sustainability

MDPI

Article

Data Governance Taxonomy: Cloud versus Non-Cloud

Majid Al-Ruithe *, Elhadj Benkhelifa * and Khawar Hameed

Cloud Computing and Applications Research Lab, School of Computing and Digital Technologies, Staffordshire University, Stoke-on-Trent ST4 2DE, UK; khawar.hameed@staffs.ac.uk

* Correspondence: majid.al-ruithe@research.staffs.ac.uk (M.A.-R.); e.benkhelifa@staffs.ac.uk (E.B.); Tel.: +966-598-343-504 (M.A.-R.); +44-791-640-6720 (E.B.)

Received: 12 October 2017; Accepted: 14 December 2017; Published: 2 January 2018

Abstract: Forward-thinking organisations believe that the only way to solve the data problem is the implementation of effective data governance. Attempts to govern data have failed before, as they were driven by information technology, and affected by rigid processes and fragmented activities carried out on a system-by-system basis. Until very recently, governance has been mostly informal, with very ambiguous and generic regulations, in siloes around specific enterprise repositories, lacking structure and the wider support of the organisation. Despite its highly recognised importance, the area of data governance is still underdeveloped and under-researched. Consequently, there is a need to advance research in data governance in order to deepen practice. Currently, in the area of data governance, research consists mostly of descriptive literature reviews. The analysis of literature further emphasises the need to build a standardised strategy for data governance. This task can be a very complex one and needs to be accomplished in stages. Therefore, as a first and necessary stage, a taxonomy approach to define the different attributes of data governance is expected to make a valuable contribution to knowledge, helping researchers and decision makers to understand the most important factors that need to be considered when implementing a data governance strategy for cloud computing services. In addition to the proposed taxonomy, the paper clarifies the concepts of data governance in contracts with other governance domains.

Keywords: data governance; cloud computing; cloud data governance; taxonomy; systematic review; holistic

1. Introduction

We are accustomed to the concepts of information technology (IT) governance [1] and corporate governance [2]. The term "governance", in general, refers to the way an organisation ensures that strategies are set, monitored, and achieved [3]. As IT has become the backbone of every organisation, by definition, IT governance becomes an integral part of any business strategy, and falls under corporate governance. Historically, data emerged out of disparate legacy transactional systems. Then, data was seen as a by-product of running the business, and had little value beyond the transaction and the application that processed it, hence data was not treated as a valuable shared asset. This continued until the early 1990s, when the value of data started to take another trend beyond transactions. Business decisions and processes increasingly started to be driven by data and data analysis. Further investment in data management was the approach taken to tackle the increasing volume, velocity, and variety of data, such as complex data repositories, data warehouses, Enterprise Resource Planning (ERP), and Customer Relationship Management (CRMs) [4]. Data links became very complex and shared amongst multiple systems, and the need to provide a single point of reference in order to simplify daily functions became crucial, which gave birth to master data management [5].

Data complexity and volume continue to explode; businesses have grown more sophisticated in their use of data, which drives new demands that require different ways to combine, manipulate, store, and present information. Forward-thinking companies recognised that data management solutions alone are becoming very expensive and are unable to cope with business realities, and the data problem must be solved in a different way [6]. During this time, the notion of data governance started to take a different direction, a more important one. Attempts to govern data failed before, 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 mostly informal, in siloes around specific enterprise repositories, lacking structure and the wider support of the organisation. Despite its recognised high importance, data governance is still an under-researched area and less practised in industry [7,8]. Researchers differ in their definitions of data governance. The governance concept can be understood in different contexts, for instance, corporate governance, information governance, IT governance, and data governance; Wende [9] and Chao [10] argue that data governance and IT governance need to follow corporate governance principles.

To achieve successful data governance, organisations need a strategy framework that can be easily implemented in accordance with the needs and resources of information [11,12]. A good data governance framework can also help organisations to create a clear mission, achieve clarity, increase confidence in using organisational data, establish accountabilities, maintain scope and focus, and define measurable successes [11,13]. To facilitate data governance, Seiner [14] argues 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 data in the organisation. Along similar lines, some authors in the literature argues that organisations should obtain responsibility for data from the information technology (IT) department, with the participation and commitment of IT staff, business management, and senior-level executive sponsorship in the organization [15]. Experts in this field show that where organisations do not implement data governance, the chaos is not as obvious, but the indicators are glaring, including dirty, redundant, and 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 [16]. The first efforts to create a framework for data governance were published in 2007 [9,17].

The emergence of cloud computing is a recent development in technology. The National Institute of Standards and Technology (NIST) [18] defined 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*". The cloud computing model enhances availability, and is composed of five essential characteristics, four deployment models, and three service models [19]. The essential characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [20]. The cloud deployment models are the private, public, hybrid, and community models [21]. In addition, cloud computing includes three service delivery models, which are: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [22]. Cloud computing offers potential benefits to public and private organisations by making IT services available as a commodity [23,24]. The generally claimed benefits of cloud computing include: cost efficiency, unlimited storage, backup and recovery, automatic software integration, easy access to information, quick deployment, easier scale of services, and delivery of new services [25]. Furthermore, other benefits include: optimised server utilisation, dynamic scalability, and minimised life cycle development of new applications. However, cloud computing is still not widely adopted due to many factors, mostly concerning the moving of business data to be handled by a third party [6], where, in addition to the cloud consumer and provider, there are other actors: the cloud auditor, cloud broker, and cloud carrier [26]. Therefore, loss of control of data, security and privacy of data, data quality and assurance, data stewardship, etc. can all be cited as real concerns of adopting the cloud computing business model [27]. Data lock-in is another

potential risk, where cloud customers can face difficulties in extracting their data from the cloud [28]. Cloud consumers can also suffer from operational and regulatory challenges, as organisations transfer their data to third parties for storage and processing [29]. In addition, it may be difficult for the consumers to check the data handling practices of the cloud provider or any of the other involved actors [23,30,31]. The cloud computing model is expected to be a highly disruptive technology, and the adoption of its services will, therefore, require even more rigorous data governance strategies and programmes, which may be more complex, but are necessary.

The general consensus among authors is that data governance refers to the entirety of decision rights and responsibilities concerning the management of data assets in organisations. This definition does not, however, provide equal prominence for data governance within the cloud computing technology context. Therefore, this deficit calls for in-depth understanding of data governance and cloud computing. This trend contributes to changes in the data governance strategy in the organisation, such as the organisation's structure and regulations, people, technology, processes, roles, and responsibilities. This is one of the great challenges facing organisations today when they move their data to cloud computing environments, particularly regarding how cloud technology affects data governance. The authors' general observation reveals that the area of data governance in general is under-researched and not widely practised by organisations, let alone when it is concerned with cloud computing, where research is in its infancy and far from reaching maturity.

This forms the main motivation behind this paper, which attempts to provide the readers with a holistic view of data governance for both cloud and non-cloud computing, using a taxonomy approach. The contribution of this paper is unprecedented, with this taxonomy expected to be very valuable in developing coherent frameworks and programmes of Data Governance for both cloud and non-cloud computing. One main question has been considering to formulate the results in this study which is following: what is the main factor that require to develop the data governance for non-cloud and cloud computing?

The remainder of the article is structured in seven sections. The next section discusses what data governance is, and why it is important, followed by a section reviewing the literature on data governance. A subsequent section presents the relationship between data governance and other governance domains. Following this, the data governance taxonomy section presents a holistic taxonomy for data governance for cloud and non-cloud. The final Section presents the conclusions, limitations of research and future work.

2. What Is Data Governance and Why Is It Important?

It is important, before developing a holistic taxonomy, to define the context of data governance. Often, researchers and practitioners confuse data governance and data management. The definition of data management provided by the Data Management Association (DAMA) is: "*data management is the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets*" [12]. Data management in general focuses on the defining of the data element, how it is stored, structured, and moved. Although there is no official standard definition of data governance, to provide clarity, we refer to the most cited definitions offered by some important organisations and specialists.

According to the Data Governance Institute (DGI), 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" [32]. The IT Encyclopedia defines data governance as: "*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*" [7]. DAMA, on the other hand, defines data governance as: "*the exercise of authority, control and shared decision-making (planning, monitoring and enforcement) over the management of data assets*" [33]. According to DAMA, data governance is, therefore, high-level planning and control

over data management [33]. Wende [9] have also argued that data governance is different from data management, that data governance complements data management, but does not replace it. Ladley [34] defined data governance as "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". Weber [7] suggested that 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 organization's mission, strategy, values, norms, and culture." More recently, "Non-Invasive", a book by Seiner in 2014, defines data governance as "the formal execution and enforcement of authority over the management of data and data related assets" [14].

Some other researchers or practitioners seem also to confuse IT governance and data governance. IT governance is a much more mature area, with the first publications on the topic released about four decades ago [35], while data governance is still under-researched. Organisations with mature IT governance practices tend to have a stronger alignment between IT and business [36], and the author argues that organisations should gain the responsibility for data from the IT department. Besides IT governance, data governance also has a significant role in aligning the organisation's business. Data governance can be used to solve an assortment of business issues related to data and information [16]. Otto [37] argued that a data governance model helps organisations to structure and document the accountabilities for their data quality. Some authors have explicitly demonstrated that data governance is different from IT governance in principle and practice [9,24]. In principle, data governance is designed for the governance of data assets, while IT governance makes decisions about IT investments, the IT application portfolio, and the IT projects portfolio. In practice, IT governance is designed primarily around an organisation's hardware and applications, not its data.

Al Rifai M. et al. [30] argues that enterprise-wide data strategy and governance are important for organisations, and are required to achieve competitive advantage. In addition, all existing sources have hitherto only addressed data governance. The fact that organisations need to take many aspects into consideration when implementing data governance has been neglected so far [9,16,38]. Moreover, some researchers show that organisations which do not implement effective data governance can quickly lose any competitive advantage [14,39]. Seiner [14] illustrated that working without a proper data governance programme is analogous to an organisation allowing each department and each employee to develop, for instance, their own financial chart of accounts. Data governance in any organisation requires the involvement and commitment of all staff, with full sponsorship by the management and senior-level executive sponsorship [40].

Recently, many organisations have become aware of the increasing importance of governing their data to ensure the confidentiality, integrity, quality, and availability of customer data [41,42]. Currently, there is no single approach for the implementation of a data governance programme for all organisations [3]. Good data governance can help organisations to create a clear mission, achieve clarity, increase confidence in using organisational data, establish accountabilities, maintain scope and focus, and define measurable successes [33,43]. Moreover, many authors have suggested that developing effective data governance will lead to many benefits for organisations. These benefits are: enabling more effective decision-making, reducing operational friction, and protecting the needs of data stakeholders as central to a governance programme [44,45]. In addition, other benefits include: training of management and staff to adopt common approaches to data issues, build standard, repeatable processes, reducing costs and increasing effectiveness through coordination of efforts, and ensuring the transparency of processes [16,17,37].

3. Review of the Literature on Data Governance

An up-to-date literature review has been undertaken to help us and the readers understand the research landscape in data governance. This review will be instrumental in developing the

aforementioned taxonomy. The review followed the systematic literature review protocol, defined by [46], with customised search strings, a study selection process, and inclusion and exclusion criteria. The search was conducted in the following libraries and databases: Google Scholar, Staffordshire e-resources Libraries, Saudi Digital Library, and the British Library (Ethos). The term "data governance" was used in this search, but we 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 organization", "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 organization) OR (governance data) OR (data governance in cloud computing) OR (data governance for cloud computing) OR (cloud data governance)).

The search covered the period between 2000 and 2017. The study selection process was based on four stages, and only 52 records on data governance, which meet the criteria and fall within the scope of the study, were attained for the final review. Table 1 provides a summary of these 52 papers, categorised by academic- and practice-oriented contributions for cloud and non-cloud computing.

Table 1. Categorisation of the resultant records on data governance.

Nature of Contribution	Format	References
Academic	Papers in journals and conference proceedings, books, working reports and theses	Non-cloud: [6,7,9,11–14,30,33,34,37,44,47–59]. Cloud Computing: [60–62].
Practice-oriented	Publications by industry associations, software vendors and analysts	Non-cloud: [38,39,63–65], [50,52,66–111]. Cloud Computing: [41,42,53,70–72].

Out of the retained 52 records, only five records were reported in academic literature on data governance for cloud services. All reported research agrees that only a few organisations have addressed data governance, and only partially. Additionally, all reported academic literature stated that data governance is one of the key components for any enterprise cloud; they also described some issues related to moving data to the cloud outside the organisation's premises, such as security, data migration and interoperability. Felici et al. [60] focused more on one aspect of data governance, accountability, where they proposed an accountability model for data stewardship in the cloud, which explains data governance in terms of accountability attributes and cloud-mediated interactions between actors. This model consists of accountability attributes, accountability practices and accountability mechanisms. Tountopoulos [73] focused on addressing interoperability requirements relating to the protection of personal and confidential data for cloud data governance. They also categorised the accountability taxonomy, composed of seven main roles, which are: cloud subject, cloud customer, cloud provider, cloud carrier, cloud broker, cloud auditor, and cloud supervisory authority. Figure 1 shows the numbers of published research on data governance in the last 10 years, following a systematic review.

Cloud data governance has also been overlooked by industry. Cloud Security Alliance, Trustworthy Computing Group, and Microsoft Corporation are regarded as the recognised leaders in this area. The Cloud Security Alliance cloud data governance working group currently focuses on the data protection aspect, with an aim to propose a data governance framework to ensure the availability, integrity, privacy, and overall security of data in different cloud models; this is far from being realised [74]. 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 embark on this path [41]. 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 about 56% of agencies are currently in the process of implementing data stewardship or data governance programmes [75].

Evaluating the existing work on data governance for traditional IT and cloud computing reveals that it is still very limited, lacking standards and unified definitions, hence a taxonomy approach to classify different aspects and attributes of data governance will be a highly valuable contribution at this stage.

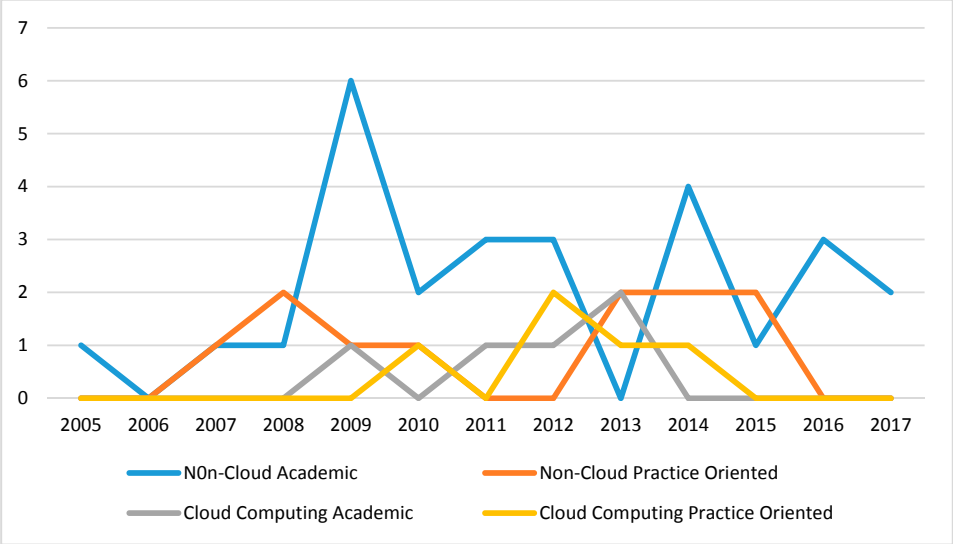

Figure 1. Number of published research on data governance in the last 10 years.

4. Data Governance and Other Governance Domains

With the emergence of new governance domains—to name but the most relevant ones, Corporate Governance, IT Governance, Information Governance, and, more recently, Cloud Computing Governance—it is easy to confuse them, something we have observed in the literature, where authors have interchanged these governance domains as if they are the same thing. It is important, therefore, to differentiate between these domains, and more important to define how they are linked to each other, particularly with respect to data governance. Figure 2 is a simplified view of the interrelations between these domains.

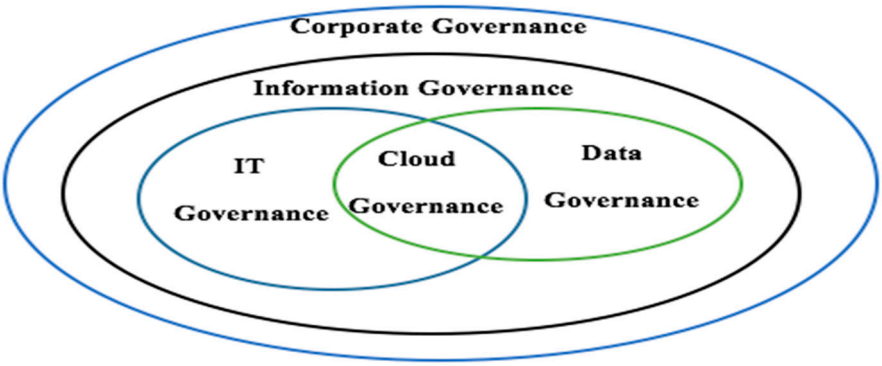

Figure 2. The interrelations between governance domains.

Corporate governance has become important, as effective governance ensures that the business environment is fair and transparent, and that companies can be held accountable for their actions [76].

In contrast, weak corporate governance leads to waste, mismanagement and corruption. According to the Organization for Economic Cooperation and Development (OECD), corporate governance is "*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*" [77].

In recent years, IT has been the backbone of every business [78]. As a result, the concept of IT governance has become more important for organisations. IT governance, similarly to corporate governance, is the process of establishing authority, responsibilities, and communication, along with policies, standards, control mechanisms and measurements to enable the fulfilment of defined roles and responsibilities [79]. Thus, corporate governance can provide a starting point in the definition of IT governance [7]. According to Herbst et al. (2013), 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*" [80]. 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 also that it is not the sole responsibility of the CIO [81].

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 [82]. 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 information in terms of value creation [83]. Gartner defines information governance as "*the specification of decision rights and an accountability framework to ensure appropriate behaviour in the valuation, creation, storage, use, archiving and deletion of information*" [84]. The information governance approach focuses on controlling information that is generated by IT and office systems, or their output, but does focus on detailed IT or data capture and quality processes.

Cloud governance is a new term in the IT field; however, it has not been given a clear definition yet [85]. 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*" [86]. The core of cloud governance revolves around the relationships between provider and consumer, across different business models [87]. The business model should define the way in which an offer is made and how it is consumed. To function at all cloud levels (IaaS, PaaS and SaaS), the business model should be devoid of the type of resources involved.

The literature reported different views on what drives what within these governance domains; in our research, we argue that data governance should be the key driver for all other governance domains, sitting at the heart of everything. The most debated relationship among these governance domains has been that of 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 must become an ingrained part of both corporate governance and IT governance [88]. Figure 3 provides an illustration of the advocated hierarchy of these governance domains, showing also the difference between management and governance.

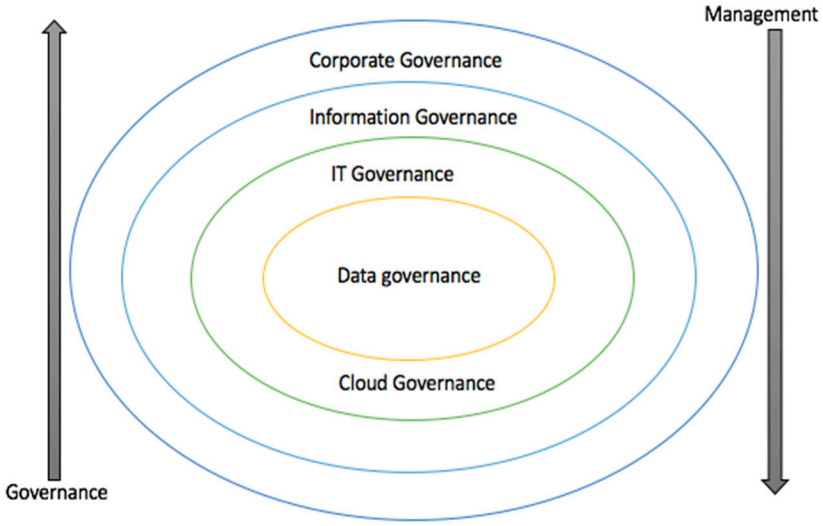

Figure 3. The hierarchy for the difference between management and governance.

5. Data Governance Taxonomy

To construct a holistic taxonomy, we must determine the key dimensions of data governance. This adopted dimension-based approach allows for the categories in the taxonomy to be broken down into discrete areas. A dimension-based approach allows more flexibility in placing content into various nodes, represented by the dimension to which they belong. In the context of data governance, this approach will allow users to manage data governance content more efficiently. Successfully achieving this could be a potentially complex process, and consequently requires more investigative effort and the involvement of different stakeholders. Therefore, the taxonomy for data governance was developed following exploratory and qualitative research, where the method employed was merrily based on a combination of analysing the relevant knowledge in the public domain, resulting from the above described systematic literature review (Section 3) and following the analytic theory [89].

The analytic theory has been useful in understanding the data governance aspects of traditional IT and cloud technology. Sein M. et al. [89] state that "*the analytic theory is used to describe or classify specific dimensions or characteristics of individuals, groups, situations, or events by summarizing the commonalities found in discrete observations. Frameworks, classification schema and taxonomies are numerous in IS*". The analytic theory has been chosen as a concept for this study to identify data governance dimensions for the cloud services. To use analytic theory in making data governance dimensions, we follow three steps. Firstly, understanding the state of the art of data governance for traditional IT and the cloud. Secondly, identifying specific dimensions or characteristics of data governance and cloud computing. Finally, developing the key data governance dimensions for cloud computing, based on the definitions of data governance and factors presented in the literature review, which will construct the desired taxonomy. The adopted approach is considered expedient in expounding a sound theoretical foundation for the study. This approach is used to contextualise the research, for which authors chose the contents that were relevant for the study and how these were employed in order to reach a scientific conclusion. Such an approach is considered essential, following a set of processes or procedures in undergoing a systematic review, which can be verified or validated scientifically.

To the best of the authors' knowledge, and following the aforementioned research approach, there is no published research that defines the key dimensions of data governance for cloud computing. In contrast, for traditional IT (non-cloud), there is some reported research, albeit not much. As illustrated above, data governance for non-cloud and cloud, although showing some similarities at a higher level, differs significantly in details, in addition to some new factors related only to cloud technology. Figure 4 shows the two main classes of data governance, considered as

sub-taxonomies: data governance for non-cloud computing, referred to herein as traditional data governance, and data governance for cloud computing, referred to herein as cloud data governance.

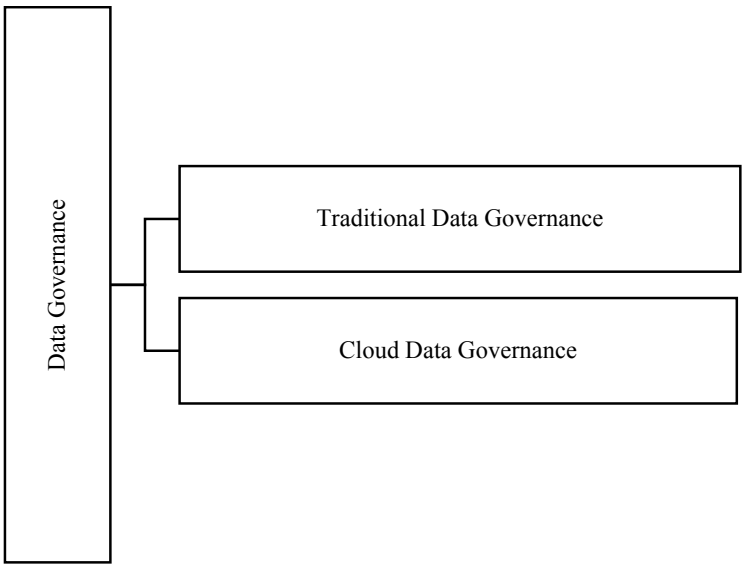

Figure 4. Two main blocks of the data governance taxonomy.

5.1. Traditional Data Governance

As shown in the systematic literature review above, the literature on traditional data governance is still considered insufficient. Some authors expressed their subjective views on aspects of data governance; this subjectivity is driven by the fact that there is no single approach to implementing standard data governance for all types of organisations [4]. This means each organisation's approach to data governance could be different. It is, therefore, very difficult to capture all the different views; instead, after further analysis of the relevant literature, we could identify common aspects of data governance which most authors seem to agree upon. Therefore, traditional data governance could be classified into three main categories: people and organisational bodies, policy, and technology, as shown in the simplified taxonomy below (Figure 5). This is followed by extended descriptions and classification of each aspect.

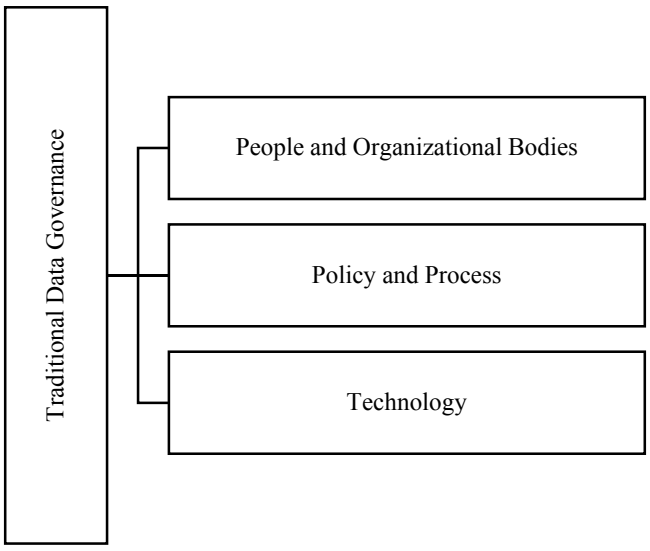

Figure 5. Traditional data governance taxonomy.

5.1.1. 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 each stakeholder. Therefore, in traditional data governance, the people and organisational bodies play important parts when organisations implement data governance for their business [90]. The element of people and organisational bodies in data governance can be defined as any individual or group that could affect or be affected by the data under discussion. People in traditional governance have many tasks, including authority, data stewardship, business rules, collaboration, accountability and culture attitude [91]. The people and organisational bodies element, in the context of traditional data governance, could include the following: data governance office, data governance council, executive sponsorship, chief information officer (CIO), data management committee, compliance committee and data stewards; each has specific roles and responsibilities within their organisations. Figure 6 below summarises the most important aspects of this class of traditional data governance, as agreed by most reported literature.

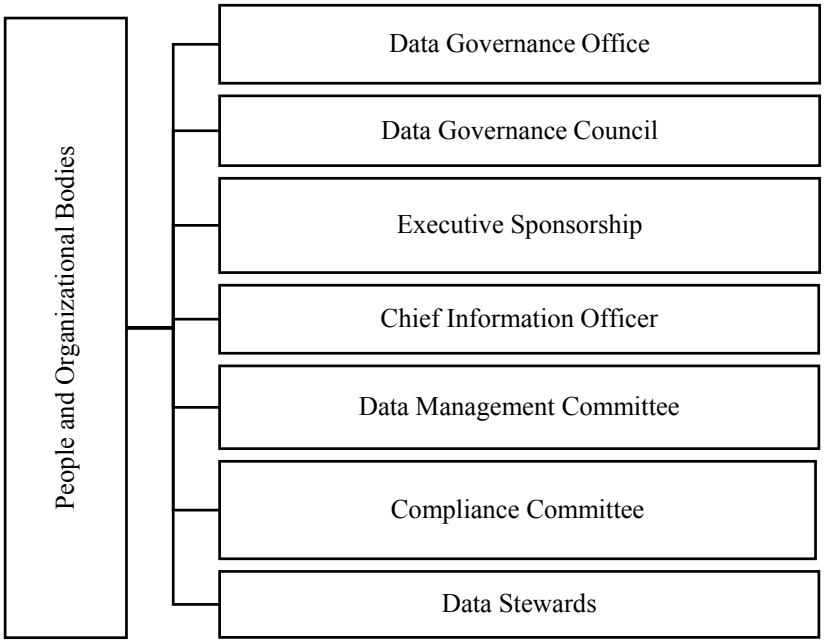

Figure 6. People and organisational bodies taxonomy in traditional data governance.

5.1.2. Policy and Process

Data governance policy is a set of measurable acts and rules for a set of data management functions in order to ensure the benefit of a business process [92]. Regarding data governance processes, they describe the methods used to govern data; these processes should be standardised, documented and repeatable. According to IBM Institute [69], 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 could include principles, policies, standards and process, as displayed in Figure 7.

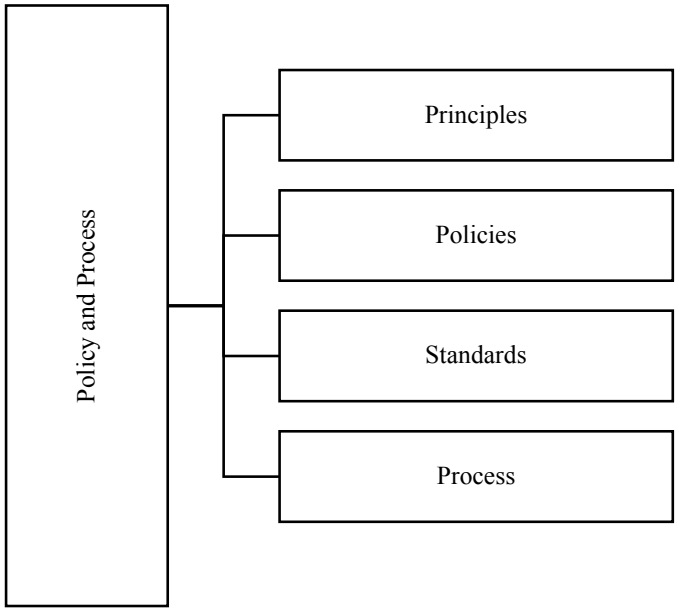

Figure 7. Policy and process elements in traditional data governance.

5.1.3. Technology

Technology is an integral factor for data governance; it is through technology that we can ensure automation and enforce and control data governance policies. However, the role of technology comes after an approved data governance policy and process. Technology in the context of data governance represents the engineering methods that are responsible for reflecting its policies and practice in a measurable way. Therefore, a fit-for-purpose plan for using technical tools to support data governance polices, within the context of roles, responsibilities, and accountabilities, must be established [4,66]. The simplest forms of technology reported for traditional data governance could include hardware, software and monitoring tools, as depicted in Figure 8.

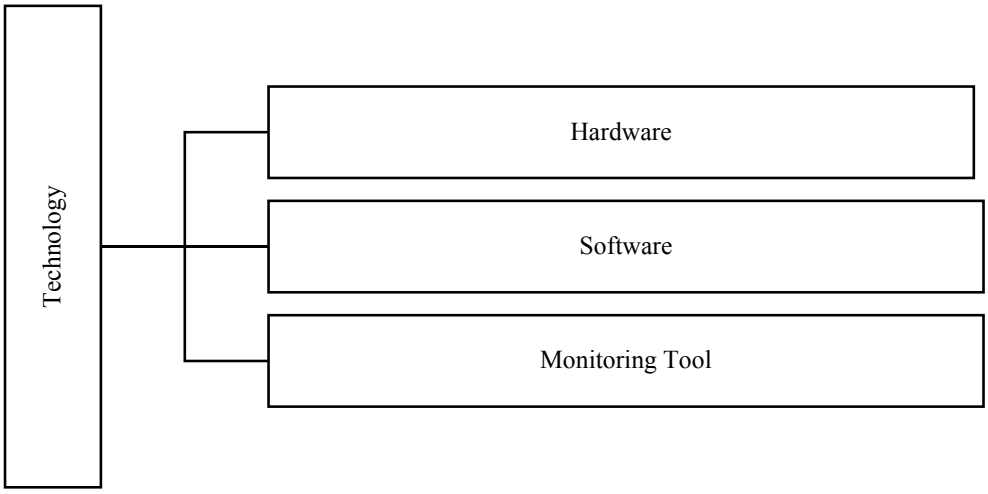

Figure 8. The technology elements of traditional data governance.

5.2. Cloud Data Governance

The impediment to the wider adoption of the cloud computing model has been linked primarily to aspects related to the data governance environment [42,53,60]. While security seems to be the most cited challenge to cloud adoption, Farrell [93] shows that 41% of the security problems in the cloud are

related to governance and legal issues. Data governance is considered to be one of the most important aspects of cloud governance [25]. Data governance programmes, built for on-premises IT infrastructure, cannot be deployed for cloud infrastructure and service provisioning, which would require completely new requirements, design and implementation [53,93]. Undoubtedly, the area of cloud data governance is becoming a topic of the coming decades [60,73], although it is still under-researched by both academia and industry, due to its novelty [7,9]. As discussed above, data governance is still underdeveloped and under-practised, even for traditional IT infrastructures, let alone cloud computing environments [4,94]. This is evidenced by the results of the systematic literature review discussed above, where only 11 records discussing data governance for cloud computing were reported. Governance in the cloud needs to understand, moderate and regulate the relationships between different cloud actors or stakeholders in terms of roles and responsibilities [24]. Data governance is meant to classify and assign responsibilities, communication, labelling and policies [57]. There are few studies reporting on data governance for the cloud services. Almost all existing work on data governance for cloud computing focuses on accountability and interoperability [57,60]. Accountability could be addressed at different levels, technological, regulatory and organisational [95].

There is a strong consensus that cloud computing will lead to change in the strategy of traditional data governance in organisations [96]. Cloud data governance is the main focus area in this research, where the aim is to construct a taxonomy that represents the different classifications of this domain. To recall, to the best of the authors' knowledge, this is the first such attempt reported, following the most comprehensive and up-to-date literature review. Figure 9 is a high-level taxonomy of cloud data governance, compiled from the analysis of relevant literature, identified from the systematic literature review. The subsequent sections contain further description of every sub-class.

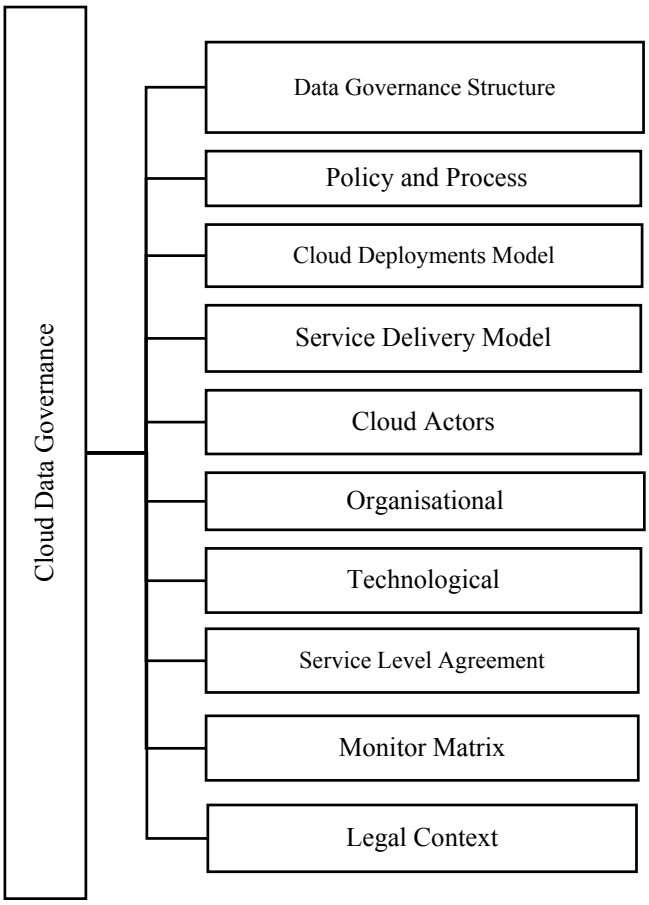

Figure 9. A Cloud Data Governance Taxonomy.

5.2.1. Data Governance Structure

Designing a data governance structure is an important factor in ensuring that requisite roles and responsibilities are addressed throughout the enterprise at the right organisational levels [13]. Several common data governance roles have been identified in existing studies, including the following: executive sponsorship, data management committee, compliance committee, data stewardship team, cloud manager, cloud provider member, IT member and legal member [9,97]. These roles must collaborate to formulate data governance bodies. Figure 10 shows an example of a typical cloud data governance structure.

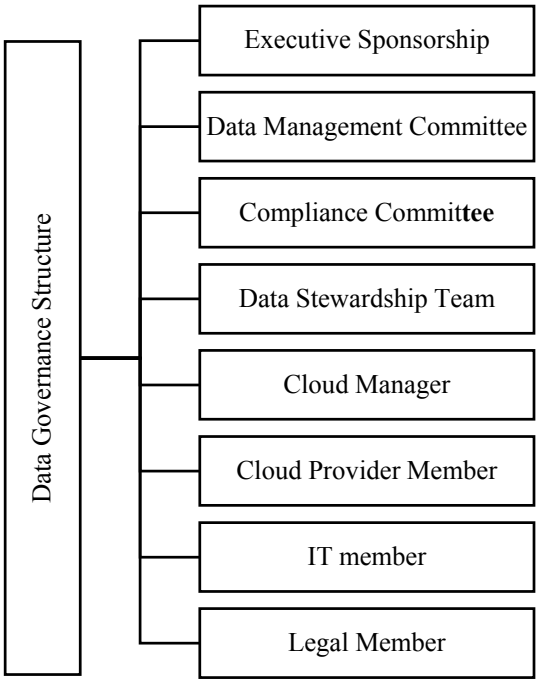

Figure 10. Cloud data governance structure.

5.2.2. Data Governance Function

This refers to master activities for data governance, including functions which data governance teams must take into account when implementing data governance programmes [98]. 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 [3,37]. Therefore, the data governance team must define all data governance policies that address cloud consumers' concerns. The data governance functions can support organisations 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 [99]. Effective data governance in cloud computing requires transparency and accountability, which leads to appropriate decisions that foster trust and assurance for cloud consumers [100]. The outcomes from data governance function activities include standard, procedure, compliance, transformation, integration, management, auditability, transparency, policies, principles and processes. This is considered the master dimension for data governance, but it must comply with other dimensions to develop effective data governance. Figure 11 shows the cloud data governance function and its concerns for cloud computing.

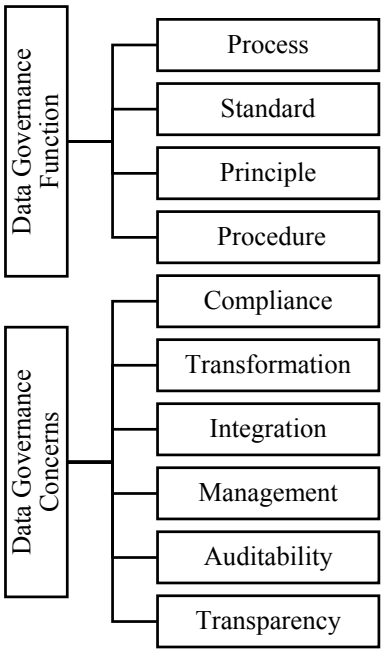

Figure 11. Cloud data governance function and its concerns for cloud computing.

5.2.3. Cloud Deployment Model

This is an important factor to consider in data governance. There are primarily four cloud deployment models, which differ in their provisions; these are the public, private, hybrid and community cloud deployment models. To address data governance, the level of risk and complexity of each cloud deployment must be taken into consideration [18]. According to [110] the implementation of data governance varies greatly, based on the adopted cloud deployment. Figure 12 shows cloud deployment model types to be considered when implementing a cloud data governance programme.

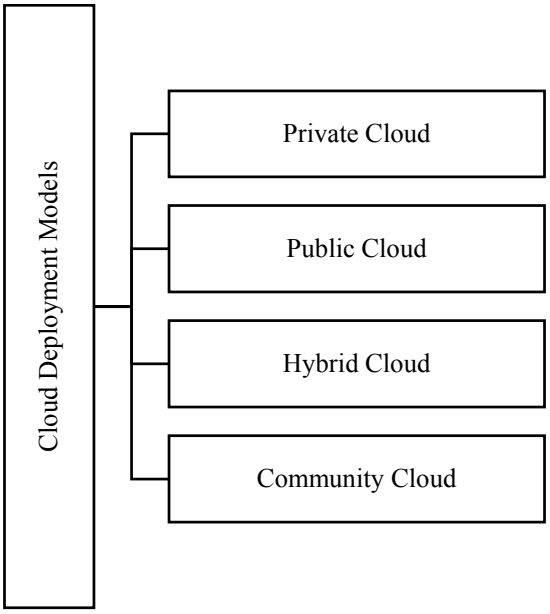

Figure 12. Cloud deployment model types for cloud data governance.

5.2.4. Cloud Service Delivery Model

Cloud services can be categorised into three delivery models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [101]. Depending on the model, the cloud consumer will have a differing level of control over their data [61] and each model will require a different approach to data governance and management. Therefore, the data governance teams must consider all the characteristics of the service delivery model and define appropriate policies to enforce control roles and responsibilities. Figure 13 shows the cloud service delivery model to be considered when implementing cloud data governance.

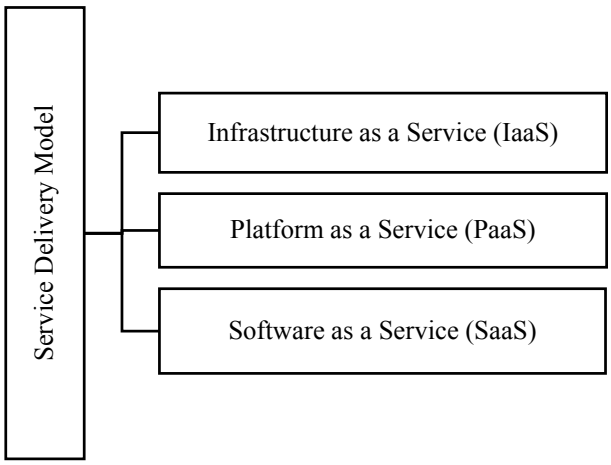

Figure 13. Cloud service delivery model for cloud data governance.

5.2.5. Cloud Actors

The actors are also a critical factor in defining cloud data governance. "Cloud actors" refers to individuals or organisations that participate in processes or transactions, and/or perform tasks in the cloud computing environment. NIST's cloud computing reference architecture distinguishes five major actors: the cloud consumer, the cloud provider, the cloud auditor, the cloud carrier and the cloud broker [18]. Each cloud actor has special roles and responsibilities in any one cloud provision, so a data governance programme must clearly define the roles and responsibilities for all cloud actors [102]. Figure 14 shows the cloud actors in cloud data governance.

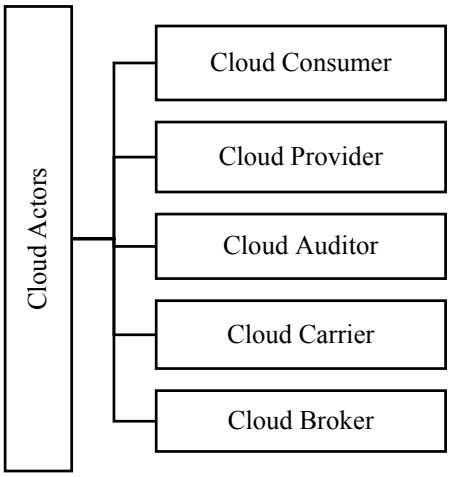

Figure 14. Cloud actors in cloud data governance.

5.2.6. Service Level Agreement (SLA)

One key issue for the cloud consumer is the provision of governance for data which they no longer directly control [103]. Contractual barriers increase between cloud actors. An SLA is an agreement that serves as the foundation of expectation for services between the cloud consumer and the provider [100]. The agreement states what services will be provided, how they will be provided, and what happens if expectations are not met; therefore, an SLA is pivotal in data governance. Thus, the cloud consumer and provider must negotiate all aspects of data governance before developing the SLA. As a result, these agreements are in place to protect both parties. 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 in defining governance plans for data which they may choose to move to a cloud provider [104]. These must 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 establishing the contract. The SLA for cloud data governance includes data governance functions; data governance requirements, roles and responsibilities; and data governance metrics and tools. Figure 15 shows the SLA elements for cloud data governance.

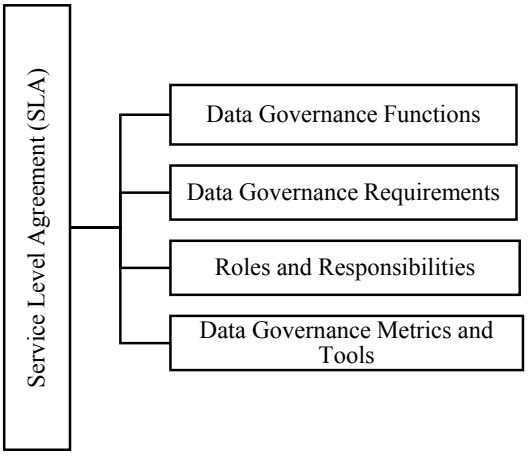

Figure 15. Service Level Agreement (SLA) elements for cloud data governance.

5.2.7. Organisational Context

Data governance is a major mechanism for establishing control over an organisation's data assets and enhancing their business value [105]. It is also a critical element of implementing a sustainable data management capability, which addresses enterprise information needs and reporting requirements. Organisational factors are important for data governance to be successful [8]. Data governance requires change management in the organisation, in addition to the participation and commitment of IT staff, business management and senior-level executive sponsorship in organisations [37]. Moreover, top management support is considered to be the critical success factor in implementing data governance [61]. Staff in organisations need to learn data governance functions, demanding top management support to enhance the organisation's staff skillset. The organisational context means defining all internal factors that organisations must consider when they manage risks [14]. There are three perspectives for organisational context: the strategic, tactical and operational perspectives. 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, the business model, decision-making processes, training plan, communication plan and change management plan. Figure 16 shows the organisational context elements of cloud data governance.

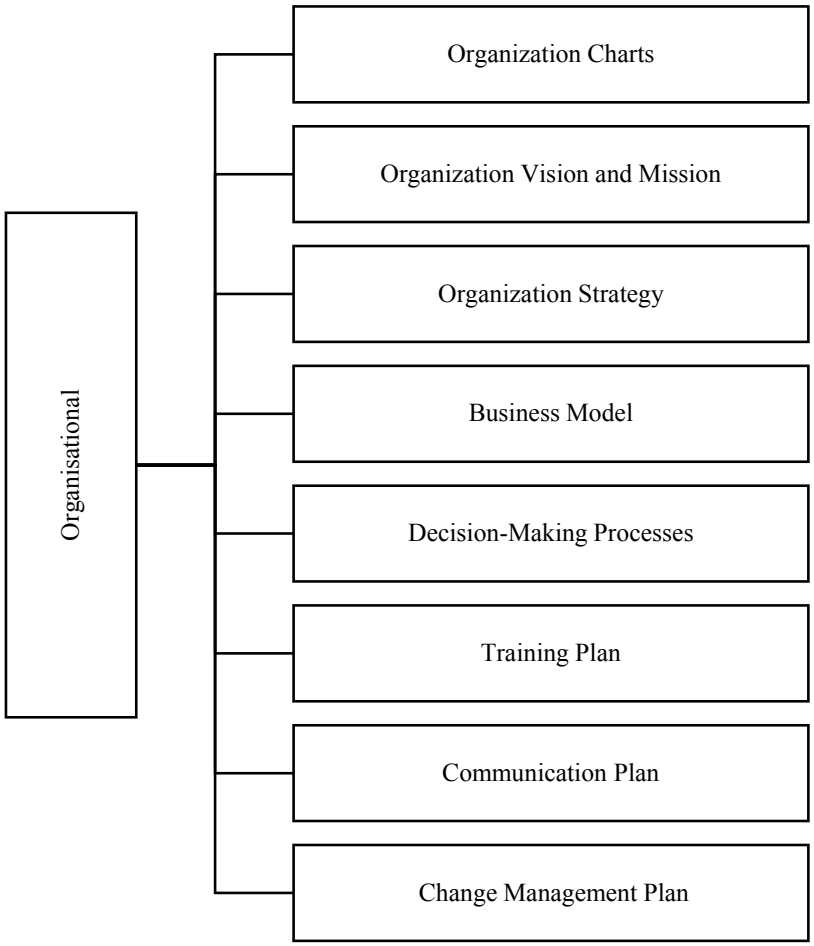

Figure 16. Organisational context of cloud data governance.

5.2.8. Technical Context

Technology is also a key element for data governance success [8]. The technical context represents the issues related to data which will affect the decision of cloud computing adoption and data governance implementation for cloud computing services [106]. Therefore, a lack of technology is considered to be a barrier to successful data governance. Technical factors encapsulate data management issues that affect organisations' strategies, such as security, privacy, quality and integrity. Therefore, it is incumbent upon organisations implementing data governance to assess all technological characteristics available in their organisation, in order to effectively implement data governance. The technical issues that could have an impact on the implementation of data governance for cloud services include availability, reliability, security, privacy, quality, compatibility, ownership, auditing, integrity, data lock-in and performance [106,107]. Figure 17 displays the technological context elements of cloud data governance.

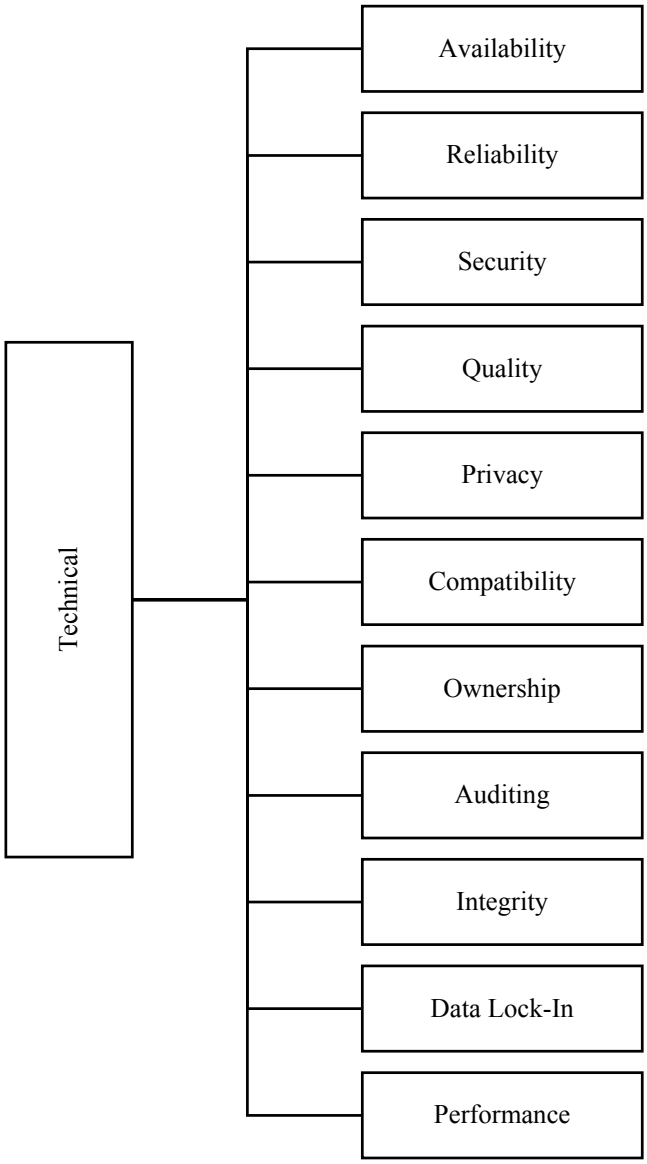

Figure 17. Technical context of cloud data governance.

5.2.9. Legal Context

The legal aspect in this context determines the external and internal laws and regulations related to the data which might affect an organisation's intent to adopt cloud technology [106], which can in turn affect the implementation of an adequate data governance programme for cloud computing services. Therefore, the data governance teams must understand what is implied about data in all relevant contracts before implementing a data governance strategy. Failure to comply with the law when dealing with confidential data erodes trust, which can seriously damage the view of the top management of an organisation regarding the trustworthiness of the cloud provider services [108]. The legal context for cloud data governance includes the Data Protection Act 1998, change of control act and cloud regulations. Figure 18 shows the legal context of cloud data governance.

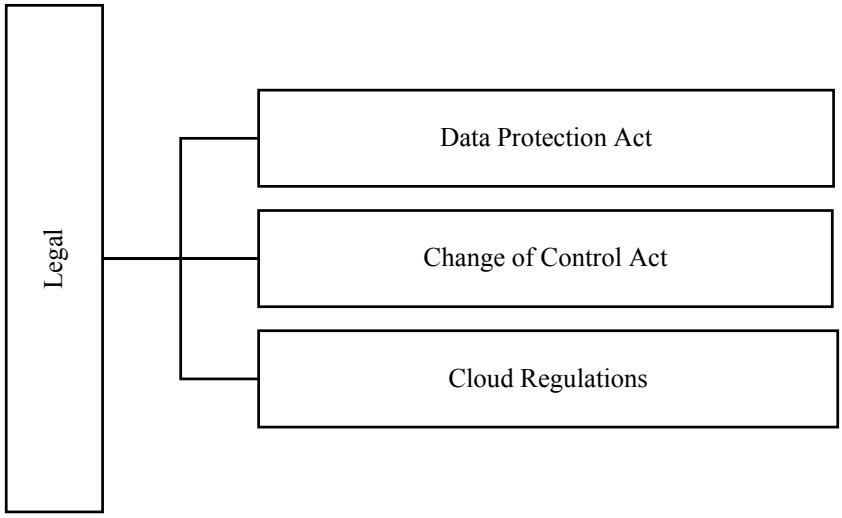

Figure 18. Legal context of cloud data governance.

5.2.10. Monitor Matrix

The monitor matrix in data governance is the exercise of authority, control and shared decision-making over the management of data assets [41]. Measuring and monitoring supports ongoing data governance efforts to ensure that all incoming and existing data meets business rules [109]. By adding a monitoring component to the data governance programme, data quality efforts are enhanced, which in turn renders data much more reliable [109]. Moreover, continuous monitoring ensures compliance with SLAs and the set requirements defined in the data governance strategy [42]. The data governance monitor matrix for cloud computing services includes the cloud control matrix, KPIs and a monitoring tool. Figure 19 shows the elements of the monitor matrix for cloud data governance.

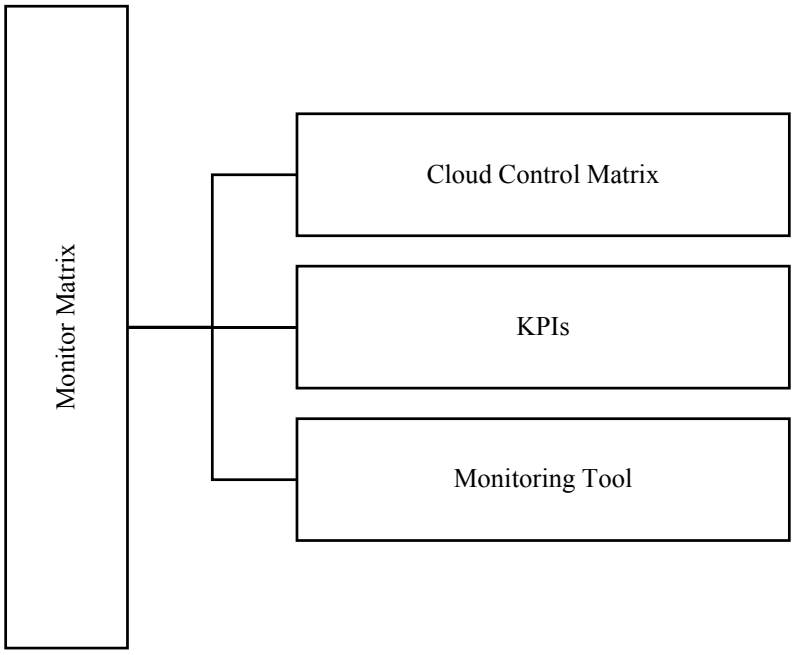

Figure 19. Monitor matrix elements for cloud data governance.

Figure 20 highlights the overall taxonomies of data governance for cloud and non-cloud.

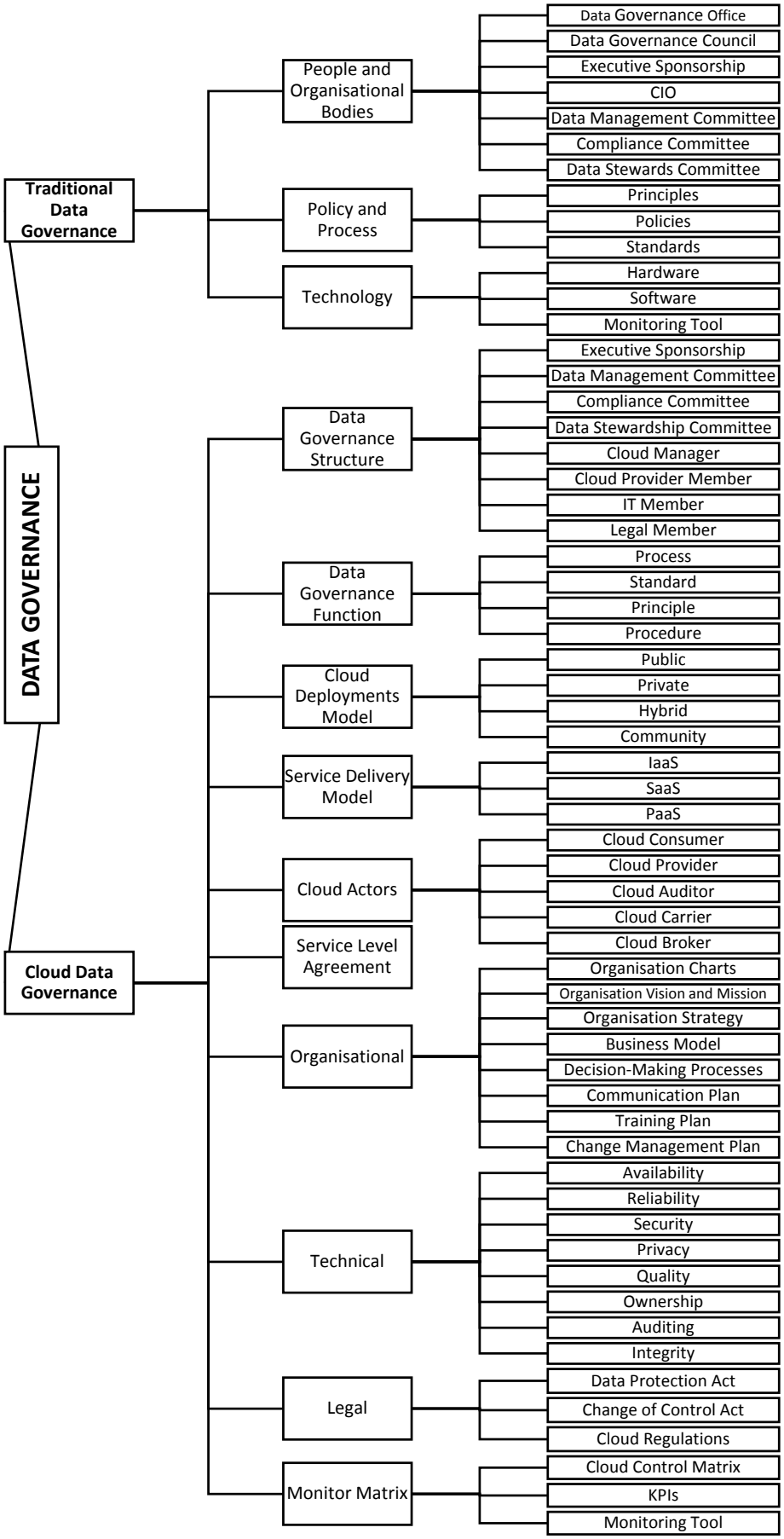

Figure 20. The overall taxonomies of data governance for cloud and non-cloud.

6. Conclusions

Data management solutions alone are becoming very expensive and are unable to cope with the reality of everlasting data complexity. Businesses have grown more sophisticated in their use of data, which drives new demands, requiring different ways to handle this data. Forward-thinking organisations believe that the only way to solve the data problem will be the implementation of effective data governance. With the absence of sufficient literature on data governance in general, and specifically for the cloud paradigm, this paper presents a useful contribution to the relevant research communities. In this paper, we proposed taxonomies for data governance, for both non-cloud and cloud computing networks. A holistic taxonomy that combines all different taxonomies is depicted in Figure 20. These taxonomies are supported by the results of a systematic literature review (SLR), which offers a structured, methodical, and rigorous approach to the understanding of the state of the art of research in data governance. The objective of the study is to provide a credible intellectual guide for upcoming researchers in data governance, to help them identify areas in data governance research where they can make the most impact.

However, this study presents a taxonomy of data governance development requirements for non-cloud and the cloud environments; thus, it does not cover a taxonomy of operational data governance risks that attempts to identify and organize the sources of operational data governance risk. Moreover, this paper is the first of its type, to the best of the authors' knowledge, to cover cloud data governance taxonomy; this presents another limitation, which is related to the lack of relevant literature in this subject domain. The literature shows that most of the existing studies focus on a survey of data governance for non-cloud environments, whilst only three sources in the literature focused on accountability of data governance in cloud computing environments.

Due to the lack of research in this subject area, future work will focus of validation of the proposed taxonomies with specialists from both academia and practitioners. Further research can investigate the application of the proposed taxonomies, especially for cloud data governance, in real world case scenarios. The presented research in this paper shows the lack of research in cloud data governance, which creates an urge for the need to develop a holistic framework for cloud data governance strategy, which highlights the main pillars, processes and attributes to design more specific data governance program. The proposed taxonomies are expected to play an instrumental role in developing such a framework.

Author Contributions: All authors have contributed in this paper by research, scoping writing, and/or reviewing of assigned sections.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nfuka, E.; Rusu, L. Critical Success Factors for Effective IT Governance in the Public Sector Organizations in a Developing Country: The Case of Tanzania. In Proceedings of the ECIS 2010, 18th European Conference on Information Systems, Pretoria, South Africa, 7–9 June 2010.
2. Salami, O.L.; Johl, S.K.; Ibrahim, M.Y. Holistic Approach to Corporate Governance: A Conceptual Framework. *Glob. Bus. Manag. Res* **2014**, *6*, 251.
3. Weber, K.; Otto, B.; Osterle, H. One Size Does Not Fit All—A Contingency Approach to Data Governance. *ACM J. Data Inf. Qual.* **2009**, *1*, 4. [CrossRef]
4. Begg, C.; Caira, T. Exploring the SME Quandary: Data Governance in Practise in the Small to Medium-Sized Enterprise Sector. *Electron. J. Inf. Syst. Eval.* **2012**, *15*, 3–13.
5. Buffenoir, E.; Bourdon, I. Managing extended organizations and data governance. *Adv. Intell. Syst. Comput.* **2013**, *205*, 135–145.
6. Niemi, E. Designing a Data Governance Framework. In Proceedings of the IRIS Conference, At Oslo, Norway, 18 August 2011; Volume 14.
7. Rouse, M. Data governance definition. Available online: www.whatis.techtarget.com (accessed on 9 April 2017).

8. Al-Ruithe, M.; Benkhelifa, E.; Hameed, K. Key dimensions for cloud data governance. In Proceedings of the FiCloud 2016, The IEEE 4th International Conference on Future Internet of Things and Cloud, Vienna, Austria, 22–24 August 2016; pp. 379–386.
9. Wende, K. A Model for Data Governance—Organising Accountabilities for Data Quality Management. In *Proceedings of the 18th Australasian Conference on Information Systems*; University of Southern Queensland: Toowoomba, Australia, 2007; pp. 417–425.
10. Chao, L. (Ed.) Cloud Computing for Teaching and Learning: Strategies for Design and Implementation: Strategies for Design and Implementation. IGI Global, 2012. Available online: https://books.google.com.hk/books?hl=zh-TW&lr=&id=PKWeBQAAQBAJ&oi=fnd&pg=PR1&dq=Cloud+computing+for+teaching+and+learning:+strategies+for+design+and+implementation:+strategies+for+design+and+implementation.+IGI+Global&ots=K2qgWXdeuQ&sig=3MkVNY_ATWYVjYNuthdn6EPAl3g&redir_esc=y#v=onepage&q=Cloud%20computing%20for%20teaching%20and%20learning%3A%20strategies%20for%20design%20and%20implementation%3A%20strategies%20for%20design%20and%20implementation.%20IGI%20Global&f=false (accessed on 1 December 2017).
11. Fu, X.; Wojak, A.; Neagu, D.; Ridley, M.; Kim, T. Data governance in predictive toxicology: A review. *J. Cheminform.* **2001**, *3*, 24. [CrossRef] [PubMed]
12. Prasetyo, H.N.; Surendro, K. Designing a data governance model based on soft system methodology (SSM) in organization. *J. Theor. Appl. Inf. Technol.* **2015**, *78*, 46–52.
13. Panian, Z. Some Practical Experiences in Data Governance. *World Acad. Sci. Eng. Technol.* **2010**, *62*, 939–946.
14. Seiner, R.S. *Non-Invasive Data Governance*, 1st ed.; Technics Publications: New York, NY, USA, 2014.
15. Russom, P. *Data Governance Strategies: Helping Your Organization Comply, Transform, and Integrate*; The Data Warehousing Institute: Los Angeles, CA, USA, 2008.
16. Kamioka, T.; Luo, X.; Tapanainen, T. An Empirical Investigation of Data Governance: The Role of Accountabilities. In Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, 27 June–1 July 2016.
17. Poor, M. *Applying Aspects of Data Governance from the Private Sector to Public Higher Education*; University of Pregon: Eugene, OR, USA, 2011; Volume 1277, p. 125.
18. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*; NIST Special Publ.: Gaithersburg, MD, USA, 2011; Volume 145, p. 7.
19. Almarabeh, T.; Majdalawi, Y.K.; Mohammad, H. Cloud Computing of E-Government. *Commun. Netw.* **2016**, *8*, 1–8. [CrossRef]
20. Kshetri, N. Cloud computing in developing economies. *IEEE Comput.* **2012**, *43*, 47–55. [CrossRef]
21. Al-Ruithe, M.; Benkhelifa, E.; Hameed, K. Current State of Cloud Computing Adoption—An Empirical Study in Major Public Sector Organizations of Saudi Arabia (KSA). *Procedia Comput. Sci.* **2017**, *110*, 378–385. [CrossRef]
22. Bojanova, I.; Samba, A. Analysis of cloud computing delivery architecture models. In Proceedings of the 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA), Singapore, 22–25 March 2011; pp. 453–458.
23. Forell, T.; Milojicic, D.; Talwar, V. Cloud Management: Challenges and Opportunities. In Proceedings of the 2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), Shanghai, China, 16–20 May 2011; pp. 881–889.
24. Al-Ruithe, M.; Benkhelifa, E.; Hameed, K. A conceptual framework for designing data governance for cloud computing. *Procedia Comput. Sci.* **2016**, *94*, 160–167. [CrossRef]
25. Ko, R.K.L.; Jagadpramana, P.; Mowbray, M.; Pearson, S.; Kirchberg, M.; Liang, Q.; Lee, B.S. TrustCloud: A framework for accountability and trust in cloud computing. In Proceedings of the 2011 IEEE World Congress on Rvices (Services), Washington, DC, USA, 4–9 July 2011; pp. 584–588.
26. Bumpus, W. *NIST Cloud Computing Standards Roadmap*; NIST: Gaithersburg, MD, USA, 2010; pp. 1–3.
27. Ramachandra, G.; Iftikhar, M.; Khan, F.A. A Comprehensive Survey on Security in Cloud Computing. *Procedia Comput. Sci.* **2017**, *110*, 465–472. [CrossRef]
28. Sirimovu, J.U.N.; Artins, O.P. *A Decision Framework to Mitigate Vendor Lock-in Risks in Cloud (SaaS Category) Migration*; Bournemouth University: Poole, UK, 2017.
29. Jennings, B.; Stadler, R. Resource Management in Clouds: Survey and Research Challenges. *J. Netw. Syst. Manag.* **2013**, *23*, 567–619. [CrossRef]

30. Rifaie, M.; Alhajj, R.; Ridley, M. Data governance strategy: A key issue in building enterprise data warehouse. In Proceedings of the iiWAS '09, 11th International Conference on Information Integration and Web-Based Applications & Services, Kuala Lumpur, Malaysia, 14–16 December 2009; pp. 587–591.
31. Neela, K.L.; Kavitha, V. A Survey on Security Issues and Vulnerabilities on Cloud Computing. *Int. J. Comput. Sci. Eng. Technol.* **2013**, *4*, 855–860.
32. Thomas, G. *The DGI Data Governance Framework*; Data Gov. Institute: Orlando, FL, USA, 2006; Volume 20.
33. Cheong, L.K.; Chang, V. The Need for Data Governance: A Case Study. In Proceedings of the 18th Australasian Conference on Information System, Toowoomba, Australia, 5–7 December 2007; Volume 100, pp. 999–1008.
34. Ladley, J. *Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program*; Newnes: Boston, MA, USA, 2012.
35. Verhoef, C. Quantifying the effects of IT-governance rules. *Sci. Comput. Program.* **2007**, *67*, 247–277. [CrossRef]
36. De Haes, W.V.G.S. Practiices in IT Governance and Business/IT alignment. *Inf. Syst. Control* **2008**, *2*, 1–6.
37. Otto, B. A Morphology of the Organisation of Data Governance. In Proceedings of the Conference 19th European Conference on Information Systems (ECIS 2011), Helsinki, Finland, 9–11 June 2011; p. 272.
38. HIMSS Clinical & Business Intelligence Committee. *A Roadmap to Effective Data Governance: How to Navigate Five Common Obstacles*; HIMSS Clinical & Business Intelligence Committee: Chicago, IL, USA, 2015.
39. Guillory, K. The 4 Reasons Data Governance Fails. Available online: http://www.noah-consulting.com/experience/papers/4%20Reasons%20Data%20Governance%20Fails%20-%20Guillory.pdf (accessed on 1 December 2017).
40. Héroux, S.; Fortin, A. The influence of IT governance, IT competence and IT-business alignment on innovation. In Proceedings of the 2016 Canadian Academic Accounting Association (CAAA) Annual Conference, Centre St. John's, NL, USA, 2–4 June 2016; pp. 1–36.
41. Salido, J.; Manager, S.P.; Group, T.C.; Corporation, M.; Cavit, D. A Guide to Data Governance for Privacy, Confidentiality, and Compliance. *Microsoft Trust. Comput.* **2010**, *6*, 17.
42. Cloud Security Alliance. *Cloud Data Governance Research Sponsorship*; Cloud Security Alliance: Seattle, WA, USA, 2012.
43. Adelman, S. Without a Data Governance Strategy. *DM Rev.* **2008**, *18*, 32.
44. Otto, B. Data governance. *Bus. Inf. Syst. Eng.* **2011**, *3*, 241–244. [CrossRef]
45. Hallikas, J. *Data Governance and Automated Marketing—A Case Study of Expected Benefits of Organizing Data Governance in an ICT Company*; University of Helsinki: Helsinki, Finland, 2015; pp. 1–89.
46. Kitchenham, B.; Charters, S. Guidelines for performing Systematic Literature Reviews in Software Engineering. *Engineering* **2007**, *2*, 1051.
47. Buffenoir, E.; Bourdon, I. Reconciling complex organizations and data management: The Panopticon paradigm. *arXiv*, 2012.
48. Badrakhan, B.B. Drive toward Data Governance. Available online: http://www.ewweb.com/e-biz/drive-toward-data-governance (accessed on 1 December 2017).
49. Weber, K.; Cheong, L.; Otto, B.; Chang, V. Organising Accountabilities for Data Quality Management-A Data Governance Case Study. In Proceedings of the Conference DW2008: Synergies through Integration and Information Logistics, St Gallen, Switzerland, 27 October 2008; pp. 347–359.
50. Office, D.G. *The State of New Jersey Data Governance Framework Strategic Plan*; New Jersey University: Jersey City, NJ, USA, 2013.
51. Neff, A.; Schosser, M.; Zelt, S.; Uebernickel, F.; Brenner, W. Explicating performance impacts of it governance and data governance in multi-business organisations. In Proceedings of the 24th Australasian Conference on Information Systems (ACIS), Melbourne, Australia, 4–6 December 2013.
52. Kunzinger, F.; Corporation, H.; Haines, P.; Consulting, N.; Schneider, S.; Solutions, V. Delivering a Data Governance Strategy that Meets Business Objectives. In Proceedings of the 14th International Conference on Petroleum Data Integration, Data & Information Management, Houston, TX, USA, 17–19 May 2010.
53. Mary, B.; Mccarthy, P.; Hill, S. Cloud Adoption Points to IT Risk and Data Governance Challenges. Available online: https://www.in.kpmg.com/SecureData/ACI/Files/cloudadoptiondaaprilmay2011.pdf (accessed on 1 December 2017).

54. Soares, S. *The IBM Data Governance Unified Process: Driving Business Value with IBM Software and Best Practices*; Mc Press: Chicago, IL, USA, 2010; p. 153.
55. Allen, C.; Jardins, T.R.D.; Heider, A.; Lyman, K.A.; McWilliams, L.; Rein, A.L.; Schachter, A.A.; Singh, R.; Sorondo, B.; Topper, J.; et al. Data governance and data sharing agreements for community-wide health information exchange: lessons from the beacon communities. *EGEMS* **2014**, *2*, 1057. [CrossRef] [PubMed]
56. Nunn, S. Driving Compliance through Data Governance. *J. AHIMA* **2009**, *80*, 50–51. [PubMed]
57. Imhanwa, S.; Greenhill, A.; Owrak, A. Designing Data Governance Structure: An Organizational Perspective. *GSTF J. Comput.* **2013**, *4*, 1–10.
58. Bhansali, N. *Data Governance: Creating Value from Information Assets*; Auerbach Publications: Boca Raton, FL, USA, 2014.
59. Sarsfield, S. *Data Governance Imperative*; IT Governance Publishing: Cambridgeshaire, UK, 2009.
60. Felici, M.; Koulouris, T.; Pearson, S. Accountability for Data Governance in Cloud Ecosystems. In Proceedings of the 2013 IEEE 5th International Conference on Loud Computing Technology and Science (Cloudcom), Bristol, UK, 2–5 December 2013; pp. 327–332.
61. Groß, S.; Schill, A. Towards user centric data governance and control in the cloud. In Proceedings of the International Workshop on Open Problems in Network Security (iNetSec), Lucerne, Switzerland, 9 June 2011; pp. 132–144.
62. Wendy, Y. Is data governance in cloud computing still a mirage or do we have a vision we can trust. *Softw. World* **2011**, *42*, 15.
63. Mustimuhw Information Solutions Inc. *Data Governance Framework: Framework and Associated Tools*; Mustimuhw Information Solutions Inc.: Duncan, BC, Canada, 2015.
64. Best Practices in Enterprise Data Governance. Available online: https://www.sas.com/content/dam/SAS/en_ca/doc/other1/best-practices-enterprise-data-governance-106538.pdf (accessed on 1 December 2017).
65. Russom, P. Data Governance strateGies. *Bus. Intell. J.* **2008**, *13*, 13–15.
66. Thomas, G. How to Use the DGI Data Governance Framework to Configure Your Program. Data Gov. Inst. Available online: www.DataGovernance.com (accessed on 23 June 2016).
67. Australian Institute of Health and Welfare. *AIHW Data Governance Framework 2014 (AIHW)*; Australian Institute of Health and Welfare: Canberra, Australia, 2014.
68. Loshin, D. *Operationalizing Data Governance through Data Policy Management*; Knowledge Integrity, Inc.: Washington, DC, USA, 2010.
69. Adler, S. *The IBM Data Governance Council Maturity Model: Building a Roadmap for Effective Data Governance*; IBM Corporation: Somers, NY, USA, 2007.
70. Salido, J. Data Governance for Privacy, Confidentiality and Compliance: A Holistic Approach. *ISACA J.* **2010**, *6*, 1–7.
71. Hunter, L. Tools for Cloud Accountability: A4Cloud Tutorial. 2015. Available online: http://www.a4cloud.eu/node/362 (accessed on 4 November 2015).
72. Solutions, C. *Data Governance in the Cloud*; Cloud Industry Forum: York Road Maidenhead, UK, 2013.
73. Tountopoulos, V.; Athens Technology Center. The Problem of Cloud Data Governance. Available online: http://www.cspforum.eu/uploads/Csp2014Presentations/Track_13/The%20problem%20of%20cloud%20data%20governance.pdf (accessed on 4 November 2015).
74. Cloud Security Alliance, Cloud Data Governance Working Group, 2015. Available online: https://cloudsecurityalliance.org/group/cloud-data-governance/ (accessed on 21 May 2015).
75. Alexandria, V. Despite Data Governance Efforts, Eighty-Nine Percent of Federal IT Professionals Are Apprehensive about Migrating IT Services to the Cloud, 2014. Available online: http://www.businesswire.com/news/home/20140909005167/en/Data-Governance-Efforts-Eighty-Nine-Percent-Federal-Professionals#.VeV27Jrovcc (accessed on 12 July 2015).
76. Youssef, A. Exploring Cloud Computing Services and Applications. *J. Emerg. Trends Comput.* **2012**, *3*, 838–847.
77. Government, A. The National Cloud Computing Strategy. *Natl. Broadband Netw.* **2013**, *2013*, 36.
78. Preittigun, A.; Chantatub, W. A Comparison between IT Governance Research and Concepts in COBIT 5. *Int. J. Res. Manag. Technol.* **2012**, *2*, 581–590.
79. Lee, S.U.; Zhu, L.; Jeffery, R.; Group, A.P. Data Governance for Platform Ecosystems: Critical Factors and the State of Practice. *arXiv*, 2017.

80. Herbst, N.R.; Kounev, S.; Reussner, R. Elasticity in Cloud Computing: What It Is, and What It Is Not. In Proceedings of the 10th International Conference on Autonomic Computing, San Jose, CA, USA, 26–28 June 2013; pp. 23–27.
81. Debreceny, R.S.; Gray, G.L. IT Governance and Process Maturity: A Multinational Field Study. *J. Inf. Syst.* **2013**, *27*, 157–188. [CrossRef]
82. Kooper, E.; Maes, M.R.; Lindgreen, R. Information Governance as a Holistic Approach to Managing and Leveraging Information Prepared for IBM Corporation. *Int. J. Inf. Manag.* **2011**, *31*, 1–27.
83. Williams, P.A.H. Information governance: a model for security in medical practice. *J. Digit. Forensics Secur. Law* **2007**, *2*, 57–74. [CrossRef]
84. Gartner, Information Governance. 2016. Available online: http://www.gartner.com (accessed on 17 May 2017).
85. Woldu, L. *Cloud Governance Model and Security Solutions for Cloud Service Providers*; Metropolia Ammattikorkeakoulu: Helsinki, Finland, 2013.
86. Saidah, A.S.; Abdelbaki, N. A new cloud computing governance framework. In Proceedings of the CLOSER 2014, International Conference Cloud Computing Services Science, Barcelona, Spain, 3–5 April 2014; pp. 671–678.
87. Kofi, J.; Kwame, K. Who 'owns' the cloud? An empirical study of cloud governance in cloud computing in ghana. In Proceedings of the 28th European Regional Conference of the International Telecommunications Society (ITS), Passau, Germany, 30 July–2 August 2017.
88. Olaitan, O.; Herselman, M.; Wayi, N. 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 (SAIMS), Pretoria, South Africa, 4–7 September 2016.
89. Sein, M.K.; Henfridsson, O.; Rossi, M. Research essay action design research. *MIS Q.* **2011**, *30*, 611–642.
90. Jansen, W.; Grance, T. Guidelines on Security and Privacy in Public Cloud Computing. Available online: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf (accessed on 1 December 2017).
91. Grant, O.I. *Oklahoma Interoperability Grant Project Oklahoma Interoperability Grant Data Roadmap*; US Department of Health and Human Services: Washington, DC, USA, 2013.
92. Bell, R. *Institutional Data Governance Policy*; Vanderbilt University and Medical Centre: Nashville, Tennessee, 2014; pp. 1–12.
93. Farrell, R. Securing the Cloud—Governance, Risk, and Compliance Issues Reign Supreme. *Inf. Secur. J. Glob. Perspect.* **2010**, *19*, 310–319. [CrossRef]
94. Wende, K. Data Governance Defining Accountabilities for Data Quality Management. In Proceedings of the Italian Workshop on Information Systems (SIWIS 2007, Side Event of ECIS 2007), Carisolo, Italy, 9–14 February 2007.
95. Theoharidou, M.; Papanikolaou, N.; Pearson, S.; Gritzalis, D. Privacy risk, security, accountability in the cloud. In Proceedings of the 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), Bristol, UK, 2–5 December 2013; pp. 177–184.
96. Trivedi, H. Cloud Adoption Model for Governments and Large Enterprises. Master's Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2013.
97. Weber, R.; Iruka, I. *Best Practices in Data Governance and Management for Early Care and Education: Supporting Effective Quality Rating and Improvement Systems*; U.S. Department of Health and Human Services: Washington, DC, USA, 2014.
98. Power, D.; Street, W. Sponsored by All the Ingredients for Success: Data Governance, Data Quality and Master Data Management. *Hub Solut. Des.* **2013**, *2043*, 1–20.
99. Cloud Standards Customer Council (CSCC). *Security for Cloud Computing 10 Steps to Ensure Success*; Cloud Standards Customer Council: Needham, MA, USA, 2012; pp. 1–35.
100. Cloud Standards Customer Council. *Practical Guide to Cloud Service Level Agreements Version 1.0*; Cloud Standards Customer Council: Needham, MA, USA, 2012; pp. 1–44.
101. Bulla, C.M.; Bhojannavar, S.S.; Danawade, V.M. Cloud Computing: Research Activities and Challenges. *Int. J. Emerg. Trends Technol. Comput. Sci.* **2013**, *2*, 206–214.
102. Badger, L.; Grance, T.; Corner, R.P.; Voas, J. *Cloud Computing Synopsis and Recommendations*; NIST Publications: Gaithersburg, MD, USA, 2011.
103. Chawngsangpuii, R.; Das, R.K. A challenge for security and service level agreement in cloud computing. *Int. J. Res. Eng. Technol.* **2014**, 2319–2322. [CrossRef]

104. Cochran, M.; Witman, P.D. Governance and service level agreement issues in a cloud computing environment computing environment. *J. Inf. Technol. Manag.* **2011**, *22*, 41–55.
105. Goals, S.; Dyche, J.; Levy, E. *Data Governance: Getting It Right!* GFT: Stuttgart, Germany, 2015; pp. 1–3.
106. Alkhater, N.; Wills, G.; Walters, R. Factors Influencing an Organisation's Intention to Adopt Cloud Computing in Saudi Arabia. In Proceedings of the 2014 IEEE 6th International Conference on Loud Computing Technology and Science (CloudCom), Singapore, 15–18 December 2014; pp. 1040–1044.
107. Khajeh-Hosseini, A.; Sommerville, I.; Sriram, I. Research Challenges for Enterprise Cloud Computing. *arXiv*, 2010.
108. Confidential, W.S.; Reserved, A.R. *Holistic Approach to Key Challenges Unstructured Data Governance Holistic Approach to Key Challenges*; WhiteBox: Schwyz, Switzerland, 2012.
109. Van der, L.M. *Measuring Data Governance*; Leiden University: Leiden, The Nederland, 2015; p. 89.
110. Cloud Standards Customer Council. Security for Cloud Computing Ten Steps to Ensure Success. Available online: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf (accessed on 14 August 2016).
111. Brett. *Data Governance Best Practices and Trends within South African Companies*; Glue Data: Cape Town, South African, 2009.