A Conceptual Framework to Determine the Digital Forensic Readiness of a Cloud Service Provider

Mpho Percy Makutsoane, Awie Leonard
Department of Informatics, School of Information Technology, University of Pretoria, Pretoria, South Africa

Abstract— **In the digital age, organisations tend to invest large sums of their finances into technology because of the demand from business to handle their data efficiently. As these organisations grow, ubiquitous systems are required to securely store their big data. Cloud computing has emerged as a solution to this demand for a reliable and cost effective alternative to organisations. However, some organisations are skeptical about cloud computing as an ideal solution because of its pronounced susceptibility of privacy, data leakage and cyber-attacks through virtual networks.**

Hence, it is pivotal for organisations to have a certain level of confidence in the Cloud Service Provider (CSP) that they select as their cloud vendor. Digital forensic readiness is one of the metrics that organisations can use to measure the CSPs' ability to thwart cyber-crimes. This paper proposes a framework based on literature and risk analysis techniques that organisations may apply when they want to migrate to the cloud. The proposed framework is a process tool to select a CSP that can provide an organisation with a digital forensic readiness cloud solution.

I. INTRODUCTION

Over the years, traditional computing has undergone major changes from the inception of ARPANET, to the Internet and web services. The evolution of web services has resulted in the innovation of loosely coupled Service Oriented Architecture (SOA) and Web 2.0. The systems management (e.g. data centre automation) and distributed computing (e.g. utility and grid computing) services have had an influence on the growth and interest toward cloud computing from both industry and academic spheres [1]. It is estimated in Indonesia that by 2016, many organisations will host a significant amount of their data on the cloud [2]. With many organisations migrating to the cloud it is important to take into account potential security concerns. [3] defines security as the protection of assets and knowing the value attached to those assets. Digital forensics is a component of security which specialises in the development of mechanisms to understand cyber-crimes and implement systematic principles once a crime has occurred [4]. Cloud Forensics has emerged as a de facto term used interchangeably with digital forensics within the context of cloud computing. One of the early emergences of cloud forensics was in the paper by [5], the term was coined based on an overview of a three dimensional model which encapsulates legal, organisational and technical elements to be considered pertaining cloud computing and digital forensics. However, in this paper the authors have adopted Digital Forensics as the de facto term.

The National Institution of Standards and Technology (NIST) defines cloud computing as "a model for enabling 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" [6]. The three main cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [28]. Cloud computing is also stacked according to the hosting models referred to as Public, Private, Hybrid and Community cloud [7]. The stack services and deployment models are important because they have an impact on the complexity of a cloud computing architecture. Cloud computing is typically used by organisations as a pay as you go model similar to the current business structures of small and large organisations outsourcing their business needs to third party vendors for utility resources such as water and/ or electricity. Paying only for required resources yields efficient operational costs on hardware and software infrastructures for organisations because their resources are leveraged only towards their business needs. [2] argue that this approach results in a faster return on investment (ROI) and lower total cost of ownership (TCO) for organisations when their resources are hosted on the cloud. However, cloud computing still poses some threats to organisations' business operations and to the personal information of their employees. According to [8] the fraudulent behaviour that happens through cyber-crimes results in security susceptibility to the organisations' data that is hosted on the cloud. The onus of responsibility over the data thus becomes a contentious issue because of the legal jurisdictions, bylaws, deployment models and Service Level Agreement (SLA) terms and conditions.

In this article we propose a framework that optimally minimises risks for an organisation that is considering hosting their data through a Cloud Service Provider (CSP). We apply Digital forensic readiness within the framework to evaluate CSPs' ability to thwart cyber-crimes and as a means of accountability from a digital forensic readiness perspective. As well, risk analysis tools and techniques are applied within the framework as resources for organisations to attain effective decision making. Finally, we present an analysis on the proposed framework by industry experts as means to scientifically validate it. The framework serves as a tool to reduce security vulnerability for organisations and also provides a systematic approach to a complex decision support system. The framework is not necessarily a generic 'one size fits all' solution, but because of its openness and adaptability, the framework can serve as an optimal solution for decision makers in different fields. Its effectiveness is also based on the open mindedness and intuitive application by respective

stakeholders; hence it is presented as a conceptual framework that can be scaled as required.

II. METHODOLOGY

In this study, we use an interpretive approach to carry out the research. The development of the framework is based on literature and the authors' observations on organisations' decision processes when in the process of electing to host their data on the cloud. The interpretivism approach seeks to understand and study the social world through behaviour as well as other complexities of human emotions, desires and norms [9]. Scholarly influences and the researcher's views of the world will form part of the development of the framework. According to [10], the ontological and epistemological approaches found in the philosophical paradigms are reflected in the beliefs and thinking of the particular school of thought, as it is observed in this paper. Therefore, it is important for the development of the proposed framework and the research as a whole that the authors are objective and free from subjective influences.

III. DIGITAL FORENSICS AND ITS COMPLEXITIES

Studies and practices on digital forensics primarily focused on networks, mobile computing and computer crimes. [11] justifies the notion of slow progression of digital forensic research within cloud computing to be a result of many challenges that are common in traditional computing. [12] claims that one of the contributing factors to this challenge is that security was not factored as a major concern when computers were developed hence there are inherent security vulnerabilities in cloud computing. [12] further argues that within traditional computing and cloud computing, end-users tend to be technologically unsophisticated whereas attackers are characteristically more technologically advanced. End-users are usually not aware of technical security risks involved in computing hence majority of them use same passwords within many of their private domains and seldom encrypt their personal data [3]. The users are also oblivious to simple but yet deceptive tactics practiced in social engineering [13]. In contrast, attackers tend to use intricate techniques and tools when they intrude information systems. These complex techniques include masquerading and spoofing their Internet Protocol (IP) addresses through proxy servers and virtual machines.

The attackers' ability to spoof their IP addresses on a Dynamic Host Control Protocol (DHCP) or Media Access Control (MAC) addresses are part of the complexities faced by digital forensic examiners. Through the Internet, an attacker can direct a hit to be from totally different location than where the host may actually reside at [14]. Computer networks and mobile computing face unique cyber threats hence the need for more rigorous technological advancements. These threats are also inherent even in cloud computing although they are not discussed in depth. These outlined concerns are vital to take into consideration within the development of the proposed framework.

IV. THE CYBER-CRIME SCENE

Crimes committed on cyber space are more complicated than on physical space because of the ubiquitous nature of the Internet [11]. The Locard's Exchange Principle expresses that "anyone or anything, entering a crime scene takes something of the scene with them and leaves something of themselves behind when they leave" [15]. This principle serves as a fundamental tool for a digital forensic examiner when evaluating many intricacies involved in a cyber-attack. The Locard's Exchange Principle is based on a triangular model based on the notion that a crime must be attributed to an attacker through irrefutable evidence. The model constitutes a suspect, the crime scene and the victim through a complicated relationship. These are vital components that are typically found on any crime scene, physical or cyber space. The Locard's Exchange Principle infers behavioural imprints through the common Latin term "Modus Operandi". The Modus Operandi means understanding the suspect's motivation, their knowledge of the victim and of a crime scene. In the understanding of the crime scene, a digital forensic examiner can deduce necessary details to uncover obscurities within a cloud computing environment.

A cyber-crime scene on a cloud computing environment has changed from traditional computing because of the technological architectures of hypervisors found on the cloud. The concept of virtualisation has drastically changed within the cloud environment because of the capability of a CSP hosting many cloud instances at a given time. A hypervisor is also referred to as a Virtual Machine Manager (VMM), which is an application that hosts multiple operating systems that run concurrently on the cloud. A user can then dynamically switch between any of the operating systems within a short period of time hence the need for digital forensic readiness in cloud computing. The complexities of virtualisation are some of the challenges that the proposed framework aims to address through the SLAs.

V. CLOUD COMPUTING ROLE AND IMPACT ON DIGITAL FORENSICS

In the paper by [16], a 2009 Gartner survey indicated that 70% of respondents do not intend on using cloud computing because of data privacy and other security concerns. In 2009, an incident was reported that Google's user's files were disclosed to unauthorised users [16]. As argued by [17], large CSPs claim that data hosted on the cloud is more secure because data is stored on multiple data centres in many different geographic locations. The reason is that even if a cataclysmic incident can occur at any of their data centres, the data remains safe because it is stored in multiple locations. A contrasting view is that sensitive corporate data stored on those data centres can be vulnerable to privacy or terrorism

attacks should the data centres be located in targeted countries [18].

Privacy in cloud computing is a major concern for organisations because different CSPs provide different cloud solutions and abide by different internal policies and country bylaws. A challenge for organisations is their lack of knowledge over who has access to their data. SLAs are important in the discussion of privacy because they evaluate many concerns such as authorisations and accessibility on organisations' data on the cloud. Mechanisms such as encryption and data hiding are possible solutions in ensuring privacy but they also have inherent shortfalls. In accordance to this claim, [19] states that public key encryption is insufficient for cloud services because of the vulnerabilities of the traditional public key encryption techniques. Thus, further mechanisms or solutions must be explored to ensure privacy hence we are proposing the framework.

A major difference between traditional computing and cloud computing is that the owner of the machine knows the location of their Information Systems (IS) physical infrastructure and its capabilities. Whereas the owner can intuitively decide to unplug the entire network connections anytime and switch off any wireless capabilities of their machine to ensure certain level of privacy. According to [20], majority of organisations and power users of cloud solutions have no knowledge of the location of the physical mediums that stores their data. As indicated earlier, knowledge of the location of the storage medium is important for a digital forensic examination purposes. The legal concerns are omitted in the implementation of the framework as they are assumed to be part of the digital forensic readiness methodology that may be followed.

VI. THE FRAMEWORK

This section is a discussion of the proposed framework which is referred to as Cloud Capability Decision Framework (C^2DF). C^2DF is indirectly developed in accordance to risk analysis models, the Mehari, Magerit, NIST8 and Microsoft Security Management Guide.

For a cloud solution to be considered a genuine cloud service; there must be customisation, self-service, elasticity and per-usage metering [1]. SaaS and PaaS, offer less flexibility in customisation as compared to IaaS because it is typically developed for a particular purpose [22]. However, both SaaS and PaaS offer certain degree of customisation by allowing tenants to Create Read Update and Delete (CRUD) their applications. The effectiveness of C^2DF is not dependent on the selection of a particular cloud service or deployment model. The major difference on the selection is mainly on the SLAs and the level of digital forensic readiness required. Irrespective of IaaS, PaaS, SaaS, the cloud must enable self-service since tenants require on demand access at any given instance. There should also be capabilities to quickly provision and deploy these resources through limited interaction with the CSP [6].

For a pragmatic application of C^2DF it is recommended that ethics should be practiced by all the relevant stakeholders. It is an important feature although it may mean different things to different schools of thought. Hence the reader is referred to [23] who developed a model with a taxonomy based on terms related to virtue, morality, integrity, legality and ethics. [24] made a study on ethics through 10-K annual reports which are regulatory annual reports that should be mandatorily released by USA firms. The research studied the 10-K annual reports from 1994 until 2006. The results from the research form an empirical analysis for the taxonomy of the framework the authors developed. The results from [23] indicate that majority of firms that make use of phrases like 'ethics' in their 10-K reports are likelier to 'sin' their stocks and/or have cases in which they were defendant of lawsuits. It is an empirical illustration that explicitly declaring you are ethical does not mean that you are actually practicing or behaving ethically. It is for this reason the relevant stakeholders should rather practice ethics as it is understood from [24].

A. Preliminary Assumptions

To apply the framework, it is suggested that several assumptions should be considered as they are listed below:

a. The CSP will provide the history of breaches that have occurred on their cloud infrastructures.
b. The CSP will disclose some legal polices and bylaws that it abides by. Information such as location of data centres and jurisdictions may also be disclosed upon agreement by both parties.
c. The organisation together with the CSP will agree on the optimal deployment and service model according to the organisation's needs and capabilities of the CSP.

TABLE I.
DEPLOYMENT AND SERVICE MODEL ARCHITECTURE

Deployment	Service	Deployment	Service	Deployment	Service
Public	SaaS PaaS IaaS	Private	SaaS PaaS IaaS	Community	SaaS PaaS IaaS

The framework follows a sequential methodological approach. Within phases 1, 2, 3 and 4, there are steps which are labeled with symbols (i) which depict iterative processes. These steps are not in a sequential order and can be repeated if deemed necessary.

B. Risk Analysis

This section is an overview of the application of the risk analysis model within the context of C^2DF. Fig.1 is an illustration of a risk analysis process model followed within the C^2DF, it is extracted from [25]. According to [26], risk analysis processes may differ with organisations because of the type of industry, personnel involved and based practices of internal preparations of risk systems. Hence other risk analysis tools can be followed as deemed relevant.

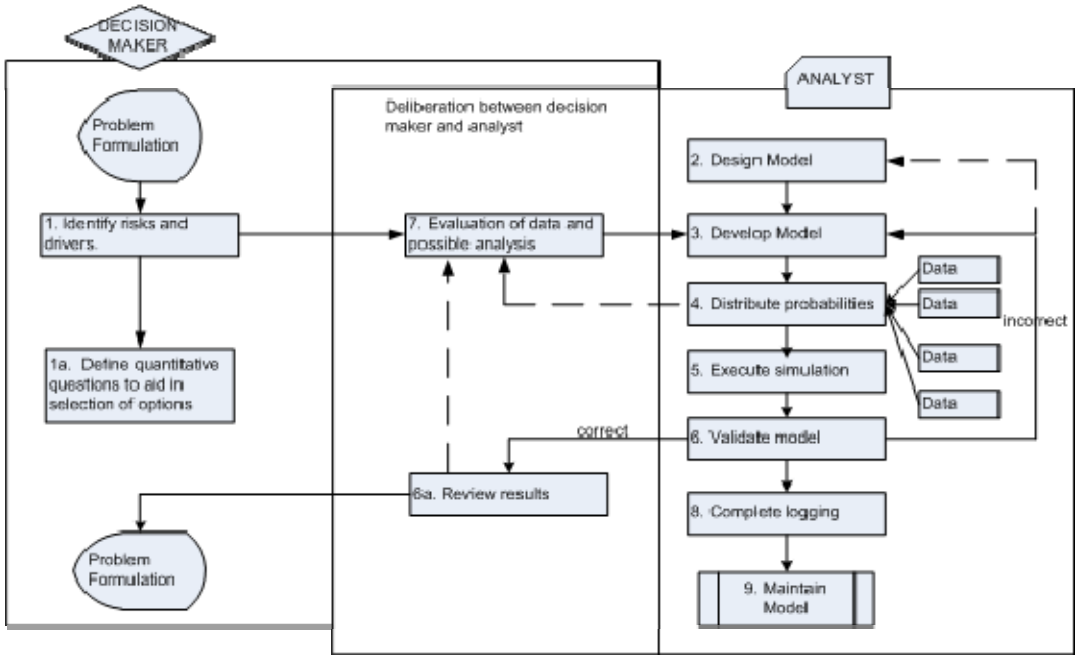

Fig. 1. An Integrated Risk Analysis Model [25]

The risk analysis model is systematic because it provides a trace and accountability on the decision making process. The application of the risk analysis model within C^2DF is to provide a trace in which auditors can re-engineer processes which were followed to reach a particular decision. It also serves as a probabilistic tool to evaluate the level of certainty for the final decision that has to be made.

1) Identification

A prompt list is developed to systematically classify different structures studied. Based on the thoroughness required, several prompt lists may be created as comparison hence why a prompt list cannot be exhausted. Outlined in Table 2 is a brief general project prompt list which can be divided further into subsection for an individual category.

Within the context of C^2DF, the prompt list is used to identify the industry of the particular organisation that is analysed. Once the industry type is established, further details are examined as illustrated within Table 2. Knowledge of the particular industry makes it easy to intuitively and quantitatively understand the sensitivity of the data that the organisation handles and the type of data that will be provided to the CSP. The sensitivity of the data is relative; however, contextualising its sensitivity provides a memorandum of understanding (MoU) between the organisation and the CSP.

2) Process Narration Overview

Fig. 1 is an illustration of a risk analysis process model. It is a high level illustration of different sub-processes within C^2DF. The process is an overall application of C^2DF. The dotted lines represent possible outcomes/actions, whereas the straight thick lines are normal outcomes/actions. The cone shape (problem formulation) depicts the start and an end to a particular action that has to be taken. The square boxes represent a particular action/ step that may be taken to reach a decision. The risk analysis process is a precursor to an implementation of the proposed framework.

TABLE II: PROMPT LIST [25]

Technical
Abstraction of Organisation's staff
Environmental
Financial
Education
Social

SUBSECTION
Abstraction of Organisation's staff
- Social class
- Education level
- Tax bracket
- Gender
- Age
- Social class

NB: Please note that the numbering on the mode references with the numbering of the steps below.

Decision Maker

1) The Decision maker formulates the problem. Within C^2DF, the problem in this case is migrating to the cloud.
   1a) Important and difficult questions are defined by the Decision maker. These questions may be posed to the CSP and also serve as an analysis to complex qualitative issues.

This step precedes the Decision maker's evaluation of data and results from the Analyst.

The results are reviewed together with the Analyst for validation.

Analyst

2) The analyst designs the model according to C^2DF phases.
3) Once the Decision maker accepts the model, then the model is developed. The model is developed according to the industry of the organisation. However, it follows the best practices model of the C^2DF. The phases are highlighted in the section that follows and the model will be clear as to how it is developed.
4) The analyst validates the data from the CSP:
   - Past breaches
   - Virtual machines managers
   - Storage capacity of hypervisors
   - Current clients
   - Digital forensic readiness information
   - Number of data centres

   The probabilities may be evaluated by the decision maker if it is deemed necessary. The Decision maker may request for further probabilities or data to be modeled.
5) A simulation to prepare the data for analysis is developed.
6) For quality assurance purposes, the results from the simulation model are validated. If discrepancies are discovered, go back to step 3 to modify or develop a new model. If necessary, may go back to the design of the model in step 2.
7) If the results are satisfactory, the results are reviewed together with the Decision maker from the organisation.
8) A report is compiled for the decision maker with the choice of CSP.
9) The model is maintained periodically. This entails validation of agreed SLAs and that the relationship between the organisation and the CSP is still is accordance.

C. Model Application

Phase 1: Evaluation of the organisation

i. CSP Perspective

The first phase is an evaluation of the organisation. This phase is intended for the organisation to disclose its policies and procedures to the respective CSP; as a result an SLA is established.

1) Size of The Organisation

This step requires the organisation to disclose its size to the CSP. There are many metrics used to validate an organisation's size, however, Table 3 is used for illustration purposes only. The grid is a simplistic tool based on an independent survey used to evaluate organisations' size. It is the discretion of an organisation to use any preferred system, methodology or measurement to evaluate its size. An ad hoc tool may be required because the size of an organisation is relative based on the economies of scale and industry types.

TABLE III.
ILLUSTRATIVE ORGANISATIONAL SIZE MODEL

Number of Staff	Annual Revenue Thousands ($)		
	1 - 99,000	100,000 - 249,000,	250,000+
1- 999	A	C	E
1000 -9,999	C	C	E
10,000+	E	E	E

Legend	
Symbol	Size
A	Small organisation
C	Medium organisation

2) Policies and procedures:

It is recommended that within C^2DF, internal policies should be stipulated and made clear to all its employees throughout the organisation. Employees of the organisation should be aware of procedures to follow in case there is a breach or data has been destroyed. The Analyst can then categorise the organisation according to list (Control Oriented, Choice Oriented, Innovative Oriented or Hands-off). The categorisation is qualitative and is used to indicate the nature of the organisation. The Analyst can use this information to compile the information for the CSP.

Control Oriented: This type of organisation requires military style of approach with the protection of its data. A control oriented organisation would require a certification body such as International Traffic in Arms Regulation (ITAR) to approve the SLA between the CSP and them. The organisation is very particular with how their data is handled and requires full disclosure of technical information and business rules concerning configuration on their cloud instances. The data should be encrypted and maintenance policies used by the CSPs should comply with ITAR.

Any breaches that would occur whilst host the organisation's data is hosted, this would result in legal actions against the CSP. A control oriented organisation typically deals with very sensitive data, hence it independently takes extra measures to protect and hide their data themselves as well. The CSP has no knowledge of the contents of the data and is not allowed to attempt to view or decrypt it (should it be encrypted). An example of such an organisation can be federal agencies or banks because of the confidentiality of their information and monetary value attached to their data. The organisation has a high level of internal security expertise.

Choice-oriented: The requirement on the rigidness on protection of the data changes periodically. The sensitivity of the data changes significantly in different periods of the year. Therefore the value and sensitivity of the data impacts on how the data should be handled by the CSP.

Consulting firms would typically be classified as choice oriented. These are organisations which deal with various types of data that may change according to the clients they have on that particular period.

The level of expertise varies in degrees from high to low.

Innovation-oriented: This type of organisation is similar to choice-oriented, but the major difference is that the nature of their data does not determine policies and procedures taken with their data. Whether the data is classified as sensitive or not, there is no difference in how it is handled, stored or transported. An example of this type of organisation is of an undercover police, an intruder should not be able to determine the level of sensitivity of the data.

The CSP is not allowed to view the contents of the data but can execute maintenances without prior notice to the organisation. Therefore, the SLA can be modified and adaptable to different circumstances. Mines can be an example of such an organisation. The level of expertise is high due to the magnitude of the data.

Hands-off: This type of organisation does not handle their data at all; the responsibilities of the data are left to the CSP. The organisation is not particularly concerned with the status of the digital forensic readiness of the CSP. All the responsibilities of maintenance, memory and protection of the data are given to the CSP. In such an organisation, the SLA contract would typically have limited terms and conditions, however this can also vary because of the organisation's policies.

An example of this type of organisation is of a relatively small enterprise or a franchise that deals with non-essential merchandise such as a restaurant or stationary shop. The data is still important for competitors not to have access to, but it is classified as non-critical.

Phase 2: Evaluation of the Cloud Service Provider

i) Organisation Perspective

The Analyst determines the probability level of certainty. The certainty level is used to determine the margin of error pertaining to the digital forensic readiness of the CSP. The margin of error is used to determine the reliability of the decision taken by the organisation when choosing a particular CSP. For this step, the organisation uses statistical risk analysis tools such as Poisson to determine the certainty level. Alpha is used to represent significance levels: $\alpha = 0.1$; $\alpha = 0.05$; $\alpha = 0.01$. The margin of error provides a quantifiable measure on the trust the organisation has on the CSP according to the digital forensic readiness model in Fig. 2. This can be evaluated on the basis of what deployment model is offered by the CSP as highlighted in Table 1.

1) SLA terms and conditions

SLA is a contract that stipulates all the details with terms and conditions of operations, legalities and policies. It is used as a legal contract to clearly disclose information on the CSP's processes and capabilities. It is a legal agreement used to bind all parties involved. It also discloses all the services that the CSP provides and in some cases how they will be carried out.

Table 4 is an example of some of the services found within the Microsoft Security Management Guide. The table only shows three focal services that must be disclosed to the organisation on how services are handled and if they are catered for. However, a comprehensive list of services is found within the guide.

Table IV: CRITICAL SLA SERVICES

Available	Service Description
Provision	Capability to allow for dynamic changes based on needs of resources.
Security	Internet protocols to make use of SSL and other cloud centric encryption mechanisms.
Disaster	Recovery Capability of data centres to withstand natural disasters, terrorism and power cuts.

Legal basis of the CSP: In this step, the organisation evaluates any certificates or compliances of the CSP. For instance, with the ITAR certification, the organisation can evaluate how the CSP complies with it. Another legal aspect to consider involves the legislative bylaws of the country that the CSP abides by. However, in the Internet space, legalities tend to be very complicated because of the ubiquitous nature of the online environment.

Technical capabilities of the CSP: What formats of data are supported within the CSP cloud infrastructure (e.g. document formats such PDF, XML and DOC). An important question for a digital forensic examiner to pose is would the integrity and fidelity of the data be retained if data is migrated? Another question that is evaluated, does the CSP have Data Loss Prevention (DLP) tools to handle migration or distribution of data? These questions provide concerns that to be considered concerning the cloud environment.

Past Cases: The organisation evaluates how does the CSP handle its legal cases and which jurisdictions does it abide by. In this step, the organisation studies other clients of the CSP and the relationship that it has with them. Another aspect of past cases involves studying how the CSP has handled any cyber intrusions or conflicts.

Phase 3: Alignment of the Cloud Service Provider with Digital Forensic Readiness model

i. Organisation Perspective

In this phase, the organisation evaluates digital forensic readiness based on the model found in Fig. 2. There are a number of models that are used to evaluate digital forensic readiness and hence currently there is no single accepted standard. It is for this reason various models can also be used and manipulated to suit the particular environment. The model is an illustration of a group of essential components that an organisation may use to evaluate the digital forensic readiness of the CSP.

The compliance of digital forensic readiness is comprehensive thus the details are omitted to retain the scope of C^2DF. However, monitoring and constant awareness by all the relevant stakeholders of the CSP should always be included regardless of the model undertaken. It is vital that the CSP outlines its procedures and policies such that regular audits can be undertaken by external firms to test for the

digital forensic readiness on its cloud solution. This can provide a sense of trust from the organisation that the CSP abides with digital forensic readiness fundamental clauses. In this phase, the organisation retains all the details of the CSP's practices and policies of digital forensic readiness. As an example of applying the model, under strategy, the organisation would want to know what strategies are in place in case a breach occurs whilst data is on the cloud.

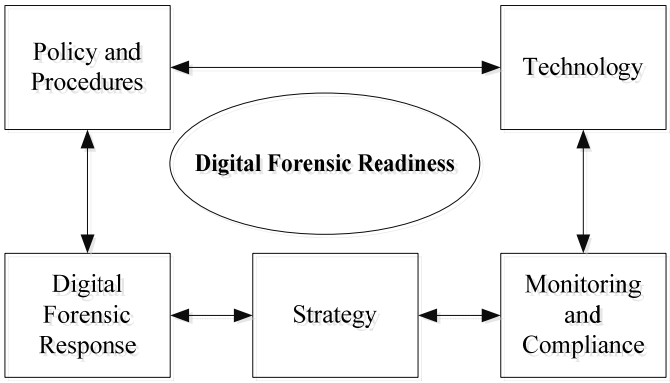

Fig. 2. Components of Digital Forensic Readiness [21]

Phase 4: Selection of the Cloud Service Provider

i. Organisation Perspective

In this phase, the organisation can choose at least two CSPs. In this regard, the organisation may apply basic intuitive approach in the selection of the CSP based on congruence of mutual policies. The selection at this point is based on results that have been extracted from the phase 1, phase 2 and phase 3. Another approach which is still under study is application of some of the more common probabilistic models' quantitative attributes can be used for selection. However, for the sake of completeness, it is assumed at this phase that the organisation would know if it would opt for a particular CSP or not based on the parameters that have been outlined.

D. Analysis of the Framework

Two experts from two different fields were consulted to provide feedback on C^2DF. The expert's feedback is discussed. A synopsis of the entire research was explained to the experts including a detailed overview from Assumptions to the Model application. Each expert was consulted at a separate location to avoid any influences or biasness from their different views. An in-depth explanation was made to each expert and thereafter sufficient time was allocated for each expert to analyse all the facets of C^2DF.

The authors took notes on all the comments the experts made. At the end of the discussion sessions with the each expert, a brief questionnaire was conducted. The questionnaire checked for the feasibility and relevance of C^2DF. The analysis is discussed according to the comments of each expert. Table 5 is a comparison of responses by the experts to a brief questionnaire.

1) Industry Expert's Comments

Expert 1 is an IT practitioner within the financial sector and is responsible for the security infrastructure of his/her respective firm. Expert 1 explained that their concern with phase 1 was with the metric used for evaluating an organisation's size was not comprehensive enough. The first concern was that evaluating the size of an organisation merely through the number of its staff is too ambiguous because there is no distinction with the employees (e.g. secretary, cleaners or security guards). The expert stated that some employees of an organisation do not directly use the cloud services. Therefore, another metric should be considered as an addition to the current system of evaluation. One of the suggestions was considering the number of workstations or actual users that interact with the cloud services in order to evaluate the size of the organisation. The expert stated that this gives a more accurate and relevant size of the organisation particularly from a CSPs' perspective.

Another feedback from expert 1 is that there is lack of clarity with the SLA criterion mainly on provision and security. The argument was that every CSP does provide some form of provisioning therefore the criterion should be more detailed. Thus the expert suggested specifying the functional and non-functional requirements that an organisation may request such as automation or manual provisioning.

2) Cloud Developer Industry Expert's Comments

Expert 2 is a developer for an ERP cloud based solution corporation. Expert 2 also commented on the table for evaluating the size of the organisation. The expert stated that the labour force factor has many discrepancies therefore another metric should be used to determine the size of an organisation. Also on the analysis of phase 1, expert 2 noted that an organisation must use a quantitative metric that clearly shows the sensitivity of their data. This gives an indication of the privacy and policies the CSP must apply in order to host the organisation's data. The expert made an example of the Coca Cola soft drink recipe. The expert explained that the recipe is very old, therefore, the Coca Cola Company requires a very secure cloud infrastructure because of the sensitivity of the recipe. The expert argued that the classification of the sensitivity of the data from 2) Policies and Procedures should be quantitatively categorised as supposed to the prescribed classification.

Expert 2 also reiterated that the Data ownership Policies of the CSP, particularly how the CSP handles data can also be re-evaluated. The expert made reference to Google Drive (cloud based storage medium) which has embedded algorithms that scans the data content. These algorithms scan data for spyware and also for extracting information that can be used for relevant advertisements to consumers. For an organisation such as Coca Cola Company, they would not want to have their data scanned or sniffed due to the high sensitivity of their data. Therefore within C^2DF, the

ownership of data should be clearly defined due to the technical implications on the cloud architecture.

Another input was with regard to phase 2; expert 2 deems it is important for the organisation to know the client base of the CSP. The expert suggested that it is a great benefit for the organisation to know the client base of the CSP currently has or has provided service to. This knowledge can assist the organisation to assess the caliber of the clients and this can indicate how the CSP regards security. The experts agreed that if a vast number of the client base has sensitive data, then the CSP is more likely to have defined digital forensic readiness techniques to cater for their clients.

TABLE 5: SUMMARY OF EXPERT'S ANSWERS

	Financial Industry Expert		
	Agree	Partially agree	Disagree
Feasible	X		
Relevant	X		
Does it provide accountability		X	
Decision should be quantified?			X
Can it add value?	X		

	Cloud Developer Industry Expert		
	Agree	Partially agree	Disagree
Feasible	X		
Relevant		X	
Does it provide accountability			X
Decision should be quantified?			X
Can it add value?		X	

VII. LIMITATIONS OF THE RESEARCH

The first major challenge with the research is that *C²DF* was not pragmatically tested within an industry environment. In order for the proof of concept to be applied, the scope of the research and costs would relatively be much higher. It would be beneficial for future research to carry out a pragmatic implementation of the framework to test its (in) adaptability and application in a real industry environment. Another limitation of the research is the likelihood of biasness from the experts because the authors were present as *C²DF* was being analysed. However, with the current constraints on the research, *C²DF* has significant value for organisations that want to migrate to the cloud should they consider applying it.

VIII. CONCLUSION

Our objective was to present *C²DF* and highlight its strengths and weaknesses. The framework is a cloud based solution that an organisation from any industry can use to make decisions regarding a CSP to host their data. It was developed as a risk analysis tool to support organisations through a systematic process for accountability and reliability. Hence the size of the organisation is not really that important, although modifications may be made to suit different scenarios. Cloud infrastructures may have privacy and security vulnerabilities on organisations' data hence digital forensic readiness within *C²DF* reduces some levels of cyber threat. The value proposition for *C²DF* is that it enforces CSPs to not only consider technical details but also business impact of their cloud services.

It is important that certain standards are implemented throughout the phases of the framework. Challenges of costs and social factors such as communication between the organisation and the CSP, the impact of these factors can be studied further. The research can also be extended further to devise mechanisms to control subjectivity and reduce its implications within the application of the framework. Therefore, more empirical work is required to quantify some of the iterative steps such as determining the margin of error and the probabilistic certainty with selection of the CSP. Given the scope and available resources of the research, *C²DF* can certainly be an effective tool for organisations seeking to host their resources on the cloud.

ACKNOWLEDGMENTS

The authors would like to thank the University of Pretoria for granting this wonderful opportunity to embark on this research. Another special thanks to the industry experts who sacrificed their time to evaluate the Framework. As a team we are grateful.

Mr Makutsoane wishes to thank his family (Mama, Ntate and Izza) for their loving care and support. Also give a token of gratitude to Aurecon for availing its resources to this research. It was truly a testing time working on this research, thanks to God we saw it through.

REFERENCES

[1] R. Buyya, S.C. Yeo, S. Venugoal, J. Brober, I. Brandic, "Cloud Computing and emergent I platforms: Vision, hype and reality for delivering computing as the 5th utility", Future Generation Computer Systems, vol. 25, pp. 599 – 616, 2009.

[2] C. Lim, A. Superman, "Risk analysis and comparative study of the different cloud computing providers in Indonesia", 2011.

[3] D. Gollmann, *Computer Security*, London UK: John Wiley and Sons, 2004.

[4] B. Carrier, *File System Analysis*, USA: Addison Wiley, 2005.

[5] K. Ruan, J. Cathy, T. Kechadi, "Cloud forensics: An overview", *Advances in Digital Forensics VII,* 2011A.

[6] P. Mell, T. Grance, "The NIST definition of cloud computing", [Online], Available at :http://www.slideshare.net/crossgov/nist-definition-of-cloud-computing-v15, 2012.

[7] D. Reilly, C. Wren, T. Berry Cloud Computing: Forensic Challenges for Law Enforcement", [Online], Available at: http://0-ieeexplore.ieee.org.innopac.up.ac.za/stamp/stamp.jsp?tp=&arnumber=5678033 2011.

[8] P. Kalagiakos, P. Karampels, "Cloud Computing Learning", *IEEE*, 2011.

[9] C. Pavitts, "The Philosophy of Science and Communication Theory", *Nova Science Publishers*, 2000.

[10] L. Silva, "Epistemological and theoretical challenges for studying power and politics in information systems", *Information Systems Journal*, 2007.
[11] F. Cohen, *Challenges to Digital Forensic Evidence*, Massachusetts USA: ASP Press, 2008.
[12] R. Vacca, *The Philosophy of Science and Communication Theory*, NY USA: Morgan Kaufmann, 2009.
[13] K. D. Mitnick, W.L. Simon, *The Art of Intrusion*, Canada: Wiley, 2005.
[14] L. Ma, H. Duan, Q. Train, Z. Li, "A honeypot based degree statistics method for scans", *IEEE*, 2006.
[15] E. Casey, *Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet*, USA: Academic Press, 2011.
[16] X. Tan, "The issue of cloud computing security in high speed railway", *International conference on electronic and mechanical engineering and IT*, 2011.
[17] S. Biggs, S., Vidalis "Cloud computing: The impact on digital forensic investigations: Internet Technology and Secured Transactions", ICITST, 2009.
[18] D. Birks, C., Wegner, "Functional encryption: Definitions and challenges: Theory of Cryptography", *IEEE*, 2012.
[19] D. Boneh, A. Wegner, B. Waters, "Functional encryption: Definitions and challenges", *Theory of Cryptography*}, p. 253 - 273, 2011.
[20] B. Hay, K. Nance, M. Bishop, "Storm Functional encryption: Definitions and challenges, Theory of Cryptography", *Proceedings of the 44th Hawaii International Conference on System Sciences*, 2011.
[21] D. Baske, A. Stander, J. Jordaan, "A Digital Forensic Readiness Framwork for South African SMEs", *IEEE*, 2010.
[22] M. Ambrust, A. Fox, R. Griffin, A., D. Joseph, R. Katz, "Above the clouds: A Berkeley view of cloud computing", *UC Berkeley reliable adaptive distributed systems*, 2009.
[23] T. Loughran, B. McDonald, H. Yun, "A Wolf in Sheep's Clothing: The Use of Ethics-Related Terms in 10-K Reports", *Journal of Business Ethics, 5th Annual Ethical Dimensions in Business: Reflections from the Business Academic Community,* p.39 - 49, 2009.
[24] W. Erhard, M. Jensen, S. Zaffron, "Integrity: A Positive Model that Incorporates the Normative Phenomena of Morality, Ethics and Legality", *Harvard Business School*, p.39 - 49, 2007.
[25] D. Vose, *Risk Analysis: A Quantitative Guide*, USA: John Wiley & Sons, 2008.
[26] X. Su, X. Zhao, "Analysis on effects of risk management level on internal control", *IEEE 18th International Conference on Industrial Engineering and Engineering Management*, p. 1202 - 1205, 2011.
[27] K. Ruan, I. Baggili, J. Cathy, T. Kechadi, "Survey on cloud forensics and critical criteria for cloud forensic capability: a preliminary analysis", *The Journal of Digital Forensics, Security and Law,* 2011B.
[28] C. Low, Y. Chen, M. Wu, T. Kechadi, "Understanding the determinants of cloud computing adoption", *Industrial Management and Data Systems*, vol.111, p.1006 - 10023, 2011.