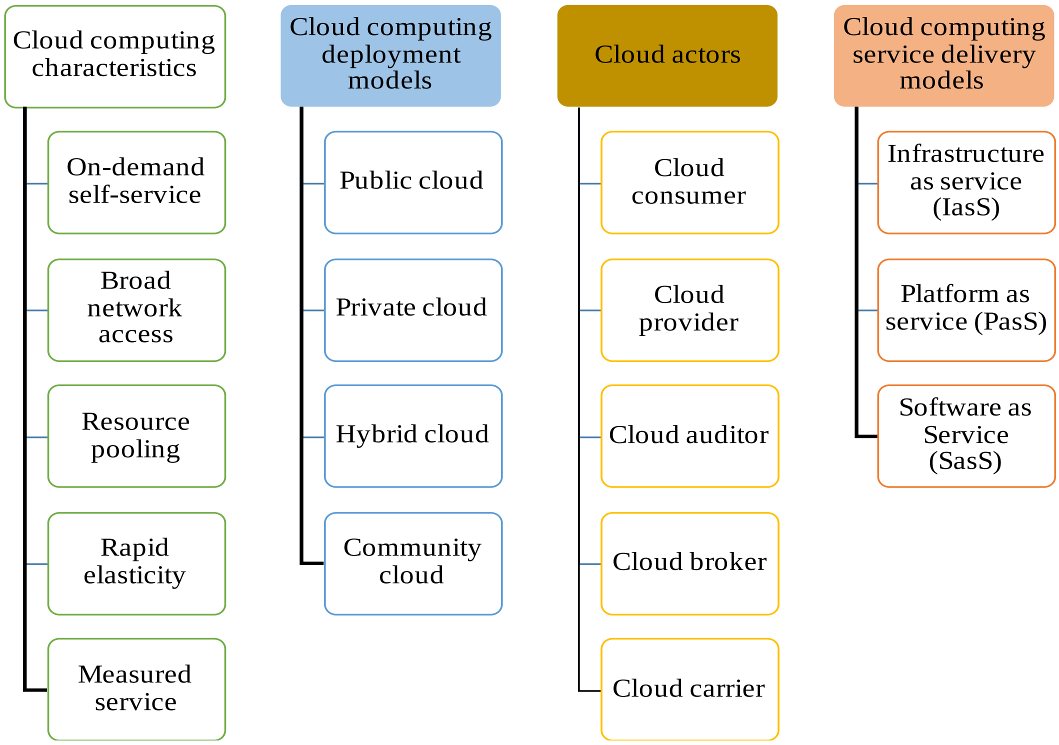

Figure 2.4. The cloud computing definition schema.

Appendix B: Systematic Literature Review of Maturity Model

- **Research Questions**

Table 4.1. Research Questions.

Nr.	Research question	Rationale
Q1	What are the most common research designs applied?	This question discovers the most important designs to develop maturity models.
Q2	What are the most common research methods applied?	This question discovers the most important methods to develop maturity models.
Q3	What are the most common theoretical foundations to develop maturity models?	This question discovers the most important theoretical foundations to develop maturity models.
Q4	How are the developed maturity models validated?	This question discovers how maturity models are validated to fit their purpose.
Q5	In what domains is maturity model research applied?	This question reveals to what extent the concept of maturity models is applicable to other domains.

- **Scope of the Study**

The overarching aim of this study is to examine the existing maturity models in information systems (IS) research. The scope of this study focuses on the articles that have been published in leading academic research on information systems, which includes journals and conference proceedings during the past six years, from 2011 until 2017. Therefore, a concept-centric approach was chosen. This is the most common approach used in a systematic review to develop and evaluate a literature review (Järvinen, 2008). Based on the concept-centric approach, the study developed a systematic classification process to identify the relevant studies in the literature.

- **Search Process**

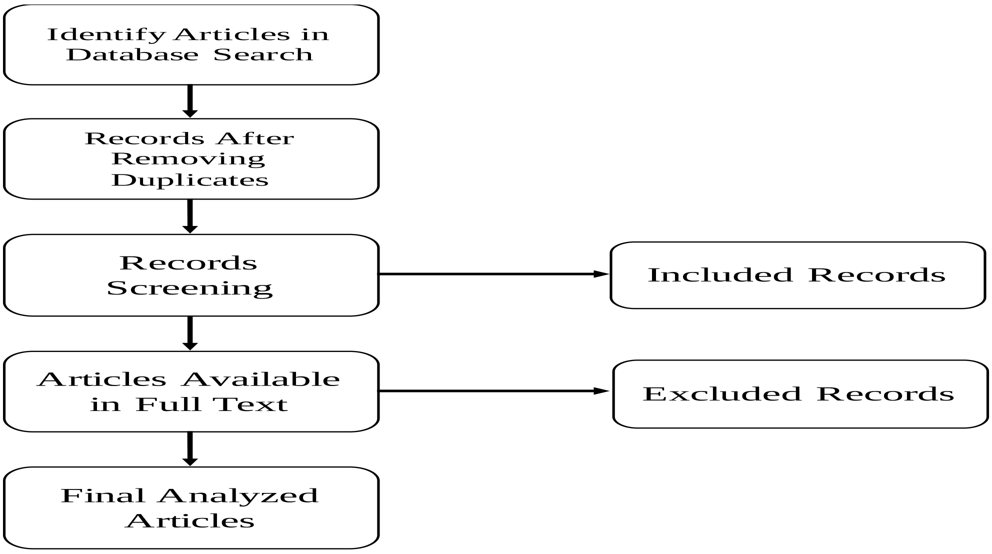

Figure 4.1. Search Process.

- **Selection of Data Sources and Search Strategy**

The main purpose of study selection is to identify those primary studies that provide direct evidence about the research question (Kitchenham & Charters, 2007). The conducted mapping study and selection of data sources were based on electronic databases. The databases selected were namely Google Scholar, Staffordshire Library resources and the Saudi Digital Library. The term "Maturity Model" is used in this search, but combinations of keywords were also tried in order to test for synonyms used in the literature and to cover a variety of maturity model publications. For all terms, the search strategy was to find the single words, for example (maturity AND model) in the title, abstract or keywords of articles. The following search terms were used:

- Model of maturity.
- Capability model.
- Process improvement model.
- Assessment model.

All these search terms were combined by using the Boolean ''OR" operator ((Maturity Model) OR (Model of maturity) OR (Capability model) OR (Process improvement model) OR (Assessment model)). This means that any sources with anyone of the search terms will be retrieved.

- **Exclusion and Inclusion Criteria**

Table 4.2. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
• Directly related to maturity model. • Maturity model development in the information system. • Peer-reviewed. • Written in English.	• Irrelevant to study of maturity model. • Not peer-reviewed papers. • White paper. • Duplicate publication. • Journals not accessible online. • Not written in English.

- **Classification Scheme**

The development of a classification scheme is important for finding the existing maturity models. A concept-centric approach was chosen for this study. It is the most common approach used in a systematic review for developing and evaluating a literature review (Järvinen, 2008). Based on this concept-centric approach, the study developed a systematic classification process to identify the relevant studies in the literature. Therefore, for structuring and analysing the identified articles, a classification scheme was developed based on systematic mapping studies in software engineering (Petersen et al., 2008), as illustrated in Figure 4.2.

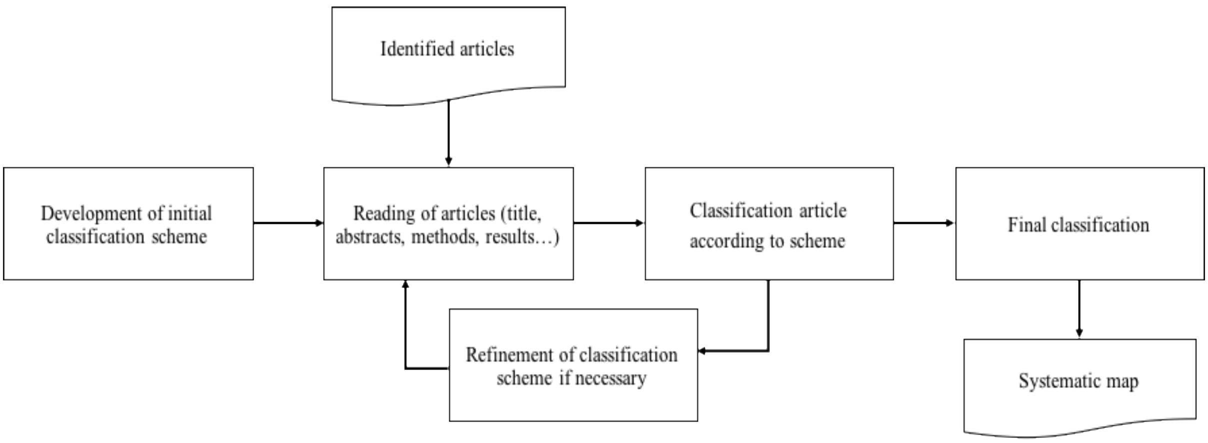

Figure 4.2. Building the Classification Scheme. Source: Petersen et al. (2008) .

To achieve the study's aims, concept categories were used to identify the final classification scheme. The concept categories used are:

- Research design.

This category includes many concepts: empirical qualitative, empirical quantitative, conceptual, design-oriented and others.

- Research method.

This category includes many concepts: case study, action research, survey, interview, focus group, Delphi study, literature review, concept development and others.

- Research content.

This category includes many concepts: concept construction, assessment, theoretical reflection, description, comparison, transfer, empirical study and others.

- Application domain.
- Developed/used maturity model.

Appendix C: Research Ethics

RESEARCH ETHICS

Proportionate Review Form

The Proportionate Review process may be used where the proposed research raises only minimal ethical risk. This research must: focus on minimally sensitive topics; entail minimal intrusion or disruption to others; and involve participants who would not be considered vulnerable in the context of the research.

PART A: TO BE COMPLETED BY RESEARCHER

Name of Researcher:	Majid Saliman H Al-Ruithe

Student/Course Details (If Applicable)			
Student ID Number:			12026575
Name of Supervisor(s)/Module Tutor:			Elhadj Benkhelifa
PhD/MPhil project:	☒		
Taught Postgraduate Project/Assignment:	☒	Award Title:	PhD Candidate
Undergraduate Project/Assignment:	☐	Module Title:	

Project Title:	A framework for strategy to design, deploy and sustain an effective cloud data governance program
Project Outline:	The aim of this study is to develop a framework for strategy to design, deploy and sustain an effective cloud data governance program. The objectives are: PHASE 1: To conduct systematic literature review to understand state of the art of data governance, that including: - Data governance for non-Cloud environments. - Data governance for Cloud environments. - Todevelopdatagovernancetaxonomy. - Existingstrategiesandframeworksforimplementingdatagovernance. - To develop a framework for strategy to design, deploy and sustain an effective cloud data governance program. – To develop Cloud data governance maturity model. – To develop methodology to implement Cloud data governance program. PHASE 2: To conduct a case study in Saudi Arabia to: -To investigate state of the art of data governance for Cloud computing including: 1. To identify barriers to implement data governance for the Cloud computing by empirical study. 2. To identify success criteria for sustaining data governance strategy for the Cloud. - Validation of the research findings through the Case Study. 1.To validate the proposed strategy framework in Saudi Arabia. 2.To validate the cloud data governance maturity model in KSA. 3.To validate the methodology to implement cloud data governance program in KSA.

Proportionate Review

	- To apply the research finding to develop a data governance programme for a selected organisation. - To develop a tool for monitoring data governance program to ensure the program is implemented according to the plan.
Give a brief description of participants and procedure (methods, tests etc.)	The researcher developed questionnaire based on the literature review. The questionnaire aims to investigate the state of data governance for non-cloud and cloud computing in the organisations of Saudi Arabia. The barriers and critical success factors that will affect data governance implementation in organisations of Saudi Arabia will be considered in the questionnaire. The questionnaire will be distributed to the targeted audiences online. The targeted audiences is the expert of cloud computing, governance and strategy in the organisations of Saudi Arabia. The questionnaire will be delivered to the respondent online by various means including post, e-mail attachments or via publishing on a web site and social media. Participation in this research study is completely voluntary. They have the right to withdraw from participation at any time. There is no need to state a reason for withdrawal. However, the proposed framework and maturity model will be validating through a case study in Saudi Arabia and will enable access to focus group comprising a strategic-level experts and stakeholders from the several different government organisations and the biggest cloud providers in Saudi Arabia. In addition, the proposed methodology to implement cloud data governance program will be validate through a case study in Saudi Arabia and will enable access to focus group comprising a strategic-level experts and stakeholders from the several different government organisations and the biggest cloud providers in Saudi Arabia.

Expected Start Date:	12/1/2015	Expected End Date:	12/1/2018

Relevant professional body ethical guidelines should be consulted when completing this form.

Please seek guidance from the Chair of your Faculty Research Ethics Committee if you are uncertain about any ethical issues arising from this application.

There is an obligation on the researcher and supervisor (where applicable) to bring to the attention of the Faculty Ethics Committee any issues with ethical implications not identified by this form.

Researcher Declaration

I consider that this project has no significant ethical implications requiring full ethical review by the Faculty Research Ethics Committee.	☒

I confirm that:		
1.	The research will **NOT** involve members of vulnerable groups. Vulnerable groups include but are not limited to: children and young people (under 18 years of age), those with a learning disability or cognitive impairment, patients, people in custody, people engaged in illegal activities (e.g. drug taking), or individuals in a dependent or unequal relationship.	☒
2.	The research will **NOT** involve sensitive topics. Sensitive topics include, but are not limited to: participants' sexual behaviour, their illegal or political behaviour, their experience of violence, their abuse or exploitation, their mental health, their gender or ethnic status. The research must not involve groups where	☒

	permission of a gatekeeper is normally required for initial access to members, for example, ethnic or cultural groups, native peoples or indigenous communities.	
3.	The research will **NOT** deliberately mislead participants in any way.	☒
4.	The research will **NOT** involve access to records of personal or confidential information, including genetic or other biological information, concerning identifiable individuals.	☒
5.	The research will **NOT** induce psychological stress, anxiety or humiliation, cause more than minimal pain, or involve intrusive interventions. This includes, but is not limited to: the administration of drugs or other substances, vigorous physical exercise, or techniques such as hypnotherapy which may cause participants to reveal information which could cause concern, in the course of their everyday life.	☒
6.	The research **WILL** be conducted with participants' full and informed consent at the time the study is carried out: • The main procedure will be explained to participants in advance, so that they are informed about what to expect. ☒ • Participants will be told their involvement in the research is voluntary. ☒ • Written consent will be obtained from participants. *(This is not required for self-completion questionnaires as submission of the completed questionnaire implies consent to participate).* ☒ • Participants will be informed about how they may withdraw from the research at any time and for any reason. ☒ • For questionnaires and interviews: Participants will be given the option of omitting questions they do not want to answer. ☒ • Participants will be told that their data will be treated with full confidentiality and that, if published, every effort will be made to ensure it will not be identifiable as theirs. ☒ • Participants will be given the opportunity to be debriefed i.e. to find out more about the study and its results. ☒	☒ N/A ☐

If you are unable to confirm any of the above statements, please complete a **Full Ethical Review Form**. If the research will include participants that are **patients,** please complete the Independent Peer Review process.

Supporting Documentation

All key documents e.g. consent form, information sheet, questionnaire/interview schedule are appended to this application.	☒

Signature of Researcher:		Date:	31/10/2016

NB: If the research departs from the protocol which provides the basis for this proportionate review, then further review will be required and the applicant and supervisor(s) should consider whether or not the proportionate review remains appropriate. If it is no longer appropriate a full ethical review form **MUST** be submitted for consideration by the Faculty Research Ethics Committee.

Next Step: STUDENTS: Please submit this form (and supporting documentation) for consideration by your Supervisor/

Module Tutor.

STAFF: Please forward this form to the Chair of Faculty Research Ethics Committee who will arrange for it to be considered by an independent member of the Faculty Research Ethics Committee.

PART B: TO BE COMPLETED BY SUPERVISOR/MODULE TUTOR (If Applicable)

I consider that this project has no significant ethical implications requiring full ethical review by the Faculty Research Ethics Committee.	☑
I have checked and approved the key documents required for this proposal (e.g. consent form, information sheet, questionnaire, interview schedule).	☑

Signature of Supervisor:	E. L[illegible]	Date:	31/10/2016

Next Step: Please forward this form to the Chair of Faculty Research Ethics Committee who will arrange for it to be considered by an independent member of the Faculty Research Ethics Committee, having no direct connection with the researcher or his/her programme of study.

PART C: TO BE COMPLETED BY FACULTY RESEARCH ETHICS COMMITTEE MEMBER

This research proposal has been considered using agreed University Procedures and is now approved.	☐
Or	
This research proposal has not been approved due to the reasons given below.	☐

Name of Reviewer:	PROFESSOR ALAN EARDLEY	Date:	2/11/2016
Signature:	W A Eardley		

Proportionate Review

Appendix D: Focus Group Guideline

Staffordshire University

Faculty of Computing, Engineering and Sciences

A Framework for Strategy to Design, Deploy and Sustain an Effective Cloud Data Governance Program

Focus Group Consent Form

By

Majid Al-Ruithe

July 2016

- **Participant Information Sheet (focus group): Cloud Data Governance.**

I would like to invite you to participate in my research project on Cloud data governance. The following will give you a short overview of what this means for you and the information you decide to give me. Before you decide it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully. Do not hesitate to talk about the study with other people.

- **Why am I doing this research?**

Although there have been some studies on data governance, the particular area of data governance for cloud computing services has not been examined in close detail in general and in Saudi Arabia. I am interested in this study because the loss data governance is one of top concerns to adopt cloud computing. Also because the Kingdome of Saudi Arabia has plan to adopt cloud computing in its organisations. In my study, I develop framework for strategy to understand how to design, deploy and sustain cloud data governance program. In the focus group I would like to validate this framework.

- **Who can take part?**

I am approaching people who have been experts in the strategy process, data governance and cloud computing in government organisations and cloud provider's companies.

- **What would be involved?**

If you choose to participate I would like to discuss your views on the phases and process in the proposed framework. This would last between 2 and 3 hours. I would like to talk to you about the following topics:
1- What aims of this framework?
2- What means each phase in the proposed framework?
3- How to implement the proposed framework?

What will I do with the information?

I will transcribe the interview and if you are interested I will give you a copy of the transcript. The transcript will only be read and used by me and not be used for any other purpose. The information from these discussions will be the basis of my PhD thesis which will be assessed in order for me to gain the PhD degree. The transcripts might also be used to write and publish articles in academic journals. You are welcome to see the final thesis and/ or a copy of the articles before they are published.

- **Will everything you say to me be kept private?**

You can say as little or as much as you wish. The transcript will be kept in a secure place. In the transcript the names of yourself as well as those people who you mention will be changed so you will not be identifiable.

- What if you change your mind about taking part?

If you decide to take part then this is your voluntary decision, therefore you are also free to withdraw from the study at any point you wish, without giving a reason.

- **Who am I?**

My name is Majid Al-Ruithe and I am a PhD student at Staffordshire University. I am supervised by two Senior Research Professors in the School of Computing. The research has the approval of the school research ethics committee and is jointly funded by the Internal of Ministry and Saudi Culture Bureau in London. If you would be interested in taking part or have any questions concerning the research, feel free to contact me at Tel: 00966598343504 or email: majid.al-ruithe@staff.ac.uk. I would be happy to answer any questions and look forward to meeting you in focus group.

Consent Form: Cloud Data Governance.

Name of Researcher: Majid Al-Ruithe

	Please Initial
1. I confirm that I have read and understood the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	
2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason.	
3. I agree to take part in the study.	

Name of participant.................................. Date................. Signature....................

Name of person taking consent...................Date................Signature.....................

2 copies: 1 for participant and 1 for research file.

FOCUS GROUP: DEMOGRAPHIC DETAILS QUESTIONNAIRE

Please answer the following questions in the spaces provided, circle or tick the most appropriate options.

1. Name: ………………………………………………………………………………

2. What is your professional background?

- ○ Chief executive officer (CEO)
- ○ Chief Information Officer (CIO)
- ○ Vice President
- ○ Senior Manager
- ○ IT Manager
- ○ Business Manager
- ○ Cloud Computing Manager
- ○ Team Leader
- ○ Other (please specify) ___________________________________

3. How many years of experience have you had in this current job?

□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years

4. Experience in develop strategy (optional):

□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years

5. Experience in Cloud computing (optional):

□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years

What is cloud types/ delivery models do you have experience?…………………………

6. Experience in data governance aspects (optional):

□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years

What is aspect of data governance do you have experience?……………………………………………………………………………………
………

Signature……………….

Thank you for taking the time to complete this questionnaire

FOCUS GROUP: DISCUSSION GUIDE

Facilitator's welcome, introduction and instructions to participants

Welcome and thank you for volunteering to take part in this focus group. You have been asked to participate as your point of view is important. I realize you are busy and I appreciate your time.

Introduction: This focus group discussion is designed to validate a framework for strategy to design, deploy and sustain an effective cloud data governance program. The focus group discussion will take no more than two hours.

Anonymity: Despite being taped; I would like to assure you that the discussion will be anonymous. The tapes will be kept safely in a locked facility until they are transcribed word for word, then they will be destroyed. The transcribed notes of the focus group will contain no information that would allow individual subjects to be linked to specific statements. You should try to answer and comment as accurately and truthfully as possible. I and the other focus group participants would appreciate it if you would refrain from discussing the comments of other group members outside the focus group. If there are any questions or discussions that you do not wish to answer or participate in, you do not have to do so; however please try to answer and be as involved as possible.

Ground rules

- The most important rule is that only one person speaks at a time. There may be a temptation to jump in when someone is talking but please wait until they have finished.
- There are no right or wrong answers
- You do not have to speak in any particular order
- When you do have something to say, please do so. There are many of you in the group and it is important that I obtain the views of each of you
- You do not have to agree with the views of other people in the group
- Does anyone have any questions? (answers).
- OK, let's begin

Warm up

- First, I'd like everyone to introduce themselves. Can you tell us your name?

Introductory question

I am just going to give you a couple of minutes to think about your experience of providing strategy, cloud computing and data governance/ general governance to your organisation. Is anyone happy to share his or her experience?

Guiding questions

1. Which phases in the framework do you feel would be helpful in terms of supporting the strategy for implementing cloud data governance program?
2. Are there any phases in the framework which you feel would not be helpful in terms of supporting the strategy for implementing cloud data governance program?

3. Which elements in the framework phases do you feel would be helpful in terms of supporting the strategy for implementing cloud data governance program?
4. Are there any elements in the framework phases which you feel would not be helpful in terms of supporting the strategy for implementing cloud data governance program?
5. Are there any changes you would suggest to improve the framework?

Concluding question

Of all the things we've discussed today, what would you say are the most important issues you would like to express about this checklist?

Conclusion

Thank you for participating. This has been a very successful discussion

Your opinions will be a valuable asset to the study

We hope you have found the discussion interesting

If there is anything you are unhappy with or wish to complain about, please contact the local PI or speak to me later

I would like to remind you that any comments featuring in this report will be anonymous

Before you leave, please hand in your completed personal details questionnaire

Please, write your report based on the results of the focus group. Please remember to maintain confidentiality of the participating individuals by not disclosing their names.

Appendix E: Questionnaire

Cloud Data Governance

Questionnaire

Majid Al-Ruithe

10 October 2016

Informed Consent Form

Introduction:

This study attempts to collect information about data governance and cloud data governance; state of order, barriers and critical success factors. Data governance is defined as "*the framework for decision rights and accountabilities to encourage desirable behavior in the use of data. To promote desirable behavior, data governance develops and implements corporate-wide data policies, guidelines, and standards that are consistent with the organization's mission, strategy, values, norms, and culture*".

Procedures:

This questionnaire consists of different types of questions, and will take approximately 20 minutes. The data collected from this study is solely for the purposes of studying data governance for traditional IT and cloud computing in Saudi Arabia.

Confidentiality:

Data collection is anonymous and confidential, no personal details are required and hence individuals will be non-identifiable. The collected data will be used for research purposes only. Participation in this research study is completely voluntary, you have the right to withdraw from participation at any time. There is no requirement to state a reason for withdrawal. An email address is required only if you wish to be informed about the findings of this study.

Copyright:

Participation Agreement:

By completing this survey, I confirm that I am happy to take part in the above mentioned research study. I have read and understood the related Information Sheet, and am able to ask questions for further clarifications. I understand that my participation in this study in totally voluntary, and I have the right to withdraw at any time without providing reasons, and without my rights being affected. I also understand that should I provide my email address, it will only be accessible to the researcher, the project supervisor and the project assessor.

Researcher Information:
If you require further information about this research, please contact the researcher on:
Mr. Majid Al-Ruithe
PhD Researcher at School of Computing- Staffordshire University- UK
majid.al-ruithe@research.staffs.ac.uk
+447479471119
+966598343504

- ○ **I have read and understand the terms above. I agree to complete this survey.**
- ○ **I don't want to complete this survey.**

Section 1: **Demographic Information (All participants)**

What is the size of your organization?	Please tick one answer: ○ More than 5,000 employees ○ 1,000 - 5,000 employees ○ 100 - 1,000 employees ○ Less than 100 employees
Please indicate what sector your organisation belong in:	Please tick one answer: ○ Military sector ○ Financial services sector ○ Healthcare sector. ○ Petrochemical Industries Sector ○ Energy & Utilities Sector ○ Telecommunication & Information Technology Sector ○ Investment Sector ○ Other (please specify)
Please indicate your role in your organisation:	Please tick one answer: ○ Top Level Executive. ○ Senior Vice President. ○ Vice President. ○ IT Manager ○ Cloud Computing Manager ○ Professional ○ Administrative/Support personnel. ○ Data governance Manager. ○ Other (please specify)
Please indicate what is the type of department you work in:	Please tick one answer: ○ IT ○ Administrative ○ Legal. ○ Finance. ○ Project Management office ○ Data Governance Office. ○ Operations ○ Research & Development ○ Other (please specify)
How long have you been working in this job? (in years)	Please tick one answer: ○ Less than 2 years ○ Between 2 and 5 years ○ Between 5 and 10 years

	○ More than 10 years
What is the level of your Experience in data governance? (in years): * (Either in Data Governance or any related fields)	Please tick one answer: ○ No experience and knowledge on data governance. ○ No experience but good knowledge about data governance. ○ Less than 2 years ○ Between 2 and 5 years. ○ Between 5 and 10 years. ○ More than 10 years.
What is the level of your Experience in cloud computing? (in years):	Please tick one answer: ○ No experience and knowledge on Cloud Computing. ○ No experience but good knowledge about Cloud Computing. ○ Less than 2 years ○ Between 2 and 5 years ○ Between 5 and 10 years ○ More than 10 years
What kinds of technology services do you use within your organisation?	Please tick one answer: ○ Traditional IT. ○ Cloud Computing. ○ Both. ○ Other.

Section 2: Data Governance

Let's start with definition of data governance:
Data governance is the framework for decision rights and accountabilities to encourage desirable behavior in the use of data. To promote desirable behavior, data governance develops and implements corporate-wide data policies, guidelines, and standards that are consistent with the organization's mission, strategy, values, norms, and culture.

Is this definition agreeing with the concept of data governance in your organisation?	Please tick one answer: ○ The definition is essentially the same in my organisation ○ My organisation has another definition. ○ My organisations have no definition for data governance

	○ Don’t know.
How do you understand the importance of implementing data governance programme in your organisation?	Please tick one answer: • Important • No Important • Don't Know

- Do you agree that each of the following is the benefits to implement data governance in organisation?

	Essential	Very Valuable	Valuable	Somewhat Valuable	Not at all valuable
Data can be a strategic asset.					
Data governance ensures trusted and used of data to make decisions.					
Data Governance can ensure data quality.					
Data Governance can ensure policy compliance.					
Data Governance can ensure repeatable business processes.					
Data Governance can ensure cross functional collaboration.					
Data Governance can ensure change awareness throughout the organisation.					
Governance leverages data to achieve operational goals.					
Cost issues can be reduced by data governance.					
Making data consistent.					
Data governance can be Improving business planning.					
Data governance can be improving financial performance.					

Section 3: Cloud Computing

A. The current state of cloud computing in the organisations:

Has your organisation adopted cloud computing?	Please tick one answer: o Yes o No. o Don't know.

1. If Yes, please answer the questions:

What type of cloud computing is your organisation already using, or implementing? Please select all that apply:	Please select all that apply: o Public Cloud o Private Cloud o Hybrid Cloud o Community Cloud. o Internal cloud. o Other o Don't know.
Which cloud computing service models are you already using or implementing, or plan to implement? Please tick all that apply:	Please tick one answer: o Software-as-a-Service o Platform-as-a-Service o Infrastructure-as-a-Service o Don't know. o Other
What percentage of your organisation's data is stored in the cloud environment? Please tick one answer:	Please tick one answer: o None stored. o Less than 1%. o Between 1% to 10%. o Between 11% to 25%. o Between 26% to 50%. o Between 51% to 75%. o Between 76% to 100%. o Don't know
What percentage of your organisation's data stored in the cloud environment is not managed or controlled by your organisation's specialist? Please tick one answer:	Please tick one answer: o No store. o Less than 1%. o Between 1% to 10%. o Between 11% to 25%. o Between 26% to 50%. o Between 51% to 75%.

	○ Between 76% to 100%. ○ Don't know
Does your organisation classify its data based on sensitivity? Please tick one answer:	Please tick one answer: ○ Yes. what type of data. ○ No. ○ Don't know
How does your organisation educate employees about cloud application risks? Please tick one answer:	Please tick one answer: ○ General data security training without specific discussion about cloud applications. ○ General data security training includes discussion of cloud applications. ○ Informal awareness effort. ○ Specialized training for each cloud application. ○ Other.
What type of knowledge/expertise is lacking within your organisation regarding cloud computing? Please tick multiple answer:	Please tick multiple answer: ○ Security. ○ Data protection. ○ Develop SLA. ○ Legal ○ Technology and implementation ○ Cloud computing market ○ Compliance ○ cloud governance ○ IT governance ○ Data governance ○ Other
What aspects of cloud computing should be improved? Please tick multiple answer:	Please tick multiple answer: ○ Security. ○ Integration with existing IT. ○ Privacy. ○ Transparency of architecture. ○ Transparency of cost models. ○ Availability. ○ Escrow. ○ Functionality/customization. ○ Performance. ○ Cloud governance. ○ Data governance.

	○ Other.

- **Which of the following is relevant to your organisation?**

Attributions about the cloud	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
My organisation is committed to protecting confidential or sensitive data in the cloud.					
My organisation has established clearly defined roles and accountabilities for safeguarding confidential or sensitive data stored in the cloud.					
My organisation is careful about sharing confidential or sensitive data with third parties such as business partners, contractors, and providers in the cloud environment.					
My organisation is proactive in managing compliance with privacy and data protection regulations in the cloud environment.					
It is more complex to manage privacy and data protection regulations in a cloud environment than on premise networks within my organization.					
My organization educates employees about safeguarding sensitive or confidential data when using cloud applications.					
My organisation follows cloud regulations from government.					

2. **<u>If No, please answer the questions:</u>**

What is your organisation's plan for cloud computing services adoption?	Please tick one answer: ○ We intend to adopt cloud computing services in the next 6 months.

	○ We intend to adopt cloud computing services in the next 1 year ○ We intend to adopt cloud computing services in the next 2 years. ○ We do not intend to adopt cloud computing services at this time. ○ I do not know
What is the biggest barrier to cloud computing adoption? Please tick multiple answer:	Please tick multiple answer: ○ Lack of Knowledge. ○ Lack of staff's skills. ○ Resistance to change. ○ Lack of Top management support. ○ Technical. ○ Organisation culture. ○ Cost ○ Data security ○ Lack of trust ○ Non-controllable externalities ○ Lack of government regulations. ○ Loss of data governance. ○ Other.

B. Cloud Computing Concern

- What level of concern to your organisation does the adoption of cloud computing offer?

	Extremely no concern	No concern	Neither concern	Concern	Extremely high concern
Security issues					
Legal issues					
Compliance issues					
Privacy issues					
Trust issues					
Integration issues					
Insecure availability					
Vendor lock-in					
Loss of data governance					
Loss of control					
Lack of performance					
Lack of functionalities					
Not know where their					

data is being held					
Immature Cloud Computing					
Vendor lock-in					
Insufficient financial benefits.					

<u>Section 4:</u> Cloud Data Governance

A. The current state of cloud data governance in the organisations:

Do you think the cloud computing bring new data governance issues compared to traditional infrastructure?	Please tick one answer: o Yes. o No. o Don't know.
Does your organisation implement cloud data governance programme?	Please tick one answer: o Yes. o No. o Don't know.

<u>If Yes, please answer the questions:</u>

Which of the following best characterizes cloud data governance processes within your organisation?	Please tick one answer o Non-existent: data governance processes for the Cloud are not applied, and the institution has not recognized the need for them. o Initial: data governance processes for the Cloud are informal and uncoordinated. o Repeatable: data governance processes for the Cloud follow a regular pattern. o Defined: data governance processes for the Cloud are documented and communicated. o Managed: data governance processes for the Cloud are monitored and measured. o Optimized: data governance best practices for the Cloud are followed, and there are provisions for amending processes.

1- **<u>If No, please answer the questions</u>:**

What is your organisation's plan for cloud data governance programme implementation?	Please tick one answer: ○ We intend to implement cloud data governance programme in the next 6 months. ○ We intend to implement cloud data governance programme in the next 1 year ○ We intend to implement cloud data governance programme in the next 2 years. ○ We do not intend to implement cloud data governance programme at this time. ○ I do not know

B. Barriers for implementing Cloud data governance.

- **Do you agree that each of the following is a barrier to implement cloud data governance in an organisation?** Please rate your level of agreement with the following statements:

	Please rate your level of agreement with the following statements:				
	Strongly Disagree	Generally Disagree	Neither disagree or Agree	Generally Agree	Strongly Agree
Lack of financial resources					
Cloud Data governance has a low priority compared to other projects.					
Inability to communicate the business value of Cloud data governance.					
Cost as major barriers to the implementation of cloud data governance.					
Cloud data governance is perceived as too complex.					
Not knowing where to start.					
Lack of focus on Cloud data					

governance policies within the organisation					
Lack of focus on Cloud data governance procedures within the organisation					
Lack of focus on Cloud data governance processes within the organisation					
Lack of focus on defined roles and responsibilities for cloud actors within the organisation					
Lack of focus on identified priorities of Cloud data governance within the organisation					
Lack of focus on Cloud data governance charter, mission, vision within the organisation					
Lack of focus on Cloud data governance communication plan within the organisation					
Lack of focus on Cloud data governance change management plan within the organisation.					
Lack of focus on Cloud data governance communication plan within the organisation					
Lack of knowledge for understanding Cloud data governance within the organisation					
Lack of training on Cloud data governance in the organisation					
Lack of of understand how to create communication plan for Cloud data governance in organisations.					
Lack of Cloud data governance office in the organisation.					
Cloud data governance is not part of organisation culture.					
Lack of understand how to build Cloud data governance matrices and					

measure in the orgonisation.					
Don't get data as a strategic asset in the orgonisation when it moves to cloud computing.					
Cloud data governance is not priority in the organisation.					
Lack of People and politics that support implementing Cloud data governance in the organisation.					
Lack of executive and stakeholder support implement Cloud data governance in the organisation.					
Lack of compliance enforcement					
Lack of funding for implement Cloud data governance in the organisation.					
Lack of technology that use to implement and monitor Cloud data governance in the organisation.					
Cloud data governance is not build into service level agreement of cloud computing service with cloud provider.					
Lack of people have skills and experience to implement Cloud data governance in the organisation.					
Lack of time to implement Cloud data governance in the organisation.					
Compliance hazard					
Complexity of storage and processing data in the cloud.					
Cloud computing not quite adopt in the orgonisation.					
Complex cloud deployment models.					
Complex cloud service delivery models.					

Lack of simple mechanisms to assess the trustworthiness of potential partners.					
Complexity of the business relationship between multiple parties.					
Complexity of the business relationship between multiple parties.					

- **Do you think there are other important barriers have not mentioned here?**
  - Yes, what are they please?
  - No
  - Don't know

C. **Critical success factors to implement Cloud data governance in the organisations:**

- **Do you agree that each of the following is the critical success factors to implement Cloud data governance at orgonisation?**

	Please rate your level of agreement with the following statements:				
	Neither critical nor important	Important not critical	Somewhat critical and important	Critical and important	Extremely critical and important
Adequate analysis, evaluation of the current of Cloud data governance					
Set up Clear Cloud data governance policies					
Set up Clear Cloud data governance procedures					
Set up Clear Cloud data governance processes					
Set up Clear Cloud data governance structure					
Defined Clear roles and responsibilities for cloud actors.					
Creating strong cloud data governance methodology.					

Identified and articulated priorities to implement cloud data governance in the organisation.					
Set up Clear cloud data governance structure.					
Set up Clear Cloud data governance mission.					
Set up Clear cloud data governance vision					
Set up Clear communication plan to implement cloud data governance.					
Defining business case for cloud data governance					
Set up Clear change management plan to implement cloud data governance.					
Clear definition of data value					
Clear classify data in the cloud.					
training and education organisation staffs on cloud data governance programme.					
Regular communication with all cloud data governance participants.					
Use the strengths of the existing culture to the Cloud data governance programme advantage.					
measured and reported for continuous improvement of cloud data governance.					
Ongoing funding for cloud data governance requirements					
Automation cloud data governance.					
Built cloud data governance into service level agreement of Cloud computing project.					
Improve staffs Skills and experience on cloud data governance.					
Top management support cloud data governance implemention.					
Establish cloud data governance council, office and committee					

Support Compliance enforcement to implement cloud data governance.					
Fellow the principle of corporate Governance					
Regulatory environment & compliance requirements to support cloud data governance implementation.					
Create clear Risk Management Strategy.					
Leadership and commitment of top management to the adoption of risk management strategy for the organisation.					
Data risk in cloud computing is assessed and managed on time.					
Involvement all stakeholders in cloud data governance					
Involvement cloud provider in cloud data governance					
Involvement other cloud actors in cloud data governance(Cloud broker, Cloud auditor, Cloud carrier).					
Involvement board of directors & top management support and ownership to support implement cloud data governance.					
Integrate with cloud deployment models features.					
Integrate with cloud service delivery models features.					
Effective alignment between cloud data governance and Cloud computing regulation.					
Effective alignment between cloud data governance and organisation strategy.					
Effective alignment between cloud data governance and business strategy.					
Effective alignment between cloud data governance and IT strategy.					
Effective alignment between cloud data governance and environmental strategy.					

Effective alignment between cloud data governance and corporate governance.					
Effective alignment between cloud data governance and IT governance.					
Effective alignment between cloud data governance and others strategy.					

- **Do you think there are other important critical success factors have not mentioned here?**
  - Yes, what are they please?
  - No
  - Don’t know

Appendix F: Awards

Appendix J: Framework Validation Questions

Staffordshire University
Faculty of Computing, Engineering and Sciences

A Strategy Framework to Design, Deploy and Sustain an Effective Cloud Data Governance Programme

By
Majid Al-Ruithe

July 2016

Section A: Respondents Background
Please select the answer which best describes your organization:
A) Government organisation.
B) Cloud Service Provider.
Please specify your organisation size of employees?
More than 5,000
1,000 - 5,000
100 - 1,000
Less than 100
How many years of experience have you had in this current job?
□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years

Your experience in develop strategy (optional):
□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years
Your experience in Cloud computing (optional):
□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years

What is cloud types/ delivery models do you have experience?private cloud/ email as a service...
....
....
Your experience in governance aspects (optional):
□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years

What is aspect of governance do you have experience?..policy for use local network..
....
....
Email address: ………………………………………………..
What is your job role?...

Have been ever involved in any strategy project? Yes/No
If yes, what was your role in this project? …
……………………………………………………………………………………………
……………………………………………………………………
Have been ever involved in any cloud computing project? Yes/No
If yes, what was your role in this project? …
……………………………………………………………………………………………
……………………………………………………………………

Have been ever involved in any governance project? Yes/No
If yes, what was your role in this project? …
………………………………………………………………………………………
…………………………………………………………………

Section B: A Strategy Framework to Design, Deploy and Sustain an Effective Cloud Data Governance Programme.

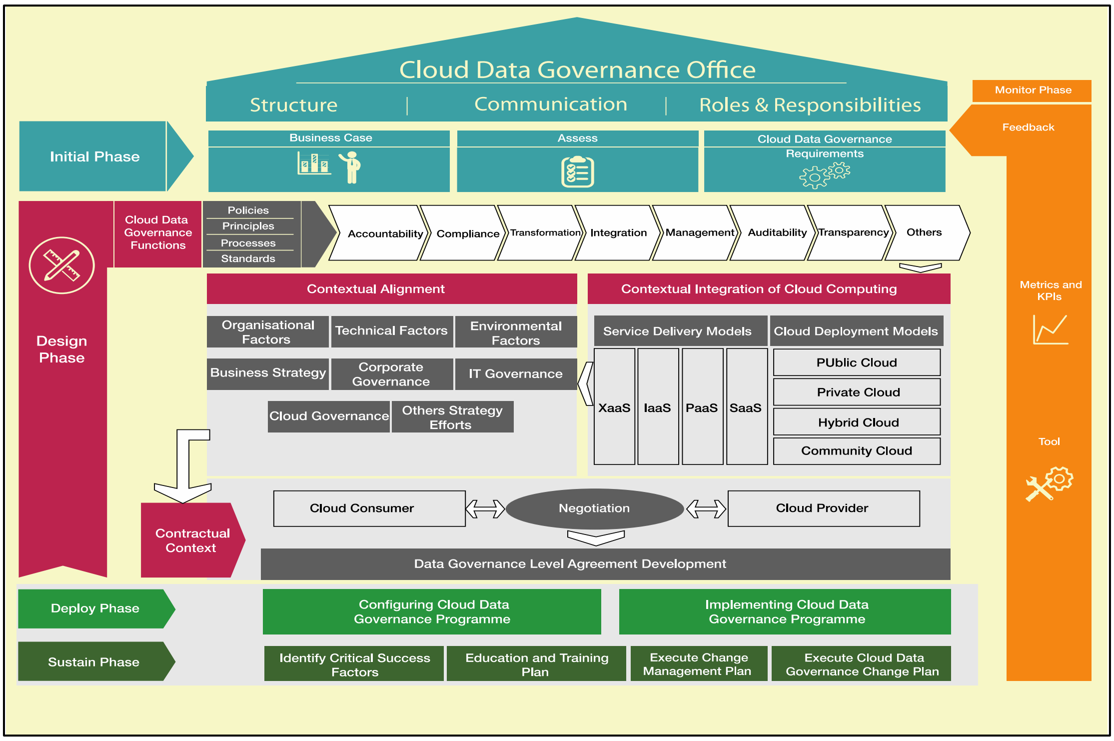

Figure 1: Strategy Framework for Developing Cloud Data Governance programme.

Please Rate the extent to which you agree or disagree with the following statements

Please Rate the extent to which you agree or disagree with the following statements	1= strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree				
	1	2	3	4	5
The framework provides a strategy to design, deploy and sustain an effective cloud data governance programme?					
The Framework supports organizational learning and innovation?					
The framework provides a structured methodology for supporting decision making to understand important processes to implement cloud data governance programme?					
Using the framework would reduce the cost, time and effort involved in the cloud data governance process?					
The framework provides a mechanism for reducing loss of data governance in cloud computing?					
The framework helps government organization to					

implement its cloud data governance programme?					
The initial phase is crucial to support important process to understand of cloud data governance requirements?					
The design phase is crucial to support important process to design cloud data governance programme?					
The deployment phase is crucial to support important process to implement cloud data governance programme?					
The monitoring phase is crucial to support important process to ensure cloud data governance programme in right direction?					
The sustain phase is crucial to support important process to ensure cloud data governance programme on-going long term?					
The framework helps government organizations to get control on their data into cloud computing environment?					
The framework helps government organizations to adopt cloud computing?					

Which phases in the framework do you feel would be helpful in terms of supporting the strategy for implementing cloud data governance programme?
…………………………………………………………………………………………………
…………………………………………………………………………………………………
……………………………………………………………

Are there any phases in the framework which you feel would not be helpful in terms of supporting the strategy for implementing cloud data governance programme?
…………………………………………………………………………………………………
…………………………………………………………………………………………………
……………………………………………………………

- **Initial phase**

Please Rate the extent to which you agree or disagree with the following statements	1= strongly agree 2= Agree 3= Neutral 4= disagree 5= strongly disagree				
	1	2	3	4	5
Establish data governance office.					
Build structure for data governance office					
Develop communication plan between data governance office team					
Establish data governance roles and responsibilities					
Define data governance business case					
Set up a data governance assessment guide					
Define data governance requirements					

Which elements in the initial phase do you feel would be helpful in terms of supporting the strategy for implementing cloud data governance programme?
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………

Are there any elements in the initial phase which you feel would not be helpful in terms of supporting the strategy for implementing cloud data governance programme?
………………………………………………………………………………………………
………………………………………………………………………………………………
…………………………………

- **Design phase**

Please Rate the extent to which you agree or disagree with the following statements	1= strongly agree 2= Agree 3= Neutral 4= disagree 5= strongly disagree				
	1	2	3	4	5
Establish Cloud data governance functions					
Integrate data governance functions within the Cloud computing context					
Align data governance functions with other strategy efforts in the organisation.					
Establish a negotiating contract between cloud provider and consumer for Cloud data governance					
Develop data governance level agreement.					

Which elements in the design phase do you feel would be helpful in terms of supporting the strategy for implementing cloud data governance programme?

………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………
Are there any elements in the design phase which you feel would not be helpful in terms of supporting the strategy for implementing cloud data governance programme?
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………

- **Deploy phase**

Please Rate the extent to which you agree or disagree with the following statements	1= strongly agree 2= Agree 3= Neutral 4= disagree 5= strongly disagree				
	1	2	3	4	5
Configuring Data Governance Activities					

Implementing Data Governance Programme					

Which elements in the deploy phase do you feel would be helpful in terms of supporting the strategy for implementing cloud data governance programme?
…………………………………………………………………………………………………
…………………………………………………………………………………………………
……………………………………………………………

Are there any elements in the deploy phase which you feel would not be helpful in terms of supporting the strategy for implementing cloud data governance programme?
…………………………………………………………………………………………………
…………………………………………………………………………………………………
……………………………………………………………

- **Sustain phase**

Please Rate the extent to which you agree or disagree with the following statements	1= strongly agree 2= Agree 3= Neutral 4= disagree 5= strongly disagree				
	1	2	3	4	5
Identify Critical Success Factors (CSFs)					
Define / update Communication Plan					
Establish / update Education and Training Plan					
Execute Change Management Plan					
Execute Data Governance Change Plan					

Which elements in the sustain phase do you feel would be helpful in terms of supporting the strategy for implementing cloud data governance programme?
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………
Are there any elements in the sustain phase which you feel would not be helpful in terms of supporting the strategy for implementing cloud data governance programme?
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………

- **Monitor Phase**

Please Rate the extent to which you agree or disagree with the following statements	1= strongly agree 2= Agree 3= Neutral 4= disagree 5= strongly disagree				
	1	2	3	4	5
Establish Data Governance Metrics and KPIs					
Establish an automated data governance tool based on					

modern technology to monitor Cloud data governance activities.					

Which elements in the initial phase do you feel would be helpful in terms of supporting the strategy for implementing cloud data governance programme?
………………………………………………………………………………………………
………………………………………………………………………………………………
…………………………………………………………

Are there any elements in the initial phase which you feel would not be helpful in terms of supporting the strategy for implementing cloud data governance programme?
………………………………………………………………………………………………
………………………………………………………………………………………………
…………………………………………………………

Are there any changes you would suggest to improve the framework?
………………………………………………………………………………………………
………………………………………………………………………………………………
…………………………………………………………

Please rate the following aspects of the framework.

Please rate the following aspects of the framework	1 = Very strong 2= Strong 3= Natural 4= Weak 5= Very weak				
	1	2	3	4	5
Ease to use					
Ease to Learn					
Clarity					
Comprehensiveness					
Usefulness					
Practicality					

Signature……………………………..

Appendix H: Maturity Model & Assessment Matrix Evaluation

Staffordshire University
Faculty of Computing, Engineering and Sciences

Cloud Data Governance Maturity Model and Assessment Matrix Evaluation (Focus Group)

By
Majid Al-Ruithe

June 2017

Participant Information Sheet (focus group): Cloud Data Governance Maturity Model.

I would like to invite you to participate in my research project on Cloud data governance. The following will give you a short overview of what this means for you and the information you decide to give me. Before you decide it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully. Do not hesitate to talk about the study with other people.

Why am I doing this research?

Although there have been some studies on data governance, the particular area of data governance for cloud computing services has not been examined in close detail in general and in Saudi Arabia. I am interested in this study because the loss data governance is one of top concerns to adopt cloud computing. Also because the Kingdome of Saudi Arabia has plan to adopt cloud computing in its organisations. In my study, I develop framework for strategy to understand how to design, deploy and sustain cloud data governance programme. Based on this framework I develop cloud data governance maturity model, and assessment matrix to assess the cloud data governance in the organisation. In the focus group I would like to evaluate maturity model, and assessment matrix.

Who can take part?

I am approaching people who have been experts in the strategy process, data governance and cloud computing in government organisations, cloud provider's companies and academia.

What would be involved?

If you choose to participate I would like to discuss your views on the maturity model and assessment matrix devlopment. This would last between 2 and 3 hours. I would like to talk to you about the following topics:
1- What aims of this maturity model and assessment matrix?
2- What means each construct in the maturity model?
3- How to implement the maturity model?
4- How to assess the cloud data governance based on the assessment matrix?

What will I do with the information?

I will transcribe the interview and if you are interested I will give you a copy of the transcript. The transcript will only be read and used by me and not be used for any other purpose. The information from these discussions will be the basis of my PhD thesis which will be assessed in order for me to gain the PhD degree. The transcripts might also be used to write and publish articles in academic journals. You are welcome to see the final thesis and/ or a copy of the articles before they are published.

Will everything you say to me be kept private?
You can say as little or as much as you wish. The transcript will be kept in a secure place. In the transcript the names of yourself as well as those people who you mention will be changed so you will not be identifiable.
What if you change your mind about taking part?

If you decide to take part then this is your voluntary decision, therefore you are also free to withdraw from the study at any point you wish, without giving a reason.

Who am I?

My name is Majid Al-Ruithe and I am a PhD student at Staffordshire University. I am supervised by two Senior Research Professors in the School of Computing. The research has the approval of the school research ethics committee and is jointly funded by the Internal of Ministry and Saudi Culture Bureau in London. If you would be interested in taking part or have any questions concerning the research, feel free to contact me at Tel: 00966598343504 or email: majid.al-ruithe@research.staffs.ac.uk. I would be happy to answer any questions and look forward to meeting you in focus group

	Please Initial
I confirm that I have read and understood the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	
I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason.	
I agree to take part in the study.	

Name of participant…………………………. Date……………. Signature………………
Name of person taking consent………………Date……………Signature……………….
2 copies: 1 for participant and 1 for research file.

Section A: Respondents Background
Please specify your organisation size of employees?
More than 5,000
1,000 - 5,000
100 - 1,000
Less than 100
What is your job role?...
How many years of experience have you had in this current job?
□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years
How many years of your experience in develop strategy?
□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years
How many years of your experience in Cloud computing?
□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years
How many years of your experience in governance aspects?
□ <1 Year □ 1-2 Years
□ 2-5 Years □ 5-10 Years
□ >10 Years
What is aspect of governance do you have experience?
....
....
....
Have been ever involved in any strategy project? Yes/No. If yes, what was your role in this project?
…………………………………………………………………………………………
……………………………………………………………………
Have been ever involved in any cloud computing project? Yes/No.If yes, what was your role in this project?
…………………………………………………………………………………………
……………………………………………………………………
Have been ever involved in any governance project? Yes/No. If yes, what was your role in this project?
…………………………………………………………………………………………
…………………………………………………………………
Has your organisation use any maturity model? Yes/No. If yes, what was your role in this project?
…………………………………………………………………………………………
Email address(optional): …………………………………………….
Signature……………………………..
Date:………………………………………….……

Section B: Cloud Data Governance Maturity Model

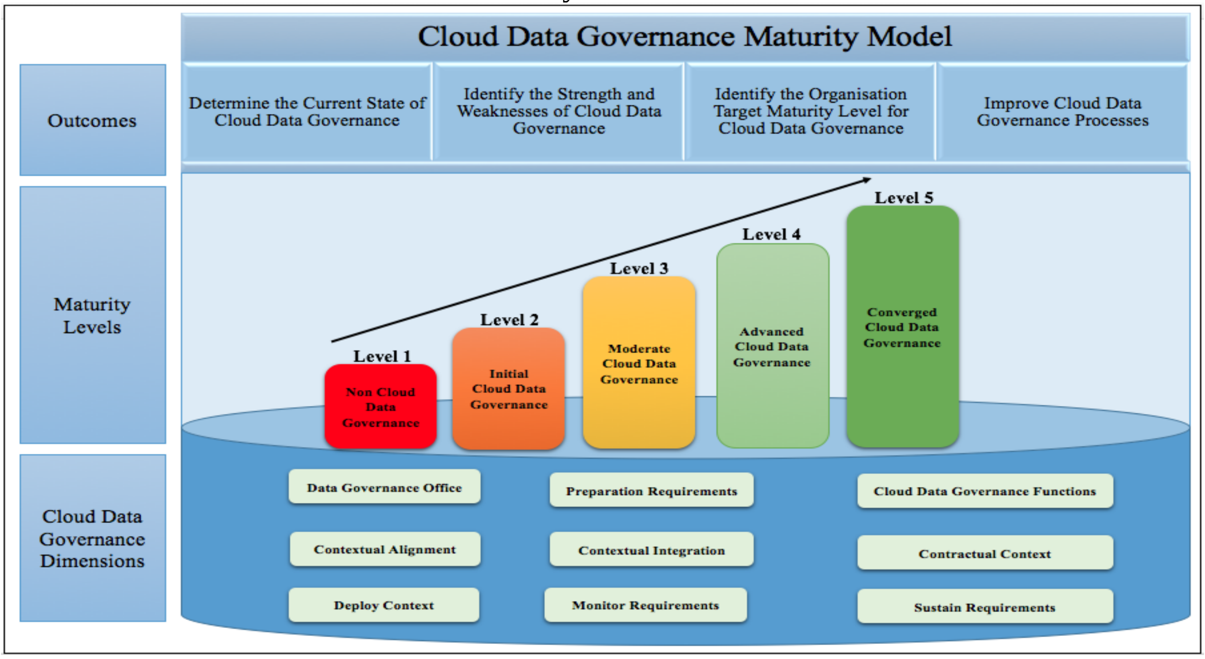

Figure 1: cloud data governance maturity model.

Evaluation criteria:

- **Completeness**

Please rate the extent to which you agree or disagree with the following statements for evaluate the cloud data governance maturity model completeness:		1= Strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree				
Sub-criteria	Statement	1	2	3	4	5
Scope	The model provides a maturity model for cloud data governance.					
Definitions	The model clearly defined the maturity level for assess the dimensions in the cloud data governance framework.					
Definitions	The model clearly defined dimensions in the cloud data governance framework which require to assess cloud data governance in the organisation.					
Definitions	The maturity levels have the right name to assess the cloud data governance in the organisation.					
Perceived Completeness	The cloud data governance maturity model and assessment method are complete and recognizable as adaptation of existing standards, models and methods for the cloud data governance.					

- **Consistency**

Please rate the extent to which you agree or disagree with the following statement for evaluate the cloud data governance maturity model consistency:		1= strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree				
Sub-criteria	Statement	1	2	3	4	5
Internal Consistency	There is consistent level of abstraction, granularity, and detail given within the cloud data governance maturity model.					

- **Practicality**

Please rate the extent to which you agree or disagree with the following statement for evaluate the cloud data governance maturity model practically:		1= strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree				
Sub-criteria	Statement	1	2	3	4	5
Ease of use	The cloud data governance maturity model is easy to use.					
Ease of use	The cloud data governance maturity model is easy to learn.					
Understandable	The cloud data governance maturity model process is simple to understand with its practices are clearly defined.					
Practical utility	The cloud data governance maturity model practice guidelines provide utility for the organisation.					
Tailorable	The cloud data governance maturity model process are flexible, tailorable and adaptable.					

- **Usefulness**

Please rate the extent to which you agree or disagree with the following statement for evaluate the cloud data governance maturity model usefulness:		1= Strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree				
Sub-criteria	Statement	1	2	3	4	5
Perceived benefits	The cloud data governance maturity model process is likely to be useful in assessing and improving the cloud data governance processes in the organisation.					
Constructiveness	The cloud data governance maturity model process is likely to be useful and provide benefits to decision makers in the organisation.					

- **Verifiability**

Please rate the extent to which you agree or disagree with the following statement for evaluate the cloud data governance maturity model verifiability:		1= Strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree				
Sub-criteria	Statement	1	2	3	4	5
Feasible test coverage	The cloud data governance maturity model process meets their development objectives.					
Stability	The cloud data governance maturity model process in different organisations would produce consistent results pattern.					
Verifiable	The cloud data governance maturity model process can be verifiable.					

Could you please give your recommendations to update and improve the cloud data governance maturity model?
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
……………………………………………………………………………………....

Section C: Cloud Data Governance Assessment Matrix

Table: The Cloud Data Governance Assessment Matrix.

Dimension /Level	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Dimension 1	Expectation-Dimension 1/ Level 1	Expectation-Dimension 1/ Level 2	Expectation-Dimension 1/ Level 3	Expectation-Dimension 1/ Level 4	Expectation-Dimension 1 /Level 5
Dimension 2	Expectation-Dimension 2/ Level 1	Expectation-Dimension 2 /Level 2	Expectation-Dimension 2/ Level 3	Expectation-Dimension 2 /Level 4	Expectation-Dimension 2/ Level 5
Dimension n	Expectation-Dimension n/ Level 1	Expectation-Dimension n/ Level 2	Expectation-Dimension n/ Level 3	Expectation-Dimension n/ Level 4	Expectation-Dimension n/ Level 5

Evaluation criteria:

- **Completeness**

Please rate the extent to which you agree or disagree with the following statements for evaluate the cloud data governance assessment matrix completeness:	1= strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree				
Sub-criteria	**Statement**	**1**	**2**	**3**	**4**	**5**
Scope	The assessment matrix provides a tool to assess the cloud data governance in the organisation based on the cloud data governance maturity model structure.					
Definitions	The assessment matrix clearly defined the maturity level for assess the each dimension in the cloud data governance framework.					
Definitions	The assessment matrix clearly defined the cloud data governance dimensions state in each level in the maturity model.					
Perceived Completeness	The cloud data governance assessment matrix are complete and recognizable as adaptation of existing standards, models and methods for the cloud data governance.					

- **Consistency**

Please rate the extent to which you agree or disagree with the following statements for evaluate the cloud data governance assessment matrix consistency:	1= strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree					
Sub-criteria	**Statement**	**1**	**2**	**3**	**4**	**5**
Internal Consistency	There is consistent level of abstraction, granularity, and detail given within the cloud data governance assessment matrix.					

- **Practicality**

Please rate the extent to which you agree or disagree with the following statements for evaluate the cloud data governance assessment matrix practicality:	1= strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree					
Sub-criteria	**Statement**	**1**	**2**	**3**	**4**	**5**
Ease of use	The cloud data governance assessment matrix is easy to use.					
Understandable	The cloud data governance assessment matrix is simple to understand with its practices are clearly defined.					
Practical utility	The cloud data governance assessment matrix practice guidelines provide utility for the organisation.					

Tailorable	The cloud data governance assessment matrix is flexible, tailorable and adaptable.					

- **Usefulness**

Please rate the extent to which you agree or disagree with the following statements for evaluate the cloud data governance assessment matrix usefulness:		1= Strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree				
Sub-criteria	Statement	1	2	3	4	5
Perceived benefits	The cloud data governance assessment matrix is likely to be useful in assessing and improving the cloud data governance processes in the organisation.					
Constructiveness	The cloud data governance maturity model assessment matrix is likely to be useful and provide benefits to decision makers in the organisation.					

- **Verifiability**

Please rate the extent to which you agree or disagree with the following statements for evaluate the cloud data governance assessment matrix verifiability:		1= Strongly agree 2= Agree 3= Neutral 4= Disagree 5= Strongly disagree				
Sub-criteria	Statement	1	2	3	4	5
Feasible test coverage	The cloud data governance assessment matrix meets their development objectives.					
Stability	The cloud data governance assessment matrix process in different organisations would produce consistent results pattern.					
Verifiable	The cloud data governance assessment matrix process can be verifiable.					

- **Strengths and Weaknesses**

Please rate the extent to which your satisfaction with the following statements for evaluate the strengths and weaknesses of the cloud data governance assessment matrix:		1=Very good 2=Good 3=Fair 4=Poor 5= Very poor				
Sub-criteria	Statement	1	2	3	4	5
Individual level in	The **level 1** in the assessment matrix provides strengths content to measure the constructs of the cloud data governance maturity model.					
	The **level 2** in the assessment matrix provides strengths content to measure the constructs of the cloud data governance maturity model.					

assessment matrix (individual score)	The **level 3** in the assessment matrix provides strengths content to measure the constructs of the cloud data governance maturity model.					
	The **level 4** in the assessment matrix provides strengths content to measure the constructs of the cloud data governance maturity model.					
	The **level 5** in the assessment matrix provides strengths content to measure the constructs of the cloud data governance maturity model.					
Individual construct in assessment matrix (individual score)	The assessment matrix provides strengths content to measure the cloud data governance office construct in the cloud data governance framework for each maturity levels.					
	The assessment matrix provides strengths content to measure the preparation requirements construct in the cloud data governance framework for each maturity levels.					
	The assessment matrix provides strengths content to measure the cloud data governance functions construct in the cloud data governance framework for each maturity levels.					
	The assessment matrix provides strengths content to measure the contextual alignment construct in the cloud data governance framework for each maturity levels.					
	The assessment matrix provides strengths content to measure the contextual integration construct in the cloud data governance framework for each maturity levels.					
	The assessment matrix provides strengths content to measure the contractual context construct in the cloud data governance framework for each maturity levels.					
	The assessment matrix provides strengths content to measure the deploy context construct in the cloud data governance framework for each maturity levels.					
	The assessment matrix provides strengths content to measure the sustain requirements construct in the cloud data governance framework for each maturity levels.					
	The assessment matrix provides strengths content to measure the monitor requirements construct in the cloud data governance framework for each maturity levels.					

Could you please give your recommendations to update and improve the assessment matrix for the cloud data governance?
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………….