Protection of personal information in the South African Cloud Computing environment: A framework for Cloud Computing adoption

Dayne Edward Skolmen
School of Information and Communication Technology
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
dayne.skolmen@gmail.com

Mariana Gerber
School of Information and Communication Technology
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Mariana.Gerber@nmmu.ac.za

***Abstract*— Cloud Computing has advanced to the point where it may be considered an attractive proposition for an increasing number of South African organizations, yet the adoption of Cloud Computing in South Africa remains relatively low. Many organizations are hesitant to adopt Cloud solutions due to a variety of inhibiting factors and concerns that lead to the mistrust in Cloud Computing. One of the major concerns identified is information security within the Cloud Computing environment. The approaching commencement of new information security legislation in South Africa, known as the Protection of Personal Information Act (POPI), may provide an ideal opportunity to address the information security-related concerns and foster a trust relationship between potential Cloud users and Cloud providers. POPI applies to anyone who processes personal information and regulates how they must handle, store and secure that information. Cloud providers who can demonstrate that they protect personal information may be more trustworthy and therefore more attractive to potential Cloud users. This paper discusses a proposed Framework for Cloud Computing Adoption which could assist South African Cloud providers in approaching compliance with the POPI Act, providing transparency and accountability to potential Cloud users, fostering a trust relationship and ultimately promoting the adoption of Cloud Computing in South Africa.**

Keywords-cloud computing; POPI; cloud adoption; trust; information security legislation; information security; privacy

I. INTRODUCTION

Many organizations in South Africa are starting to look for ways to integrate Cloud Computing into their operations, causing an increasing interest in this relatively new technology [1]. However, despite the growth in interest, various sources have noted that the adoption of Cloud Computing in South Africa remains low [2,3,4]. By default, Cloud Computing has a lack of trust as it shifts most of the Information Technology (IT) infrastructure and data storage to off-premises third-party providers (called Cloud providers). This is perhaps the biggest concern of potential customers (called Cloud users), since the loss of direct control over their data limits their ability to ensure confidentiality, integrity and availability (CIA) [5, p. 51].

It is important to realize that Cloud Computing is not simply the purchase of a specific product or service; it is rather a partnership between the Cloud user and the Cloud provider. "The Cloud provider should be considered a trusted partner as it becomes an extension of the organization's IT department. In order for this to happen, both Cloud user and Cloud provider must commit to communication and transparency" [6]. Trust plays a vital role in the adoption of Cloud Computing. Cloud users require assurance that Cloud providers are making every effort to ensure the security and privacy of their information in the Cloud. Knowing these vital details is sure to instill a sense of confidence in the Cloud user. It is also likely to improve the reputation of Cloud providers which may in turn promote the adoption of Cloud Computing.

As mentioned previously, the security of information in the Cloud has been identified as a prominent concern for organizations looking to adopt Cloud solutions. One way to address this concern is to introduce information security legislation to regulate how personal information is handled, stored and secured in the Cloud environment.

The South African government has recognized the need for all organizations to protect personal information, hence the creation of the Protection of Personal Information Act, commonly known as PPI or POPI. For the purpose of this paper, the acronym POPI will be utilized. The eventual commencement and implementation of the POPI Act may produce a refreshed view of Cloud Computing in South Africa. Potential Cloud users may feel assured that their personal information will be secure because Cloud providers are compliant with information security legislation. This could lead to the building of trust between potential Cloud users and Cloud providers and thereby promote the adoption of Cloud Computing in South Africa. "In terms of regulation, compliance, security and privacy, the Protection of Personal Information Act (POPI) plays a significant role in the decision to adopt Cloud solutions in South Africa" [7].

The identified problem is that the uncertainties relating to regulation, compliance, security and privacy of personal information, lead to mistrust in Cloud Computing and ultimately cause barriers to the adoption of Cloud solutions in South Africa. The focus of this paper is to discuss a framework

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

to promote Cloud Computing adoption through compliance with the POPI Act. By addressing the information security-related concerns that cause mistrust in Cloud Computing, it is believed that such a framework would be useful to South African Cloud providers and could assist in the promotion of Cloud Computing adoption in this country. A literature review was conducted to gather relevant background information and a Design Science approach was utilized to develop the Framework for Cloud Computing Adoption.

The paper is arranged as follows: Section II defines the environment of Cloud Computing and its unique characteristics, functionality, benefits and risks from a general perspective. Section III discusses the status of Cloud Computing adoption in South Africa. Section IV provides a comprehensive review of the POPI Act. Section V establishes the elements of trust in Cloud Computing. Section VI discusses the proposed Framework for Cloud Computing Adoption and its unique components. Section VII concludes the paper with a summary of the developed framework, an overview of what was accomplished, and suggestions for future research.

II. Cloud Computing

A. Overview of Cloud Computing

“Organizations are faced with a number of challenges and issues in decentralized, multiple-server, physical, non-virtualized IT environments” [8]. The cost of storage is increasing due to the dependency on infrastructure, maintenance and technical skills required. For small organizations that cannot afford large infrastructure and expensive software, a potential solution could come in the form of virtualization and outsourced services. There is a need for a new computing paradigm, as the advancements in IT require cost-effective computing services without installing them at local sites [9]. With the above-mentioned need for cost-effective outsourced computing services, Cloud Computing could be an ideal solution and technology to encourage organizations to move from having their own local servers to storing data and accessing computing services over the internet.

“Cloud Computing is a current trend that reveals the next generation application architecture” [10]. In the phrase Cloud Computing, the term Cloud (also phrased as "the Cloud") is used as a metaphor for "the Internet" and is believed to be derived from the cloud symbol that is often used to represent the Internet in flow charts and diagrams [11]. Typically, the Cloud is a large pool of usable resources such as hardware and software which are stored on remote servers and are easily accessible via the Internet [12,13]. Therefore, the phrase Cloud Computing can be understood as internet-based computing, where different computing services are delivered to, or accessed by, the Cloud user through the internet.

The act of delivering hosted services over the Internet can be broadly divided into three basic service models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-service (SaaS). IaaS provides the Cloud user with computational and storage infrastructure as a fully outsourced service. PaaS provides the Cloud user with a computing platform for application development and deployment. SaaS enables Cloud users to consume software on a pay-per-use pricing scheme, while the Cloud provider maintains the software and hardware [14]. These three service models have been explained in detail by [8] and [15]. Furthermore, Cloud Computing consists of four deployment models that define how Cloud users interact with the Cloud. These deployment models include Private Cloud, Public Cloud, Hybrid Cloud, and Community Cloud [14]. Each of these deployment models have been described in detail by [16] and [11].

With the establishment of the Cloud Computing environment, one can see that virtualization would appear to offer compelling benefits, which could theoretically drive organizations to move to the Cloud when these desirable aspects are in line with an organization’s business needs.

B. Benefits of Cloud Computing

The usage of Cloud Computing provides a wide range of benefits to an organization. Cloud Computing has been described as a routine part of digital life [17]. Cloud Computing is utilized in daily activities such as online services, sending and receiving emails, or uploading and storing photographs, documents and business records [17]. It has enabled the convenient mobility of sharing data among mobile devices anywhere in the world through the internet. Cloud Computing has also cut the cost of doing business by providing flexible and cost-effective resources. The flexibility of Cloud Computing has been described as a paradigm that supports on-demand network access in order to share computing resources such as network bandwidth, storage, applications, etc. [18]. Computing resources have the ability to be rapidly supplied or released according to an organization’s needs. This feature makes Cloud Computing highly cost-effective as it functions on a pay-per-use pricing model. Reference [19] attributes the huge growth of Cloud services to the ability of Cloud users to pay for only what they need and only when they need it.

Cloud Computing has been successful in supporting business growth by reducing costs related to IT. Reference [8] has identified a few of the potential savings from the outsourcing of IT resources to a third party service provider. These include “no maintenance for upgrades or new installation costs; less hardware to purchase and support; the elimination of the cost of power, cooling, floor space and storage; a reduction in operational costs; pay as you go pricing scheme which allows total flexibility; efficient use of IT resources.”

Though the many benefits associated with Cloud Computing may seem desirable, there is, however another side to consider. “The real cost of Cloud Computing is more than just pay-as-you-go. The real cost is hidden and is difficult to fathom - the cost of risk” [19].

C. Risks associated with Cloud Computing

Risk is the key factor that dictates the Cloud Computing industry. The Cloud Computing industry is fraught with risk, since Cloud providers and Cloud users both face uncertainties. Risks faced by the Cloud user include security, reliability and the overall lack of control. For the Cloud provider, risk takes the form of an unpredictable demand for service. If Cloud users were to assume the full burden of these risks they would never host critical applications in the Cloud. However if the Cloud providers assumed this burden, the potential liabilities would increase costs and discourage business.

Therefore, complete risk bearing by either of the parties is not sustainable for Cloud Computing. "With the unique functionality of Cloud Computing technology, Cloud providers and Cloud users need to learn to thrive on symbiotic relationship and devise dynamic and mutually beneficial agreements and contracts, where both parties can define parameters of the relationship based on risk sharing and mutual financial success by embracing unprecedented contractual obligations" [19].

It is evident that Cloud Computing offers many potential benefits. However, as with the adoption of any technology, there are risks to be considered. These risks should be shared by both the Cloud user and Cloud provider in order for the relationship to be beneficial to both parties. Having established the Cloud Computing environment along with its associated benefits and risks, it is necessary to consider the current status of Cloud Computing in South Africa by focusing on adoption rate, legislation, privacy and security.

III. Cloud Computing in South Africa

The term Cloud Computing is becoming more familiar to South African organizations. While Cloud Computing has been developing rapidly in first world countries, the lack of bandwidth has been one of the factors limiting the adoption of Cloud Computing in South Africa. However, Quentin Pienaar [20], the divisional director of business systems at MiX Telematics, has noted a shift over the past few years which has seen a rise in the attractiveness of Cloud Computing and many organizations are increasingly utilizing the Cloud. This growth has been attributed to a decrease in data costs and more readily available bandwidth from the arrival of several undersea cables from a submarine cable operator known as SEACOM [20].

The potential benefits of Cloud Computing become more relevant for businesses operating in developing countries, especially small and medium-sized enterprises (SMEs) which have to compete with larger organizations to gain sustainable advantage. The relevance of Cloud Computing in SMEs is therefore the potential for cost saving due to the outsourcing of expensive infrastructure and services, which will further improve efficiency [21].

Although the benefits of Cloud Computing may be very desirable, South African organizations seem hesitant to adopt Cloud Computing solutions due to a variety of inhibiting factors. A telephone survey was conducted to identify the concerns of potential Cloud users when considering adopting local Cloud solutions. A sample of 27 South African Cloud providers were interviewed. The results of the survey identified that the top concerns of potential Cloud users from the perspective of Cloud providers were availability, security, cost and lack of control [22]. Security was identified as the underlying top concern of potential Cloud users when considering local Cloud solutions.

Since the benefits of Cloud Computing can only exist if the confidentiality, integrity and availability of information in the Cloud are intact, the factor that this research will focus on will be legislation. The implementation of information security legislation could theoretically mitigate the information security-related concerns of potential Cloud users, thus allowing organizations to take advantage of the full benefits of Cloud Computing.

As mentioned above, the approaching commencement of new information security legislation in South Africa, known as the Protection of Personal Information Act (POPI), may provide an ideal opportunity to address the information security-related concerns and foster a trust relationship between potential Cloud users and Cloud providers.

IV. Protection of personal information

As technology expands, exposure of valuable and precious information to risk becomes inevitable. Access is far easier to acquire, yet technology does not always provide proper safeguards for the protection of this information. "If security laid in virtualization technology is vulnerable it could cause major security breaches from both an organization's and provider's perspective" [23]. Data breaches have been identified as one of the most common and costly security failures in organizations [24]. "With the proliferation of network technologies, data breaches of consumer personal information continue to become an ever-increasing part of the information age in which we live" [25]. In modern society, information is power. Both collecting and collating personal information are means of acquiring power, usually at the expense of the data subject [26, p. 1463]. A data subject is the person to whom personal information relates [27, p. 12]. Thus, there is a need to implement regulations and legislation that protect data subjects and their personal information.

POPI has the greatest impact on Cloud Computing adoption. This is due to the vast amount of personal information being stored in the Cloud and the need to protect this information in order to assure a safer Cloud environment for current and potential Cloud users. It is crucial that the safeguards required by POPI are addressed by implementing appropriate controls in order to secure the Cloud environment, since a breach of this information could have a considerable impact on data subjects.

A. Protection of Personal Information Act (POPI): Overview

POPI is based on the European data protection directive, as it aims to ensure that personal information in South Africa is processed in accord with internationally accepted data protection principles [28]. Personal information is comprised of "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person" [27, p. 14].

POPI applies to anyone who processes personal information and regulates how they must handle, store and secure that information. The processing of personal information has been defined as "any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including the collection, receipt, collation, storage, updating and use of the information" [27, p. 14]. In order to understand the current stage and development of POPI, the development stages of the act will now be explained.

The cabinet passed POPI as a Bill on 14 August 2009. A Bill is a proposed new law, or draft law, which has not yet been approved by Parliament [29]. When a Bill becomes an Act (law), it has been passed by Parliament or the Provincial Legislature in question, signed by either the President or the Premier of the province, and published in the Government Gazette. The developmental stages of an Act in Parliament of South Africa are listed as [30]:

- Tabled in Parliament
- Comments invited by Parliamentary Portfolio Committee on Justice
- Forwarded to National Council of Provinces for approval
- Forwarded to National Assembly for approval
- Sent to the President for signature
- Published in Government Gazette

The current stage of POPI within this process is that Parliament has passed the Act and the President has signed it into law as the Protection of Personal Information Act (No. 4 of 2013) on 26 November 2013. The President signed a proclamation, which was gazetted on 11 April 2014 where the effective date of certain sections of the Act was proclaimed as 11 April 2014. The next step is POPI's full commencement date in the Government Gazette and then the final countdown to its implementation and a compliance deadline.

Even though the commencement of POPI is approaching, many South African organizations are only beginning to encounter terms such as protection of personal information or data privacy. Thus, with the requirement for organizations that process personal information to implement POPI within their business, there is a need for organizations to understand the basic conditions of protecting personal information under the approaching law.

Once section 114 of POPI is enacted, which entails the transitional arrangements, all processing of personal information must conform to the requirements of the Act within one year. POPI requires the appointment of an Information Regulator who will be in charge of issuing the penalties for non-compliance. The duties of the Information Regulator are as follows [27, pp. 48-52]:

- to provide education;
- to monitor and enforce compliance;
- to consult with interested parties;
- to handle complaints;
- to conduct research and to report to parliament;
- to deal with codes of conduct; and
- to facilitate cross-border cooperation in the enforcement of privacy laws by participating in any initiative that is aimed at such cooperation.

Requirements enforced under the Act are widespread and non-compliance may result in severe penalties and consequences, including fines of up to 10 million Rand or 10 years imprisonment and may expose organizations to civil damage claims by data subjects [27, p. 100]. These penalties could cause severe reputational damage for organizations as well as for the data subjects whose information was compromised. This could result in various losses for organizations such as the loss of customers, failure to attract new customers, loss in market share or competitive advantage, loss in productivity and ultimately, a loss in revenue. However, POPI also has its advantages as it represents good business practices, which could theoretically increase business value and trust through compliance.

B. Opportunities and Benefits of POPI

The commencement of POPI will place significant demands on the resources of organizations, both in terms of time and cost. However, there are added opportunities and benefits that organizations can maximize whilst implementing POPI requirements into their operations. For this to be achieved POPI compliance needs to be approached in a holistic manner that is beneficial to the organization and not in isolation just because organizations are required to comply by law [31]. "POPI compliance is not just about obeying the law; it is essential to doing business in a data-driven world – and has tangible benefits for profitability and competitiveness – giving a company that gets compliant early a competitive advantage" [32]. The potential opportunities and benefits resulting from POPI compliance are:

1) **Data quality improvement (integrity)**

In achieving compliance, the business processes that will need either to be implemented or amended will ensure a better quality of organizational data. Organizations looking to gain competitive advantage out of "Big Data", will as a result be better placed to collect and harness such data in an ethical and legal manner.

2) **Improving business management**

Fulfilling the requirements for the processing and securing of personal information will provide organizations with an opportunity to review current business processes and consider ways to improve efficiency.

3) **Competitive edge**

Having POPI-compliant data management processes in place will be a market differentiator for organizations that have taken the initiative to comply before the commencement of the Act. This gives organizations the opportunity to improve their image. Customers are more likely to do business with compliant organizations, as this will assure them that their personal information will be safe.

4) **Savings on data breach costs**

By mitigating the risk posed by data breaches or data leakages, organizations can save millions of Rands. In late 2013 the personal information (including credit and debit card information) of more than 110 million Target consumers was exposed due to Target's failure to maintain proper internal controls relating to data security. This resulted in a severe drop in profit, decrease in stock price and millions of Dollars of potential liability claims in more than 140 class-action lawsuits filed on behalf of banking institutions, consumers and shareholders [33, p. 2].

5) **New overseas business opportunities**

POPI compliance presents the opportunity of doing business with European Union organizations. Europe has strict standards when it comes to data protection. Organizations may not deal with countries that do not have similar data protection laws in place. Compliance with international standards could lead to greater investment opportunities.

6) **Building customer relationships and customer trust**

Cloud users will take comfort in knowing their information and interactions with organizations are secure and protected. By achieving and maintaining POPI compliance, organizations will be in a position to confidently reassure their customers. Transparency will assure that customers know exactly what data and personal information organizations have, where it is located, its accuracy, and who within the organization has access to view, create and update it. These are essential steps in building trust with customers.

Having established the opportunities and benefits resulting from POPI compliance, building a trust relationship stands out as a highly desirable benefit for Cloud providers. The requirements in the POPI Act for safeguarding personal information, accountability from the responsible party and full transparency may be useful in fostering trust in Cloud Computing. In order to better understand how trust in Cloud Computing can be achieved, the following section will analyze the elements of trust.

V. Elements of Trust

Since trust is a critical aspect of Cloud Computing [34], it is important to identify what creates trust between a potential user and a service provider. Reference [35] states that "trust revolves around 'assurance' and confidence that people, data, entities, information or processes will function and behave in expected ways."

As previously mentioned, Cloud Computing has an inherent lack of trust as it shifts most of the IT infrastructure and data storage to off-premises third-party providers. According to Dean Chivers, Director of Deloitte Legal, "the POPI Act will be the catalyst for companies to add value while achieving compliance. Companies should engage with their customers in the process and use it as an opportunity to build customer trust in the company by highlighting the company's efforts to treat customer's personal information with respect and confidentiality" [36]. The presence of trust ensures the successful adoption and continued use of the Cloud, whereas the absence of trust results in ineffective performance and inefficient use of the services offered by the Cloud [37, p. 6]. Trust in Cloud Computing has been identified to be based on compliance, transparency and accountability [38]. These three fundamental elements of trust form the underlying foundation of the Framework for Cloud Computing Adoption. Ultimately, trust is the core factor in promoting the adoption of Cloud Computing.

"There is a vital need for assurance of compliance for any well-governed organization in order to confidently embrace and fully benefit from an IT solution (such as Cloud Computing). There should be confidence and trust that this can be done in a manner that is compliant with internal and external requirements and demonstrates due care" [39, p. 168]. In order for potential Cloud users to confidently embrace and fully benefit from Cloud Computing, there are certain components that the Cloud provider needs to possess.

The next section will discuss the Framework for Cloud Computing Adoption. Each of the framework's components will then be introduced and related back to the elements of trust.

VI. Framework for Cloud Computing Adoption

Throughout this paper, there has been an underlying emphasis on Cloud Computing adoption in South Africa being relatively low. Although this has been established as a clear problem, there is no clear solution. Cloud providers do not know what they need to do in order to promote the adoption of their services. A unique opportunity is presented to Cloud providers with the approaching commencement of the POPI Act and the requirement for every organization in South Africa that processes personal information to comply with the Act. The need for the Framework for Cloud Computing Adoption emerged from these factors.

In order to promote adoption of a relatively new technology, various components must be studied in order to establish which ones promote adoption. These components have been identified and combined into a framework. Fig. 1 depicts the Framework for Cloud Computing Adoption which is proposed to be utilized by Cloud providers to assist in promoting the adoption of Cloud solutions in South Africa.

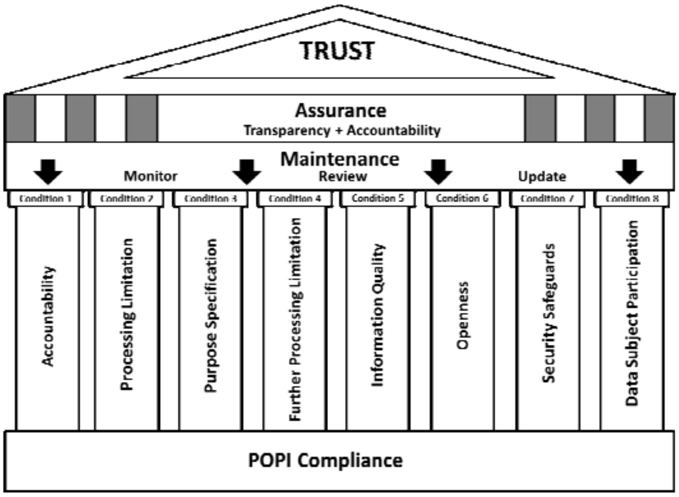

Figure 1. Framework for Cloud Computing Adoption

A discussion of the functionality and integration of each component in the framework will now follow.

The initial starting point of the framework was identifying who its potential users would be. Once it was determined that the framework would be utilized by South African Cloud providers, there was a need to identify why potential Cloud users in South Africa are hesitant to adopt Cloud solutions. The concerns of potential Cloud users that lead to mistrust in Cloud Computing were identified in Section III. The framework focused on addressing the information security-related concerns of potential Cloud users. This was utilized as the input to the framework.

The first component of the framework is a high-level approach to **compliance** with the POPI Act.

A. POPI Compliance

Cloud providers need to take a proactive approach to the protection of personal information. Cloud providers must align their business processes and practices with the eight conditions of the POPI Act. The eight conditions for the lawful processing of personal information form the eight support pillars of the framework depicted in Fig. 1. These conditions are defined below [27]:

- **Accountability** - The organization must ensure that the conditions contained in the Act are complied with.
- **Processing Limitation** - Personal information may only be processed in a fair and lawful manner**.**
- **Purpose Specification** - Personal information may only be processed for specific, explicitly defined and legitimate reasons.
- **Further Processing Limitation** - Personal information may not be processed for a secondary incompatible purpose**.**
- **Information Quality** – The organization must ensure that personal information is kept reliable, accurate and up-to-date.
- **Openness** - Data subjects must be aware that personal information is being collected by the organization.
- **Security Safeguards** - Personal information must be protected through the use of reasonable technical and organizational safeguards.
- **Data Subject Participation** - Data subjects may request the correction/deletion of any personal information held about them that may be inaccurate or misleading.

The approach to POPI compliance will differ from organization to organization and the assessment period and number of changes required will be unique to each type of business. It is important to understand that, just as one cannot achieve 100% security, the same goes for 100% compliance with POPI. However, the responsible parties must be able to show that they have done what is reasonably practicable, thus demonstrating due care [27].

The POPI compliance component of the framework assists the Cloud provider with four high-level steps to approach compliance with POPI, namely; **Identification**, **Awareness**, **Assessment** and **Guidelines**. Each of these steps will be discussed in detail.

Step 1: Identification

The initial starting point is for the Cloud provider to determine if POPI is applicable to them. If it is identified that the Cloud provider processes personal information, then they are given the title of **responsible party** and are required to comply with POPI. In terms of POPI the responsible party is “a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information” [27, p. 16]. The purpose of processing personal information refers to WHY it is being processed and the means for processing personal information refers to HOW it is being processed.

Once the Cloud provider has identified that they are the responsible party, they need to identify (if already in existence) or assign an Information Officer or equivalent individual and register them with the Information Regulator. Once the Information Officer has been assigned, they must take up their duties and responsibilities in terms of the Act. The responsibilities of the Information Officer include [27, pp. 64-66]:

- “The encouragement of compliance, by the body, with the conditions for the lawful processing of personal information;
- dealing with requests made to the body pursuant to this Act;
- working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body;
- otherwise ensuring compliance by the body with the provisions of this Act; and
- as may be prescribed.”

The Information Officer or equivalent individual in charge of overseeing compliance will need to assess the impact of POPI on the organization, conducting a POPI risk assessment and identify, collect and create a register of all documents that will be affected by POPI. The Information Officer must then identify all personal information being processed and if any special personal information is being processed. In terms of section 26 of the POPI Act the processing of special personal information is prohibited unless certain requirements prescribed in the Act are met. Given the highly sensitive nature of special personal information, a higher degree of protection is required. Special personal information includes information concerning [27]:

- the religious or philosophical beliefs of a data subject,
- a data subject's race or ethnic origin,
- trade union membership of a data subject,
- data subject's political persuasion,
- health and sex life of a data subject,
- biometric information of a data subject, or
- criminal behaviour of a data subject.

The authorization section in sections 27-35 of the POPI Act relates to specific authorization requirements for the processing of each type of special personal information. The Information Officer needs to determine what the purpose is for processing personal information and special personal information and the manner in which they are processed.

Step 2: Awareness

The Information Officer must raise awareness of POPI by conducting an awareness workshop with departmental managers and key stakeholders and displaying effective posters around the organization. The Information Officer should launch an education programme within the organization. This programme could offer new and existing employees online training which is cost-effective. However, depending on a person's individual roles and responsibilities within the organization, a more advanced education program may be required as greater risk is implied. This advanced programme should include all key aspects of business risks and implications on information retention and exchange, as well as the processes that generate and consume personal information.

Step 3: Assessment

The third step of the POPI compliance approach includes a high-level POPI assessment which consists of compliance indicators for each condition. Since POPI is a high-level document, it only states that responsible parties must protect personal information, and does not provide details on how responsible parties must do this. For this reason, the Cloud provider's current information management policies, practices and processes will be assessed in line with ISO27001 and in terms of the eight information protection conditions contained in the POPI Act. The objective of the assessment is to provide the Cloud provider with a high-level overview of its readiness to comply with the requirements of POPI. Furthermore, this assessment will assist the Cloud provider in forming a baseline for compliance.

In the construction of the POPI assessment, compliance indicators were derived from an alignment of the requirements of POPI and information security controls in ISO/IEC 27002 [40]. Each compliance indicator has relevant questions linked to it. These questions are provided to assist the Cloud provider in their evaluation of the compliance indicator. For the purpose of this paper a sample of the high-level assessment for condition 7 of POPI has been provided in Fig. 2.

POPI Assessment

Condition 7: Security Safeguards

Compliance Indicators:

1) Periodic Information Security Risk Assessments performed across People, Process, and Technology

Has your organization undertaken a risk assessment in respect to the protection of personal information? If yes, where gaps or deficiencies (risks) are noted in the processing of personal information, are policies and procedures updated to ensure the gaps or deficiencies are remediated?

2) Alignment to security best practice standards

Has your organization identified/adopted any generally accepted information security practices and procedures that generally apply to your organization or are required in terms of the specific industry or professional rules and regulations?

3) Update third party contracts and review third party security practices

Does your organization have appropriate contractual safeguards in place with your third party processors (e.g. SLAs, confidentiality agreements)? If yes, do your third party contracts include clauses for the processing and securing of personal information, notification in the event of a breach of personal information and provisions dictating what happens to the personal information once the contract ends or is terminated?

4) Security Incident Management and Breach Notification Procedures

In the event of an information breach (i.e. lost laptop or flash) is the incident reported and communicated to the data subject? Does your organization's incident management plan specifically address incidents related to information loss?

5) Protection of personal information during cross-border transfers

Does your organization share personal information with entities in other countries? If yes, do you obtain assurance that the recipient of the personal information is legally bound (through laws, regulations, codes, agreements etc.) to ensure a substantially similar level of protection in respect of personal information?

Figure 2. High-level assessment for Condition 7 of POPI

At the end of the assessment a rating for each condition can be determined by the number of compliance indicators in place. Furthermore, possible penalties in the case of non-compliance under the act are provided to show the importance of protecting personal information. "Information is an organizational asset, which is why it is essential to control the way in which it is used and stored. Ultimately, POPI will prove an invaluable tool to ensure the integrity, security and privacy of an organization's information" [32].

Step 4: Guidelines

In the case of non-compliance, high-level guidelines are provided to address the critical gaps identified during the high-level assessment of the eight conditions of POPI. These guidelines consist of the condition name, the applicable section of the POPI Act, a description of the condition for a clear understanding, and high-level guidelines to approach compliance with each condition. The guidelines will also help the Cloud provider understand the importance of data privacy and information security. For the purpose of this paper a sample of high-level guidelines to address condition 7 of POPI have been provided in Fig. 3.

POPI Guidelines

Condition 7: Security Safeguards

POPI Act Reference: Sections 19, 20, 21, 22 and 72

Description: Reasonable measures must be taken to identify all foreseeable internal and external risks, establish and maintain appropriate safeguards against these risks, regularly verify that the safeguards are effectively implemented and ensure they are continually updated. The responsible party must notify the Information Regulator and the data subject when the personal information of a data subject has been accessed or acquired by any unauthorized person.

The compliance indicators for Condition 7 outlined in the POPI assessment in Step 3 should be addressed as follows:

1) The organization must conduct regular risk assessments to identify and manage all reasonably foreseeable internal and external risks to personal information under its control. The organization must ensure that the security safeguards are continually updated to cater for new risks or threats faced by the organization.

2) The organization must consider the various information security standards, practices, procedures and codes that are generally or specifically applicable to it.

3) Third parties may not process personal information without the knowledge and authorization of the organization. The organization must have a written contract with the third party which requires the third party to maintain the confidentiality and integrity of personal information processed on behalf of the organization.

4) The Information Regulator as well as the affected individuals must be notified of all security breaches. The organizations incident management plan must include incidents related to information loss.

5) For third parties located outside of South Africa the organization must ensure that the third party complies with any foreign laws relating to personal information applicable to the third party or enter into a contract requiring information to be protected.

Figure 3. High-level guidelines to address Condition 7 of POPI

The Cloud provider needs to utilize the abovementioned guidelines and implement adequate controls from an internationally accepted information security standard such as ISO/IEC 27002. This procedure does not end once all conditions have been addressed and compliance with POPI is achieved, as the Cloud provider must **maintain compliance**. This forms the second component of the framework.

B. *Maintenance*

The Cloud provider will need to introduce a process to continuously **monitor**, **review** and **update** the controls implemented to ensure continued compliance with the POPI Act and alignment to good practices. There will need to be periodic reviews in the form of audits to assess the status of compliance with POPI. From the findings of these audits, updates should be made to ensure that compliance is maintained. This process is based on the performance evaluation and improvement sections of ISO/IEC 27001 [41, pp. 7-9]. The process will be continuous, as seen in Fig. 4.

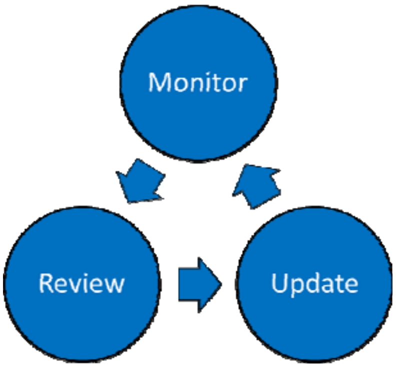

Figure 4. Process for maintaining compliance

Once POPI compliance has been achieved and maintained, the Cloud provider will be in a position to provide potential Cloud users with **assurance**, this forms the third component of the framework as depicted in Fig. 1.

C. *Assurance*

Assurance encompasses **transparency** and **accountability** and will be utilized to build a trust relationship between the potential Cloud user and Cloud provider. “Transparency and accountability are a recognized basis for gaining trust in Cloud providers” [34, p. 3]. Reference [4] identified that “organizations are hesitant to adopt Cloud because of poor vendor transparency, as well as an inability to assess risks and audit Cloud provider security measures.”

In the context of this paper, transparency means a level of openness about an organization’s handling and securing of personal information. POPI requires complete transparency; responsible parties need to be open with their users and adequately inform them about how they are handling, backing up, securing and protecting their personal information. Audit reports should be shared with potential Cloud users to provide assurance of data protection implementations. Cloud providers must demonstrate the existence of effective security controls that will assure organizations that their information is properly secured against unauthorized access, change and all forms of destruction in the Cloud [42, p. 8].

Accountability for the protection of personal information will fall on the responsible party. Fig. 5 illustrates two scenarios relating to how POPI determines accountability in the Cloud environment. Both scenarios are discussed below.

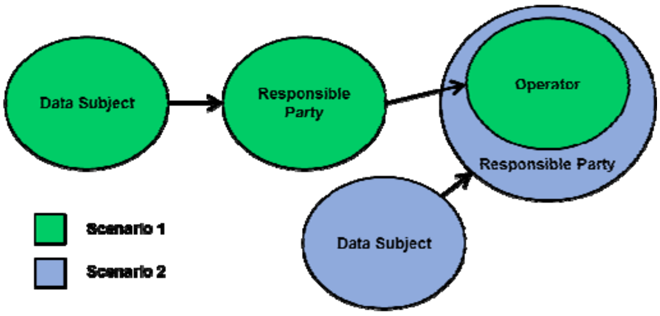

Figure 5. POPI accountability in the Cloud Computing environment

The circumstances of Scenario 1 are unique to Cloud Computing. The *responsible party* in this case will be the Cloud user, as they will store the personal information of their clients (*data subjects*) within the Cloud. Thus, giving the Cloud provider the title of *operator*. An operator is defined as "a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party" [27, p. 12]. This creates a few concerns in terms of accountability and preserving the confidentiality and integrity of information in the Cloud. The personal information stored in the Cloud may lack integrity if it is not kept up to date, as the responsible party will have to keep track of this from the data subject. If there is a breach in the Cloud then POPI states that the responsible party will be held fully accountable. According to POPI, the operator is only responsible for complying with Condition 7 of the Act (Security Safeguards). Therefore, the partnership between the responsible party and the operator needs to be strictly governed by a highly detailed Service Level Agreement (SLA) to ensure that the operator also inherits some form of liability in the case of a data breach.

In Scenario 2 the data subject stores their personal information in the Cloud. In this scenario the Cloud provider is the responsible party and is therefore accountable for any breaches of personal information in the Cloud.

Both scenarios put the accountability on one entity, the responsible party. However, as mentioned previously, in order for both the Cloud user and Cloud provider to fully benefit from this partnership, there needs to be accountability on both sides. It is important to understand that Cloud providers may have many users and those users may be responsible parties or data subjects. Thus, in either case the Cloud provider will have to inherit responsibilities to comply with all eight conditions of POPI.

The relationship developed through the process of providing transparency and accountability is likely to build **trust** between the Cloud user and Cloud provider, which is the final component of the framework.

D. Trust

Throughout the process of achieving compliance and providing assurance, a trust relationship should form between the potential Cloud user and Cloud provider. Since trust plays a central role in helping consumers overcome perceptions of risk and insecurity [43, p. 334], the development of a trust relationship may assist in addressing the information security-related concerns of potential Cloud users that lead to mistrust in Cloud Computing.

Finally, the envisaged output of the framework is the promotion of the adoption of local Cloud solutions; this should follow the critical establishment of trust between the potential Cloud user and the Cloud provider.

VII. Conclusion

Due to Cloud Computing being a relatively new technology, there are many barriers to the adoption of Cloud solutions in South Africa. However, ensuring security of personal information through compliance with information security legislation is one aspect that provides an opportunity to mitigate the information security-related concerns, build trust relationships with potential Cloud users and ultimately promote the adoption of Cloud Computing in South Africa. Hence, Cloud providers need to be aware of the unique opportunity that is likely to increase business value and the overall reputation of their organization. The establishment of assurance and trust are vital aspects in the promotion of Cloud adoption and may be acquired through compliance with the POPI Act. The framework addressed compliance through analyzing the Act and providing an IT perspective to simplify the process of approaching POPI compliance. The Framework for Cloud Computing Adoption represents a part of the solution to assist Cloud providers in advancing from low Cloud adoption to the promotion of Cloud adoption.

This paper defined the unique environment of Cloud Computing, established the status of Cloud adoption in South Africa and the top concerns of potential Cloud users that influence the adoption rate, provided a comprehensive review of the POPI Act and discussed the proposed Framework for Cloud Computing Adoption. The framework offers Cloud providers guidance in the form of a high-level approach to POPI compliance, which gives them the opportunity to mitigate the information security-related concerns, build trust relationships with potential Cloud users and ultimately promote the adoption of Cloud Computing in South Africa.

Future research could focus on creating a compliance tool based on the Framework for Cloud Computing Adoption. Other future research could focus on mitigating the non-information security-related concerns inhibiting Cloud adoption in South Africa. Dr Mariana Carroll has summed up what the adoption of Cloud Computing can do for any organization, "Today's business environment is all about opportunity; and the only way to enjoy opportunities is to embrace change. By embracing the Cloud, organizations are enabled to transform the way they deal with employee and customer interaction, collaboration and innovation" [44].

Acknowledgment

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the National Research Foundation.

References

[1] Deloitte, "Cloud Computing in a South African business context," n.d. [Online]. Available: http://www.deloitte.com/view/en_za/za/0603e80244fc8210VgnVCM100000ba42f00aRCRD.html

[2] M. Mujinga, "Developing Economies and Cloud Security : A Study of Africa," Journal of Emerging Trends in Computing and Information Sciences, vol. 3, no. 8, pp. 1166–1172, 2012.

[3] K. Van Der Schyff, and K. Krauss, "Cloud Adoption in South African: A Higher Education Perspective on Information Security Concerns," in SIG GlobDev First Pre- ECIS Workshop, Barcelona, Spain, 2012, June 10.

[4] A. Moyo, (2013). "SA cloud adoption behind BRICSS," 2013. [Online]. Available:

http://www.itweb.co.za/index.php?option=com_content&view=article&id=65786

[5] C. Rong, S.T. Nguyen and M.G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," Computers & Electrical Engineering, vol. 39, no. 1, pp. 47-54, 2013.

[6] S. Payne, "Building trust between cloud providers and consumers," 2013. [Online]. Available: http://www.networkworld.com/article/2164050/tech-primers/building-trust-between-cloud-providers-and-consumers.html

[7] M. Carroll, "Cloud computing and PPI: Finding your bearing," 2014. [Online]. Available: http://deloitteblog.co.za/2014/01/16/cloud-computing-and-ppi-finding-your-bearing/

[8] M. Carroll, P. Kotzé, and A. van der Merwe, "Going virtual: popular trend or real prospect for enterprise information systems," in ICEIS 12th International Conference on Enterprise Information Systems, pp. 214–222, 2010.

[9] M. Sajid, and Z. Raza, "Cloud computing: issues and challenges," in International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5474674

[10] A. Lin, and N. Chen, "Cloud computing as an innovation: Percepetion, attitude, and adoption," International Journal of Information Management, vol. 32, no. 2012, pp. 533–540, 2012.

[11] D. Zissis, and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2010.

[12] L.M. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, "A break in the clouds: Towards a cloud definition," Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2009.

[13] M.A. Vouk, "Cloud computing: Issues, research and implementations," Journal of Computing and Information Technology, vol. 16, no. 4, pp. 235–246, 2008.

[14] P. Mell, and T. Grance, "The NIST definition of cloud computing," NIST SpecialPublication, pp. 145–800, 2011.

[15] S. Carlin, and K. Curran, "Cloud Computing Technologies," International Journal of Cloud Computing and Services Science, IJ-CLOSER, vol. 1, no. 2, pp. 59-65, 2012.

[16] S. Ramgovind, M.M. Eloff, and E. Smith, "The management of security in Cloud computing," in Information Security for South Africa, IEEE, pp. 1-8, 2010.

[17] D. Hakim, "Europe Aims to Regulate the Cloud," The New York Times, 2013. [Online]. Available: http://www.nytimes.com/2013/10/07/business/international/europe-aims-to-regulate-the-cloud.html?pagewanted=all&_r=0

[18] P. Mell, and T. Grance, "The NIST definition of cloud computing," NIST SpecialPublication, 2009. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[19] S. Kulkarni, "Cloud computing - As much a business as a technology," 2014. [Online]. Available: http://www.lntinfotechblogs.com/Lists/Posts/Post.aspx?ID=56

[20] Q. Pienaar, "Deloitte Technology Trends 2013 Report – Elements of postdigital," 2013. [Online] Available: http://www.deloitte.com/assets/Dcom-SouthAfrica/Local%20Assets/Documents/tech_trends_2013.pdf

[21] M.J. Mohlameane, and N.L. Ruxwana, "The Potential of Cloud Computing as an Alternative Technology for SMEs in South Africa," Journal of Economics, Business and Management, vol. 1, no. 4, pp. 396–400, 2013.

[22] D.E. Skolmen and M. Gerber, "Potential Cloud users' concerns when considering a local Cloud Computing solution," unpublished.

[23] H. Mouratidis, S. Islam, C. Kalloniatis and S. Gritzalis, "A framework to support selection of cloud providers based on security and privacy requirements," The Journal of Systems and Software, vol. 86, no. 2013, pp. 2276-2293, 2013.

[24] IBM, "Data breach: An information resource for data breach prevention and response," 2012. [Online]. Available: http://www-935.ibm.com/services/uk/en/it-services/data-breach/

[25] M. Anandarajan, R. D'Ovidio and A. Jenkins, "Safeguarding Consumers Against Identity-related Fraud: Examining Data Breach Notification Legislation Through the Lens of Routine Activity Theory," International Data Privacy Law, vol. 3, no. 1, pp. 51-60, 2013.

[26] A.M. Froomkin, "The Death of Privacy?," Stanford Law Review, vol. 52, no. 1461, pp. 1461-1543, 2000.

[27] POPI, "Government Gazette: Protection of Personal Information Act," 2013. [Online]. Available: www.gov.za/documents/download.php?f=204368

[28] C. Matthes, "Unpacking the POPI Act: The ins and outs of protecting personal information," 2014. [Online]. Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=71001

[29] L. Bassett, "Article: Process of drafting legislation," Justice Today, Issue 1, p08, 2012. [Online]. Available: http://www.justice.gov.za/docs/articles/2012-drafting-legisltation.html

[30] Education & Training Unit, "The Policy and law making process," 2011. [Online]. Available: http://www.etu.org.za/toolbox/docs/govern/policy.html

[31] KPMG, "Practical steps to becoming POPI compliant," 2014. [Online]. Available: http://www.kpmg.com/za/en/issuesandinsights/articlespublications/protection-of-personal-information-bill/pages/default.aspx

[32] D. Kafouris and D. Chivers, "Getting with the POPI programme," 2013. [Online]. Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=69449

[33] N.E. Weiss and R.S. Miller, "The Target and Other Financial Data Breaches: Frequently Asked Questions," Congressional Research Service, 2015. [Online]. Available: https://fas.org/sgp/crs/misc/R43496.pdf

[34] J. Huang and D.M. Nicol, "Trust mechanisms for cloud computing," Journal of Cloud Computing, vol. 2, no. 1, pp. 1-14, 2013.

[35] P. Cofta, "Trust, Complexity and Control. Confidence in a Convergent World," Ontiario: John Wiley, 2007.

[36] Deloitte, "Is POPI a necessary evil or opportunity for value add?," n.d. [Online]. Available: https://www.deloitte.com/view/en_id/id/cedcf5313c129210VgnVCM200000bb42f00aRCRD.htm

[37] V. Bourne, "Rising to the Challenge," 2010 Global IT Leadership Report, 2010. [Online]. Available: http://networkworld.com

[38] N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux, S. Creese and P. Hopkins, "The Cloud: Understanding the Security, Privacy and Trust Challenges," Information Society and Media TR-933-EC, 2010.

[39] M. Willett and R. Von Solms, "A Framework for Assuring the Conformance of Cloud-based Email," in The 8th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 168–173, 2013.

[40] ISO/IEC 27002, Code of practice for information security controls, 2nd ed. International Organization for Standardization (ISO), 2013.

[41] ISO/IEC 27001, Information security management systems - Requirements, 2nd ed. International Organization for Standardization (ISO), 2013.

[42] M. Vael. (2010, 24 July 2010). Cloud Computing: An insight in the Governance & Security aspects. [Online]. Available: http://www.isaca.org/Groups/Professional-English/information-secuirty-management/GroupDocuments/Across%20Cloud%20Computing%20governance%20and%20risks%20May%202010.pdf

[43] D.H. McKnight, V. Choudhury and M. Kacmar, "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology," Information Systems Research, pp. 334-359, 2002.

[44] N. Lundin, "South African enterprises ready for cloud adoption in 2014," 2014. [Online]. Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=135455