Addressing emerging risks in transborder cloud computing and the protection of personal information: The role of internal auditors

T Banda Jangara
Department of Auditing
University of Pretoria

H Bezuidenhout
Department of Auditing
University of Pretoria

ABSTRACT

There is general consensus amongst researchers that most South African companies are not yet ready to comply with the Protection of Personal Information Act No. 4 of 2013 (the POPI Act) as they lack the necessary skills, knowledge and understanding to effect such compliance. Whilst the flow of personal information to trans border clouds is lawful according to section 72 of the POPI Act, and cloud services offer benefits such as cost savings and agility, it has been determined that companies are yet to take cognisance of the fact that there are risks associated with such transfers. Five preeminent emerging risks associated with cloud data storage include data location, security, privacy, legal compliance and the cloud service providers themselves. Because of their role as assurance providers, with knowledge about organisational strategy, processes and operations, internal auditors are found to be uniquely positioned within companies to assist effectively with risk management as required by The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and the corporate governance standards presented in King III. Internal auditors have been shown to be able to assist in mitigating each of the five emerging risks through their effective auditing of contracts, policies, procedures and controls, which ultimately results in effective advice and assurance for boards, management and stakeholders.

Key words

Cloud computing; internal auditing; personal information; risk management; transborder

1 INTRODUCTION AND BACKGROUND

Today, it is common knowledge that there are certain risks associated with the transfer of personal information by organisations to transborder clouds (European Commission 2012:5; Fischer 2012:5). Moreover, the mismanagement of personal information can have very serious consequences for organisations that collect personal data as part of their business processes. In 2008, the South African subsidiary of Zurich Insurance experienced a data leak during a routine transfer of data to a data storage centre, resulting in the loss of the personal information of 46 000 clients. The company was subsequently fined £2.3 million by the United Kingdom Financial Services Authority (FSA). The FSA stated that Zurich Insurance had failed to oversee the service provider that had been entrusted with the management of the information, and that it should have had full control of the process, despite the outsourcing arrangement (BBC News 2010). In another incident, Sony reportedly lost $171 million after a cyber-attack that resulted in 77 million accounts (complete with customers' personal information, including names, logins, passwords, emails addresses and credit card numbers), being compromised in 2011. British regulators subsequently fined Sony £250 000 for failing to prevent the cyber-attack (AON South Africa 2012; CBS News 2013). These are just two examples of many cited in the media, where personal information that is under the control of companies has been compromised. South African companies must take cognisance of the fact that without adequate protection, personal information may be lost, leaked and exposed to misuse, with negative and potentially damaging consequences.

In South Africa, the latest King Report on Corporate Governance (King III) issued by the Institute of Directors in Southern Africa (IOD 2009) gives guidance on what constitutes good corporate governance for all legal entities (Walker & Meiring 2010; Marks 2010). Chapter 4 of King III (IOD 2009:73) states that the governance of risk is the responsibility of the board of directors and is of paramount importance in conducting business. Because information is viewed as a business asset, the protection of personal information is one of the King III recommendations (IOD 2009; IT Governance

Network 2010). Boards of directors in companies want the assurance that all data or information management risks have been identified and mitigated, where necessary. Internal auditors can assist with fulfilling this requirement through risk identification and assessments, identification of the correct risk responses, continuous monitoring and the provision of assurance (in the form of formal reports on their analyses of situations) (IOD 2009:73, 93; Telavance 2012).

Information technology (IT) governance is the focus of Chapter 5 of King III (IOD 2009:82). Companies need to ensure that their IT infrastructures and business procedures enhance their abilities to achieve their business goals. In this regard, cloud computing is a technology that holds great benefits, especially for information management, but in order to be effective its inherent risks must be identified and managed (IT Governance Network 2010; AbuOliem 2013:521-522). IT should be treated as an integral part of organisation-wide risk management processes, with the integrity and security of information and privacy needing to be managed effectively (IOD 2009:85-86; IT Governance Network 2010). Compromising security and privacy are two of the five emerging risks inherent in the transfer of personal information to transborder clouds.

When it becomes operational in 2016, the Protection of Personal Information Act No. 4 of 2013 (the POPI Act) will have an impact on virtually every area of business, as it introduces a new and stringent personal information management standard with which companies will have to comply (IT Governance Network 2010). This will then put South Africa on par with other countries that have enacted and implemented data protection legislation (Liston 2012: 15; Wehler 2013). Moreover, failure to comply with the POPI Act, as well as any kind of data loss, can result in mandatory fines, similar in magnitude to those described above; this is in addition to the reputational damage organisations might suffer from the negative publicity relating to the loss of customers' personal information (the POPI Act at section 107; PwC 2012:2-4; Lamprecht 2013; Wehler 2013). Section 19 of the POPI Act makes it clear that organisations are responsible for securing the personal information that is entrusted to them by data subjects. The section states that this must be done by taking measures to identify and address risks relating to the management of personal information.

An area of business on which the POPI Act will have an impact, and of which internal auditors need to aware, is the transborder flow of personal information to the cloud (Kafouris 2014). IT is an industry characterised by rapid advances in both software and hardware innovation, and where trends emerge, experience wide-spread adoption and change rapidly. In a recent KPMG survey, 59% of the participants agreed that cloud computing is not going to be a short-lived fad; in fact, it represents the present and future of IT (Chung & Hermans 2010:16). In 2010 it was estimated that by 2014, cloud computing would be an industry worth $148 billion (Gartner 2010). Many organisations in South Africa have already migrated their IT operations to the cloud, and many more are currently in the process of doing so. The use of cloud solutions, many of which are located outside the country, is also increasing in South Africa (Bortz 2011a).

Whilst the transfer of personal information to foreign-based clouds is allowed in terms of section 72 of the POPI Act, organisations have to take cognisance of the fact that there are risks associated with the transfer of data, which are outside their control. This is because outside service providers are used, and they are domiciled in (and subject to the legal systems of) foreign territories (Watson 2013; De Stadler 2013b). In addition to the security and privacy risks, there are also the risks associated with the diminution (or even complete loss) of control over the information that is entrusted to cloud service providers; and there is a potential conflict between South African law and the laws on data protection in the territories to which the information has been transferred (Bortz 2011b; Chan, Leung & Pili 2012:4).

The *International Standards for the Professional Practice of Internal Auditing* (IIA Standards 2013) state that internal auditors must know about information technology governance and risks and risk management processes, and have the skills necessary to conduct technology-related audits (IIA Standards 2013: 1210.A3; 2110.A2; 2120.A3). Internal auditors can therefore be expected to provide their companies with guidance on identifying and mitigating the risks associated with the transfer of personal information to transborder clouds (CIIA UK 2014:1; IIA Dallas 2012:14-15; Protiviti 2012:3). In order to provide adequate protection for personal information when transferring it to transborder clouds, five risks need to be addressed. Addressing these risks can form the basis on which internal auditors can build comprehensive audit plans and provide management with risk management advice and assurance for personal information flows to transborder cloud solutions. These risks relate to:

1 data location;
2 security;
3 privacy;
4 legal compliance; and
5 cloud service providers (Chan *et al* 2012:1-22; European Commission 2012:5-24; Hahn, Askelson & Stiles 2006:1-23; New Zealand Government 2009:8-38; Protiviti 2012:2).

Because these are emerging risks, there is a heightened need for effective risk management, and good corporate governance dictates that the internal audit function plays an active part in risk management (IOD 2009:93; IIA Standards 2013: 2110.A3). Internal auditors can assist companies with the identification and mitigation of these risks because they are uniquely positioned, both by training and position within corporate structures, to provide assurance and consulting services to companies. As noted previously, and repeated here because of its seriousness, failure to adequately manage the personal information that is transferred to a cloud service provider outside South Africa can result in severe penalties against and reputational damage to organisations (PwC 2012:2-5; Kafouris 2014).

The objectives of this research are therefore:

- to introduce cloud computing as a technology which has benefits for companies, while also highlighting the fact that it carries inherent risks that need to be addressed if it is going to be used successfully;
- to highlight the impact of the POPI Act on the management of personal information in South Africa by summarising the requirements of section 72 of the Act;
- to explain the crucial role of internal auditors in evaluating risk; and
- to give insight into the role that internal auditors can play in providing companies with assurance that the five risks identified above can be managed.

2 VALUE OF RESEARCH

Chan *et al* (2012:1), predicted that the use of cloud computing solutions would increase drastically in 2014. Currently (this research was conducted in April 2014), 50% of companies in South Africa already use cloud solutions, and growth at 16% per year is being forecast (Speckman 2014). With this anticipated growth, it is imperative that companies understand how to legally transfer personal information to the cloud, while simultaneously ensuring that the associated risks are identified and managed.

Organisations are at varying stages of maturity in their efforts to comply with the POPI Act. There is a broad consensus amongst authors of articles published in the general circulation media and gathered during informal discussions, that most organisations are not yet ready to manage the risks already present when dealing with personal information, nor are they able to comply with the POPI Act; it appears that they indeed lack the necessary skills, knowledge and understanding to effect such compliance (Dlamini 2013; Lamprecht 2013; Kolver 2014; Phakathi 2014).

This research is important because, in the light of the immanent implementation of the POPI Act, the progress made in the protection of personal information by South African companies is inadequate to create the requisite internal governance frameworks, from a risk management and compliance perspective, that are necessary for the optimal and legal use of transborder cloud computing services (Bortz 2012; Senathipathi, Chitra, Angeline Rubella & Suganya 2013:2712). The internal auditing profession can and must play a pivotal role in assisting to mitigate the risks associated with the transfer of personal information to transborder clouds. This research will contribute to the body of work that companies and internal auditors can draw on in their efforts to address these important tasks.

3 RESEARCH METHOD AND LIMITATIONS

The research methodology used in preparing this article is a literature review. This research explores a relatively new area which is at the intersection of technological, legal and internal auditing issues. The research is limited to the review and analysis of legislation in the areas of personal information protection, cloud computing, and the transborder flow of personal information, an overview of internal auditing in the academic arena, and the review of professional journals and opinion pieces by industry players.

4 LITERATURE REVIEW

4.1 Cloud computing

4.1.1 Introduction to cloud computing

Cloud computing provides an internet-based system of shared resources, software and information, all of which is available on demand. The systems are managed by service providers who are responsible for the necessary infrastructure, and this allows organisations to avoid the cost of owning and managing their own IT facilities and staff (Krutz & Vines 2010:3-6; Wolfe 2011:599). Cloud computing is considered a "new technology" because some of the advantages and risks that it introduces into the IT arena are new (Von Solms & Viljoen 2012:73).

There are three cloud service delivery models (Infrastructure as a Service 'IaaS', Software as a Service 'Saas', and Platform as a Service 'Paas'), and four deployment models (private cloud, public cloud, community cloud and hybrid cloud) (Hon, Hornle & Millard 2011:3; Noltes 2011:7-11). For the purposes of this research, the distinction between these models will not be considered.

While 50% of South African companies use cloud computing solutions, and a further 16% intended to start doing so in 2014, there is an even greater projected growth in cloud computing use in the rest of Africa: 44% of Nigerian companies and 24% of Kenyan companies report that they will begin to make use of the cloud "soon" (Speckman 2014). Despite this actual and projected growth, a survey by Portio Research revealed that more than 50% of IT decision-makers apparently know very little about cloud computing (Hsu 2012:14). As custodians of the personal information provided to them by customers, organisations (their directors and management) remain ultimately responsible for the protection of that information, even if it is transferred to a foreign-based cloud (IOD 2009:82-87; Tomaszewski 2013:3).

4.1.2 Advantages of cloud computing

Cloud computing's advantages include its ability to provide flexible and universal access to IT resources (both software and hardware infrastructure), and the fact that costs can be charged to customers on the basis of actual use (Hon *et al* 2011:3). The benefits of using the cloud, which make it so attractive to organisations, include the following:

- *Cost management* Organisations are able to determine what IT services they require without having to spend capital on (almost instantly obsolete) infrastructure. They can also pay for services as and when required, as opposed to entering into long-term, binding enterprise agreements preferred by local suppliers.

- *Agility in sourcing and deploying services* This has become possible because solutions are already housed in the cloud, and do not need to be rolled out into IT systems housed on organisations' premises.
- *Availability* Services are usually uninterrupted because the cloud is internet-based and thus borderless and free of operational work-day and work-shift considerations.
- *Scalability* Cloud services can be adjusted almost instantly to accommodate varying levels of demand; this can assist organisations in controlling costs.
- *Increased efficiency* Because IT management is outsourced to cloud service providers IT departments can then focus on core skills and drive innovation for business development.
- *Resilience* In the face of cyber-attacks and any type of denial-of-service event, the cloud provides almost unlimited disaster-recovery options, including mirrored data centres in multiple locations (Krutz & Vines 2010:4-10; Bilton 2011; Chan *et al* 2012:3).

4.1.3 Transborder cloud computing

According to a Deloitte and ITWeb survey, 56% of South African organisations stated that they did not transfer information across the borders of South Africa. Most of them, however, used third parties to provide them with cloud computing solutions, and thus had no idea of their data's ultimate destination, or where it was managed or stored (Chivers & Kelly 2012). The probability is that their information is being transferred outside the country, without their knowledge, as many servers are housed internationally (Kafouris 2011; Chivers & Kelly 2012). The strict and onerous requirements contained in the POPI Act do not tolerate this lack of knowledge of the ultimate storage place of personal information that organisations hold. To be able to ensure the protection of information, companies have to be aware of where it is. They also need to be fully aware of what transborder clouds are and the implications of using them because the risk inherent in the use of cloud solutions for personal information rests with organisations, regardless of where their service providers transfer the data (AbuOliem 2013:522).

4.1.4 Classification of information and the risks associated with cloud computing

According to AbuOliem (2013:521), "[c]loud computing is only attractive if it embodies the principles on privacy and data ownership". It has to be accepted that there are risks associated with the transfer of data to the cloud. Information is valuable and attacks on information technology systems continue to increase in criminal efforts to gain access to information (Fowler 2003:1). During a discussion held at Microsoft's South African offices in February 2014, Watson explained that for security purposes, before organisations make use of cloud solutions, they must go through a process of classifying information, as making use of the cloud inevitably involves some loss of control; information is often transferred off the organisation's premises and subsequently managed by cloud service providers.

The classification of information involves its categorisation according to its critical value to the organisation, and the safeguards that are necessary to ensure information confidentiality, integrity and availability (Fowler 2003:3; Hahn *et al* 2006:17). By classifying information, organisations can show how they arrive at the decisions they make for managing information, including what technology is used to process it, how it is transferred, and how it is protected (Fowler 2003:3; Hahn *et al* 2006:17). For the purpose of this research, the process of information classification will not be explored. It is sufficient to state that by classifying information, the decision to transfer it to the cloud can be critically considered in the light of the risks to which it will be exposed, and the consequences that will follow if the risks materialise.

Some of the risks that have to be explored by organisations when considering adoption of the cloud include the following:

- loss of control over the information by data subjects (providers of personal information) and the organisations which collect it;
- limited or no access to information by data subjects when it is required;
- loss of privacy and security, as cloud service providers may have access to the information;
- the threat of cyber-attacks and the consequent compromising of information;
- challenges in controlling costs: verifying that what is charged for services is commensurate with what is actually being provided;
- jurisdictional conflicts with cloud servers' host countries, where data protection and privacy laws are incompatible or non-existent; and
- difficulties in mounting challenges in the event that information security is breached (Hurwitz, Bloor, Kaufman & Halper 2009; New Zealand Government 2009:4-28).

4.1.5 Cloud computing and internal auditing

As mentioned previously, cloud computing is a technology whose use is projected to increase (Chan *et al* 2012:1; Speckman 2014). Internal audit professionals need to be aware of the advantages and of the risks associated with the use of technologies such as cloud solutions (IIA Dallas 2012:9; Protiviti 2012:3; Sammut 2013). Internal audit is well positioned as an assurance provider to assist company boards and management to identify the key risks that are inherent in the use of cloud solutions (Protiviti 2012:3) To address the impact of cloud computing on the company's risk profile, internal audit has to shift its focus from traditional IT processes and procurements, to include risks specific to this technology (Sammut 2013).

In accordance with the IIA Standards (2013: 1210.A.3 & 2120.A1) and corporate governance standards such as those presented in Chapter 7 of King III (IOD 2009), the internal audit function can, and ultimately must help the business to identify, assess and mitigate the risks associated with cloud computing, in order to ensure that business benefits are realised. Slater (2012:7) believes that in addition to auditing the cloud solutions and cloud service providers so that companies engage appropriate services, internal auditors can also play a crucial role in ensuring that the company has in place adequate security and legal compliance frameworks to mitigate the chances of risk realisation (IIA 2004:203; Hahn *et al* 2006:1; IIA Standards 2013: 2110.A2; Grant Thornton 2014).

4.1.6 The protection of personal information in cloud computing

In most organisations information has become their most valuable asset and resource (Fick 2010:22). Accordingly, it has to be treated with the same, if not a higher, level of care as the organisation's financial assets. This involves the preparation and implementation of adequate information governance measures (Fick 2010:22). Nevertheless, using cloud computing for processing and storing personal information raises serious data management risks (European Commission 2012:5; Fischer 2012:5). According to Bortz (2011a), the biggest risk organisations have to contend with when placing personal information in the cloud is the protection of data and privacy.

Many organisations have failed to pay appropriate attention to data protection in cloud solutions (Fischer 2012:34). In the cloud, information is often managed by cloud service providers, and is not fully controlled and/or monitored by the companies that gather the data. This means that there is diminished control over who can access information and who can use it. Protecting intellectual property and safeguarding employee, customer and third party data have therefore become key challenges. If any form of information management risk is realised, with personal information being illegally accessed and used, there are serious legal, financial and reputational repercussions for companies (Hsu 2012:14; PwC 2012:4; Kafouris 2014). In addition, the requirements of the POPI Act hold serious implications for the users of cloud solutions (Bortz 2011b). Persons, both natural and juristic, need the assurance that their personal information is protected, regardless of the jurisdiction in which it is housed. Hence, companies that gather the data have to adhere to the conditions stipulated by data protection laws, including the POPI Act (Fischer 2012; Kafouris 2014).

4.2 The Protection of Personal Information Act 4 of 2013 (POPI Act)

4.2.1 Introduction to the POPI Act

The POPI Act was signed into law in November 2013. Its enactment established a new and higher standard to which organisations need to adhere when managing personal information. The definition of 'personal information' is found in Chapter 1 of the POPI Act, and covers a broad spectrum of personally identifiable information categories. It also specifically extends protection to the personal information of juristic persons (De Stadler 2013b; Wehler 2013).

The purpose of the POPI Act is clearly stated in section 2 of the Act. It is to protect personal information by giving effect to the right to privacy, while balancing this against other rights such as the right of access to information. It also recognises that there needs to be regulatory guidance for the free flow and use of personal information for legitimate local and international objectives, such as the provision of services and business processes (Kuner 2011:10; Gardner 2012). The Act is designed to provide assurance that natural and juristic persons' personal information will be subject to rigorous controls when being collected, transferred, stored, secured and used by organisations, thereby minimising the opportunities for inadvertent and/or negligent disclosure and misuse (Dlamini 2013; Wehler 2013).

This new law aligns South Africa's data privacy and protection legislation with international best practice. Having been modelled on the EU's Data Protection Directive 95/46/EC (EU Directive), the POPI Act is Africa's first comprehensive data and information protection law (Wehler 2013). However, it does differ in some respects from the EU Directive. Firstly, the EU Directive deals with 'data' in general (which includes personal information), while the POPI Act focuses specifically on personal information. Given its South African focus, for the purpose of this research, data therefore refers to personal information (Fischer 2012:36; Watson 2013). It is also important to note that the definition of personal information contained in the Act includes juristic persons, whereas the EU Directive limits its scope to natural persons (Dhont & Woodcock 2014).

Chapter 3 (Part A) of the POPI Act provides eight "*Conditions for Lawful Processing of Personal Information*", the operational essence of the Act. When these are complied with and implemented fully, they provide protection for personal information, and by complying with the Act, organisations (responsible parties) avoid prosecution and possible penalties (Gardner 2012; O'Donoghue 2013).

Section 19 is part of Condition 7 (Security Safeguards) of Chapter 3 of the POPI Act, and sets out what the Act requires in terms of securing personal information to ensure its integrity and confidentiality. According to section 19(1), when personal information is under an organisation's control, the organisation is obliged to take all necessary technical and organisational measures to prevent any kind of loss, damage or unlawful access that may result in the information and the data subjects who supply the information, being compromised. Section 19 (2) goes on to state that:

19. (2) In order to give effect to subsection (1), the responsible party must take reasonable measures to-

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

This section, together with King III's (IOD 2009) recommendations on corporate governance standards, and the IIA's Standards (2013: 1210.A3, 2120.A1) on information technology risk management, collectively form the basis on which this research is premised, in that it focuses on the management of risks associated with the transborder flows of personal information to the cloud.

An organisations' failure to comply with the POPI Act, and its failure to protect the personal information in their possession or that they have control over, must be reported to the Regulator. The consequences of such a failure can result in any of the following penalties:

- significant reputational damage;
- loss of customer confidence and business;
- imprisonment for between 12 months and 10 years (section 107 of POPI);
- fines of up to R10 million (section 109 of POPI); and/or
- civil action which could be instituted by individuals or in the form of a class action (Gardner 2012; O'Donoghue 2013; Kafouris 2014).

4.2.2 The impact of POPI on the work of the internal auditing profession

The POPI Act affects every area of business because all organisations have to ensure that all personal data is managed in accordance with its parameters (IT Governance Network 2010). In this rapidly changing regulatory and business environment, internal audit needs to find new ways to deploy its risk- and control-based skills to help the company to achieve its strategic objectives and to facilitate value creation (CIIA UK 2014:2; Ernest & Young 2011:4; KPMG 2008:6-7). This includes being able to assist with management of risk pertaining to personal information. An important role that the internal audit function plays is to provide "advice to management on governance risks and controls, for example, the controls that will be needed when undertaking new business ventures" (The Institute of Chartered Accountants in England and Wales (ICAEW) 2004:3). The introduction of the POPI Act can be considered as having engineered a new venture which will have an impact on the way in which companies conduct their business.

Internal auditors have to be qualified and skilled in the operations of the businesses they serve (CIIA UK 2014:1). Besides providing guidance for the effective implementation of the controls outlined in the POPI Act, internal auditors also need to be able to test (during their audits) the efficacy of policies, processes, controls and risk mitigation steps that organisations' management teams have put in place in order to comply with the Act (Grant Thornton 2014). In addition to being familiar with the positive controls and requirements within the POPI Act, internal auditors must simultaneously understand the severity of the consequences of failing to comply with the POPI Act (Hahn *et al* 2006:1-2; Grant Thornton 2014).

4.2.3 The POPI Act and transborder flows of personal information: section 72

Information and technology have rendered the world borderless in terms of the flow of data. There are legal benefits to these advances in information flow as countries have been forced to develop effective data protection and privacy legislation (Hahn *et al* 2006:1; Kuner 2011:24). Because of the global nature of these information flows, territories are also harmonising their legislation to ensure that information can flow unhindered between countries with similar legislation (Kuner 2011:24). South Africa has recognised that harmonising its legislation with existing international laws is crucial; hence the inclusion of Section 72 in the POPI Act, which specifically regulates transborder information flows (Watson 2013; De Stadler 2013b). Quoting from the POPI Act:

TRANSBORDER INFORMATION FLOWS

Transfers of personal information outside Republic

72. (1) A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless-

(a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that-
  (i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and
  (ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

(b) the data subject consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

(e) the transfer is for the benefit of the data subject, and-
  (i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

4.2.4 Application of section 72 to transborder cloud computing solutions

The POPI Act contains certain provisions that have a direct impact on the use of foreign-based cloud solutions. Some of these provisions are found in section 72 (Bortz 2011b; Watson 2013). This section provides a good balance between the protection of personal information while simultaneously recognising the importance of the unhindered transfer of that information both out of and into the Republic, for legitimate business purposes (Watson 2013). This is beneficial for South African organisations that make use of foreign-based cloud computing solutions (Pieters 2013), and for the cloud computing service providers who transfer clients' personal information abroad for processing, management and storage (Wehler 2013).

Under section 72(1) (a), organisations are now obliged to establish what data protection laws exist in the jurisdictions to which they want to transfer personal information (Bortz 2011b). There must thus be assurance that the level of data protection in the jurisdiction where the cloud's hardware and management reside is at least comparable to the requirements of the POPI Act (Fischer 2012). If no comparable law exists, organisations can make use of Binding Corporate Rules (BCRs), which ensure that a high level of protection is afforded to personal data in an organisation. These would need to be comparable to standards set by the POPI Act (Bortz 2012).

4.3 Internal auditors and risk management: transfer of personal information flows to the transborder cloud

The role of internal audit in private organisations is to provide independent assurance that risk management, governance and internal control processes for information management are in place and operating effectively (CIIA UK 2014). Slater (2012:2) adds that internal auditors also have the task of ensuring that companies will meet the requirements to pass external audits.

4.3.1 Strategic positioning of internal auditors in companies

Chapter 7 of the King III report (IOD 2009) stresses that the internal audit function in companies not only assesses controls, but goes further and assists with risk management processes (Marks 2010). This includes the management of risks faced by the personal information that companies collect and use in the course of their business (IT Governance Network 2010). Internal auditors can and must play a pivotal role in assisting organisations to ensure that they adequately protect personal information when it is transferred to transborder clouds (PwC 2011:1-2; Protiviti 2012:3).

Internal auditors, through a combination of assurance and consulting, assist organisations to achieve their goals (CIIA UK 2014:1). Internal auditors are uniquely positioned within organisations, fulfilling their role as independent advisors by maintaining a thorough knowledge about their organisation's strategy, processes and operations (ICAEW 2004:1-2; CIIA UK 2014:1). The multidimensional nature of the internal auditor's role lends credence to the assertion that through effective internal auditing, the risks that are associated with the transborder flows of personal information to the cloud can be identified and effectively managed. Internal auditors have the following advantages over normal line and staff functions in that they have

- access to management whom they can independently advise;
- access to international best practice through organisations such as the Institute of Internal Auditors (IIA);
- an in-depth understanding of organisational structure, strategy and operations;
- skills to assess policies, processes and procedures, and the ability to test their efficacy;
- the ability to identify fraud, and to control shortfalls and inherent risks; and
- the critical knowledge to recommend controls to mitigate risk and to ensure compliance (Hahn *et al* 2006:1, 17-25; Protiviti 2012:3; CIIA UK 2014).

Barac and Coetzee (2012:36) state that there is an increasing demand for internal auditors who have the skills and ability to identify and advise on the mitigation of business risks, and that there is currently a lack of such specialisation in areas such as information technology, information management and risk management. In order to assist their organisations effectively, internal auditors need to add to their abilities by continually enhancing their skills and in-depth knowledge about the risks associated with personal information management and cloud computing, as is required by the IIA Standards (2013: 2120.A1; 1210.A3).

4.3.2 Risk management process: the role of internal auditors

The National Institute of Standards and Technology (NIST) defines risk as "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization" (Noltes 2011:23). The likelihood of a future negative event occurring is considered by assessing how often similar threats to an IT system have occurred, as well as the system's potential vulnerabilities. Impact refers to the extent of harm that could be caused to the organisation by the exploitation of identified vulnerabilities. Accordingly, risk is measured as the product of 'likelihood' and 'impact' (Noltes 2011:23).

According to the IIA Standards (2013), internal auditors must "evaluate the effectiveness and contribute to the improvement of risk management processes" (IIA Standards 2013: 2120:A1). With the passing of

the POPI Act, internal auditors face a new and exacting challenge in dealing with data protection in South Africa. According to PwC (2012), "[k]eeping the audit committees of their organisations appraised of emerging risks and effective ways to address them is a key role of internal audit". The IIA Standards (2013) state that internal auditors must have the necessary proficiency and expertise to identify key information technology risks, and the skills and procedures to perform appropriate audits (IIA Standards 2013: 1210:A3).

Internal auditors also need to ensure that threats to information technology are fully considered and that the necessary policies, procedures and controls are in place so that organisations comply with legislative and corporate governance requirements (IIA Standards 2013: 1210.A3 & 2120.A2; PwC 2012:8; IOD 2009: 93). In order to accurately inform the audit committee about emerging information technology risks and how to mitigate them, it is important for internal auditors to understand the information technology governance systems of their organisations. They can then assess the effectiveness of the systems in furthering the objectives of the organisations (IIA Standards 2013: 2110.A2).

Internal auditors can play an effective risk management role by effecting the following:

a *Risk identification, assessment and analysis*. The internal audit function assists companies to identify and assess the risks they might face in achieving their business objectives. Internal audit also helps assess the likelihood of the risk being realized, and the probable impact thereof, helping to prioritize management attention by ranking risks in terms of their potential severity.

b *Controls evaluation and remediation*. The internal audit function can assess whether the institution's controls, which include the policies and procedures they have put in place, are adequate to mitigate the identified risks.

c *Regulatory compliance*. Regulatory compliance risk has greatly increased due to increasing number of statutory and regulatory frameworks that must be complied with. These include the King III report (IOD 2009), the new (2008) Companies Act, and now the POPI Act. A culture of compliance can enhance an organization's risk maturity through ongoing internal audit assessment and associated remediation efforts.

d *Improved process effectiveness and efficiency*. Internal audit can also help to enhance the effectiveness and efficiency of continuous assessment processes, and to identify any shortcomings in the methodology used to complete tasks.

e *Assurance to the board, management and other stakeholders*. Internal audit provides assurance that companies have governance frameworks that effectively mitigate the various risks they face, and that contribute to meeting business objectives (Telavance 2012; Ernest & Young 2011:5-6; PwC 2011; Chan *et al* 2012:4-6, 17-20; CIIA UK 2014:1-2).

4.4 Five emerging risks inherent in the transfer of personal information to the transborder cloud, and the associated role of the internal auditor

Nicolaou, Nicolaou and Nicolaou (2012) state that companies must be able to audit their cloud services in order to assess the adequacy of controls for risks that are inherent in the use of cloud technology. It is axiomatic that knowledge of these risks is critical in that it enables internal auditors to audit a cloud computing solution properly, and thereby to add value to their organisations (Nicolaou *et al* 2012). Five emerging risks require analysis, understanding and effective management if personal information is going to be transferred to the transborder cloud in a manner that is compliant with the requirements of section 72 of the POPI Act. These risks are or relate to the following:

1 data location;
2 security;
3 privacy;
4 legal compliance; and
5 cloud service providers (Chan *et al* 2012:1-22; EU Commission 2012:5-24; Hahn *et al* 2006:1-23; New Zealand Government 2009:8-38).

Internal auditors can provide assurance that the management of such risks is appropriate by being aware of the risks associated with the use of this technology, and by assisting in the mitigation of such risks through ongoing assessments and audits (IIA Dallas 2012:9; Protiviti 2012:2). To ensure the security of personal information and compliance with legislative requirements (including those of the POPI Act), specific risks should be proactively identified, understood and management protocols developed prior to making use of cloud services (Protiviti 2012:6; Bortz 2011b). It is essential that internal audit participates in the process from the initial stages of cloud technology implementation, and before the "live" personal information is transferred to the cloud. Failure to do this invites the possibility that the associated risks will be realised, with negative consequences for companies. After the decision has been taken to make use of cloud solutions, it is also important to continuously evaluate and monitor responses to the known risks, and to identify the potential for new ones (New Zealand Government 2009:6; Protiviti 2012:6). Because South African companies are increasingly making use of cloud computing, and in view of the fact that the POPI Act will come into effect in 2016, it is imperative that internal auditors augment their knowledge base, and enhance their skills so that they can provide the requisite levels of assurance (Cloud Security Alliance 2011:46; IIA Dallas 2012:26).

4.4.1 Data location

When cloud solutions are hosted outside national borders, it is possible that neither the primary locations nor the backup locations of the data centres to which personal information is transferred are known to the company (Protiviti 2012:2; Chivers & Kelly 2012; Chan *et al* 2012:14). Thus transferring data outside national borders can limit the control that companies can exercise over their personal

information (New Zealand Government 2009:6; Chan *et al* 2012:5; European Commission 2012:5). This will in turn have a direct bearing on the security of the personal information, as it may be difficult to establish the jurisdiction in which the data is stored, which will in turn affect the ability of companies to show compliance with personal information protection requirements (Chan *et al* 2012:5, 14).

Internal auditors give assurance regarding the management of risks associated with data locations by conducting audits (including physical audits of actual locations), before the company signs contracts, service level agreements (SLAs) and operation level agreements (OLAs) with service providers (Noltes 2011: 34-36; Bortz 2012; Sammut 2013). Simultaneously, company management must be assisted to understand the information protection and data security issues, and the legislative and regulatory prerequisites which will have an impact on security, before making use of transborder clouds (Chan *et al* 2012:14). If data centres are situated in locations with inadequate or incompatible data protection laws (laws which are not comparable with the POPI Act), internal auditors can advise companies to negotiate a location change to meet regulatory requirements, or to find alternative service providers in more POPI-compliant jurisdictions, as the consequences of failing to comply with the Act are significantly dire.

4.4.2 Security

Security is a serious concern when transferring information to a transborder cloud (Krutz & Vines 2010:20; Bortz 2011b), and effective security is key to successful transfer. Security risk management includes the prevention of data leakages and loss, and the limiting of opportunities for malicious insiders and cyber-attacks (Chan *et al* 2012:5). Threats to security are of particular concern and require intensely focused attention because, by making use of cloud service providers and transferring information outside South Africa, companies are introducing the additional risks that arise when they surrender the right to respond directly to events which may affect the integrity of personal information now residing in cross-border clouds (New Zealand Government 2009: 22; Hurwitz *et al* 2009:102; Bortz 2011b).

Condition 7 of the POPI Act (s 19) states that companies must put 'security safeguards' in place in order to protect personal information against threats (Grant Thornton 2014). The nature of security threats is evolving at a rapid pace and these need to be assessed regularly (New Zealand Government 2009:23). New methods of attack are constantly being employed and it is imperative that internal auditors keep abreast of new threats by engaging in fora where attacks on cloud information and security issues are discussed (Fowler 2003:1; IIA 2004:171; PwC 2012:8). It is also necessary for internal audit to develop new skills and tools in order to identify data security risks and make sure that their companies implement the correct policies, processes and controls to secure personal information in the cloud (ENISA 2009:19; PwC 2012:10). To provide security assurance regarding this cloud information, internal audit needs to make it clear, usually through the audit committee, that information management and security are the joint responsibility of the board and management, and is not just an IT departmental issue (PwC 2012:10).

Companies must ensure that internal audit can regularly audit the information management security processes that are in place and provide the board with its assurance reports (IIA 2004:171; Bortz 2012). Comprehensive assessments and continuous monitoring of personnel skills, policies, procedures and controls have to be conducted to identify any weaknesses which could result in security breaches, both internally and at service provider locations (Cloud Security Alliance 2011:75-80; UK Government 2012:14; PwC 2012:8). This includes conducting vulnerability assessments and penetration tests (Hahn *et al* 2006:21; Cloud Security Alliance 2011:123, 128). It is also necessary for internal audit to have the ability to assess the service providers' security policies and security certifications, to ensure that the level of service that is being provided meets the needs of the company (Bortz 2011b; European Commission 2012: 22; Noltes 2011:19).

4.4.3 Privacy

The protection of privacy is a risk management issue (IIA 2004:203; Hahn *et al* 2006:1). Companies must manage personal information effectively in order to maintain their good reputations. This includes ensuring that privacy laws are adhered to and that data subjects' privacy rights are protected when personal information is collected and transferred to transborder clouds (New Zealand Government 2009:25; Krutz & Vines 2010:42, 49). According to Bortz (2011b), loss of privacy is one of the biggest risks that cloud users face. It is therefore necessary, as part of the audits that internal auditors undertake, to ensure that service providers have adequate privacy policies, protection procedures and controls in place before any contract is signed (Bortz 2011b; Hahn *et al* 2006:5). Breaches in security and privacy, which could compromise the personal information that is transferred outside South Africa to the cloud, can result in severe penalties and jail time, as is stipulated in the POPI Act, in addition to reputational damage to organisations (PwC 2012:2-5; Kafouris 2014).

Internal auditors can also give assurance by working with legal counsel to assess the degree to which the right to privacy which is given effect by the company's policies, procedures and controls in relation to personal information, is also applicable (practically enforceable) to data that is transferred to the cloud. A clear understanding of the data management process is essential if internal auditors are going to perform regular reviews of these processes, to test their efficacy and identify any threats (Hahn *et al* 2006:4, 20; Grant Thornton 2014). Performing gap analyses of information flows and management procedures in internal procedures, and recommending implementation of best practice to assess consistency and compliance, is something that internal auditors can do to provide further assurance that privacy is being protected (Hahn *et al* 2006:5).

4.4.4 Legal compliance

There are national and regional laws and regulations which require that personal data be protected (Cloud Security Alliance 2011:36). Compliance with these laws and regulations is a crucial starting point for the protection of personal information and the right to privacy (Hahn *et al* 2006:18). Hence, when making use of cloud solutions, companies must ensure that they adhere to legal and regulatory requirements (Cloud Security Alliance 2011:38, 47; Protiviti 2012:2).

Personal information has to be managed in accordance with the requirements of the POPI Act. More specifically, for transborder transfer of data to the cloud, section 72 has to be complied with (Watson 2013; De Stadler 2013b). (Section 72 requires the cloud service provider to have in place "substantially similar" legal and/or corporate rules to those present in the POPI Act.) In order to give assurance with regard to the legal compliance risks associated with the transfer of personal information to the transborder cloud, internal auditors must have a good understanding of the POPI Act's requirements in general and of section 72 in particular. Companies should have processes in place that ensure compliance in every area of the business that handles personal information (Watson 2013; De Stadler 2013b).

Assurance can only realistically be given once an assessment of staff training and awareness programmes has been undertaken, and internal auditors are confident that there is an organisational culture of compliance (IIA 2004:180; UK Government 2012:21). An evaluation of the legal aspects of policies, procedures, processes and controls by internal audit will also assist companies to achieve their compliance goals (Bortz 2011b; Cloud Security Alliance 2011:48 UK Government 2012:22).

4.4.5 Cloud service providers

Cloud solutions are often provided by independent cloud service providers (as opposed to globally represented corporates with their own corporately managed (internal) cloud service). By contracting providers of cloud services to store/secure/manipulate/manage their data, companies thus cede to outsiders control over the personal information originally obtained by and entrusted to these companies (New Zealand Government 2009:6). Therefore, these cloud service providers have to be carefully evaluated, and selected and managed in a manner that ensures that the solutions they provide will benefit the company, and will not expose it to undue risks that may negatively affect the business (Bortz 2011b; Protiviti 2012:3). Ultimately, the company is responsible for the security of the personal information, even if it engages cloud service providers and gives them physical/electronic control over the information. As there may be jurisdictional issues associated with engaging service providers whose services are domiciled and/or provided from outside South Africa, specialist legal advice should be obtained when agreements are drafted and before they are signed (New Zealand Government 2009:28)

In providing assurance, the internal auditor's role includes investigating all service providers before services are procured, and thereafter constantly monitoring them to ensure that the required services are being provided in a manner that demonstrates compliance with legislative requirements (UK Government 2012:12; Protiviti 2012:6). A "right-to-audit" clause must be included in all agreements between companies and cloud service providers (Cloud Security Alliance 2011:50; Chan *et al* 2012:13; Bortz 2012; Teremi 2012:13). Internal auditors must also participate in the negotiation or review of all service provider contracts and SLAs to ensure that they are comprehensive; contracts must provide information about the services to be provided, the location of data centres to which personal information will be transferred, the processes and procedures involved in managing personal information in the cloud, and finally, the penalties for breaches must be explicit and comprehensive (Noltes 2011:24; Protiviti 2012:5; Chan *et al* 2012:13; Bortz 2012). Internal auditors must review these service provider contracts, agreements and processes to ensure that all the requirements of section 72 of the POPI Act are met, because liability for any compliance failures rests with the company.

5 CONCLUSIONS AND FURTHER RESEARCH

As transborder data flows increase globally, there is a need to regulate the management of information when it is transferred outside its country of origin (Kuner 2013:1). It is therefore important for companies to measure the risks that are present when transferring personal information outside South Africa (even though this is permissible in terms of section 72 of the POPI Act), and then decide whether it is prudent to do so. It is clear from the case of the Zurich Insurance data leak that there can be serious financial and reputational consequences to any kind of breach or failure in the measures employed to protect personal information (Telavance 2012; Ernest & Young 2011:5-6; PwC 2012:7-8; Chan *et al* 2012: 4-6, 17-20; CIIA UK 2014:1-2).

In South Africa, the regulation of personal information transfer to transborder clouds is an exciting new area where the issues of compliance with the POPI Act (legal), cloud computing (IT) and internal auditing (auditing and risk management) intersect, and presents opportunities for the internal auditing profession to play a pioneering and critical role in enabling the successful integration of these diverse fields. The importance of having a skilled and active internal audit function has been repeatedly emphasised: the diversity of their skillset enables them to play a leading role in this new area. This research has attempted to show that internal auditors, as independent assurance providers with a keen understanding of their companies' business strategies, operations and goals, can lead their companies to the achievement of compliance with the POPI Act, by helping organisations to successfully mitigate the risks that flow from the use of transborder clouds for storage and processing of personal information.

Internal auditors can play a crucial role in cloud computing risk management in that they are able to give assurance on the management of the five emerging risks associated with the transfer of

personal information to the transborder cloud, risks associated with data location, security, privacy, legal compliance and cloud service providers' operational procedures. Knowledge of these risks is critical in order for internal auditors to audit transborder cloud computing solutions effectively and thus to add value to their organisations (Nicolaou *et al* 2012). The auditing of cloud service providers (to assess the solutions they provide and the adequacy of these to meet the company's needs), is a key internal audit function (Bortz 2011b; Protiviti 2012:3). If the wrong service providers are engaged, it may result in the risks being realised, and the personal information in the transborder cloud being lost or compromised. Internal audit can provide assurance on risks associated with data location and security by conducting audits (including physical audits of actual locations and certifications), before the signing of agreements with service providers, as well as by determining the legal and regulatory regimes that pertain at the locations of transborder cloud data centres, and the adequacy of security measures they have in place to protect personal information (Cloud Security Alliance 2011:75-80; Noltes 2011:34-36; Bortz 2012; Sammut 2013). An internal audit assessment of the company's culture of compliance (including general awareness and staff training programmes, policies and controls), can provide assurance that the protection protocols for personal information are congruent with the requirements of the POPI Act (IIA 2004:180; UK Government 2012:21). Internal audit can also give assurance that the right to privacy is being protected by reviewing company and service provider privacy policies and procedures. In addition, gap analyses may be performed to ensure that all weaknesses are being identified and mitigated (Hahn *et al* 2006:5; Grant Thornton 2014).

As this is a new area, this research is necessarily introductory and is intended to give some insight into the impact that the POPI Act has already had on the specific area of transborder transfers of personal information. Further research can and must be undertaken on the development of comprehensive organisational frameworks and audit plans for this area of business life. At a national level, regulations should be developed (as has been done overseas), where data protection laws have led to research on and the publication of guidelines for cloud computing, with a focus on data protection. South Africa has developed data protection legislation based on international standards, and this work can be taken further by the development of comprehensive regulations regarding management of personal information in specific areas such as cloud computing.

Acknowledgement

Thanks to Tammy Bortz, Director at Werksmans Attorneys, for providing initial insights into cloud computing and POPI.
Thanks to Theodore Watson, Attorney at Microsoft South Africa, for kindly sharing his knowledge, practical experience and time for this research.

REFERENCES

AbuOliem, A. 2013. Cloud computing regulation: An attempt to protect personal data transmission to cross-border cloud storage services. *International Journal of Computer and Communication Engineering*, 2(4):521-525.

AON South Africa. 2012. *South African businesses unprepared for the growing risk of cyber attacks.* [Online]. https://www.aon.co.za/index.php/en/news-articles/244-south-african-businesses-unprepared-for-the-growing-risk-of-cyber-attacks (Accessed: 28 April 2014).

Barac, K. & Coetzee, G.P. 2012. The effect of specific internal audit function features on the demand for internal auditors in South Africa. *The Southern African Journal of Accountability and Auditing Research*, 13:36.

BBC News. 2010. *Zurich Insurance fined £2.3m over customers' data loss*. [Online]. http://www.bbc.co.uk/news/business-11070217 (Accessed: 28 April 2014).

Bilton, A. 2011. Internal audit and the cloud: part 1. *Audit & Risk.* [Online]. http://auditandrisk.org.uk/features/internal-audit-and-the-cloud-part-1 (Accessed 2 May 2014).

Bortz, T. 2011a. (t.bortz@werkemans.co.za) Discussion on cloud computing. [Email to:] Jangara, T.C. (tjangara@deloitte.co.za). January 2011.

Bortz, T. 2011b. *South Africa: SA business warned to mitigate cloud computing risks*. Werksmans Attorneys. [Online]. http://www.werksmans.com/virt_media/sa-business-warned-to-mitigate-cloud-computing-risks/ (Accessed: 9 January 2012).

Bortz, T. 2012. Contracting in the cloud (Part 2) – so what's new? *Legal Brief Werksmans Attorneys*. [Online]. http://www.werksmans.com/legal-briefs-view/contracting-in-the-cloud-part-2-so-whats-new/ (Accessed: 24 November 2013).

CBS News. 2013. *Sony fined in U.K. over PlayStation cyberattack*. [Online]. http://www.cbsnews.com/news/sony-fined-in-uk-over-playstation-cyberattack/ (Accessed: 28 April 2014).

Chan, C., Leung, E. & Pili, H. 2012. *COSO Enterprise risk management for cloud computing*. Crowe Horwarth LLP. [Online]. http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf (Accessed: 20 January 2014).

Chartered Institute for Internal Auditors United Kingdon (CIIA UK). 2014. What is internal audit? [Online]. http://www.iia.org.uk/about-us/what-is-internal-audit/ (Accessed: 27 June 2014).

Chivers, D. & Kelly, T. 2012. Why SA companies should take heed of the Protection of Personal Information Bill. *Deloitte SA Blog*. [Online]. http://deloitteblog.co.za/tag/protection-of-personal-information-bill/ (Accessed: 27 February 2014).

Chung, M. & Hermans, J. 2010. *KPMG's 2010 Cloud Computing Survey*. Netherlands. KPMG.

Cloud Security Alliance. 2011. *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0*. [Online]. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (Accessed: 15 January 2014).

De Stadler, E. 2013a. *Intro to the Protection of Personal Information bill (part 1): When does PoPI apply?* [Online]. http://www.esselaar.co.za/legal-articles/intro-protection-personal-information-bill-part-1-when-does-popi-apply (Accessed: 4 February 2014).

De Stadler, E. 2013b. *Intro to POPI (part 8): Trans-border information flow*. [Online]. http://www.novcon.co.za/articles/intro-popi-part-8-trans-border-information-flow (Accessed: 4 February 2014).

Dhont, J. & Woodcock K. 2014. *South Africa enacts new data protection law*. Lorenz International Lawyers. [Online] http://www.lorenz-law.com/wp-content/uploads/South-Africa-Enacts-New-Data-Protection-Law.pdf (Accessed: 14 February 2014).

Dlamini, A. 2013. POPI headache looms. *IT News Africa* October 14, 2013. [Online]. http://www.itnewsafrica.com/2013/10/popi-headache-looms/ (Accessed: 5 January 2014).

European Network and Information Security Agency (ENISA). 2009. *Cloud computing: Benefits, risks and recommendations for information security*. [Online]. https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment (Accessed: 23 July 2014).

Ernest & Young. 2011. *Internal audit's evolving role: A proactive catalyst of business improvement.* [Online]. http://www.tapestrynetworks.com/upload/Tapestry_EY_ACLN_InSights_Apr11.pdf (Accessed 28 June 2014).

European Commission. 2012. Article 29 Data Working Party. *Opinion 05/2012 on Cloud Computing.* [Online]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (Accessed: 14 February 2014).

European Parliament and Council. 1995. EU Data Protection Directive (Directive 95/46/EC) (EU Directive). [Online]. http://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm (Accessed 14 February 2014).

Fick, J. 2010. Directorship: A king's ransom. *IOD Directorship Magazine*. Jan - Mar 2010, 22-25.

Fischer, P. 2012. Global standards: Recent developments between the poles of privacy and cloud computing. *3 JIPITEC 1* para 33-8.

Fowler, S. 2003. *Information classification: Who, why and how*. SANS Institute.

Gardner, Z. 2012. Protection of Personal Information Bill, No. 2. *ENS Africa*. [Online]. http://www.ensafrica.com/news/Protection-of-Personal-Information-Bill-No-2?Id=816&STitle=corporate+commercial+ENSight (Accessed: 3 February 2014).

Gartner, 2010. *Gartner says worldwide cloud services market to surpass $68 billion in 2010*. [Online]. http://www.gartner.com/newsroom/id/1389313 (Accessed: 22 July 2014).

Grant Thornton. 2014. New POPI Act brings operational, financial and legal burden to businesses and their third party outsource service providers – Grant Thornton. [Online]. http://www.gt.co.za/news/2014/05/new-popi-act-brings-operational-financial-and-legal-burden-to-businesses-and-their-third-party-outsource-service-providers-grant-thornton/ (Accessed: 19 June 2014).

Hahn, U., Askelson, K. & Stiles, R. 2006. Global Technology Audit Guide 5: Managing and auditing privacy risks. *The Institute of Internal Auditors (IIA)* 1-25.

Hon, W.K., Hornle, J. & Millard C. 2011. *Data protection jurisdiction and cloud computing: When are cloud users and providers subject to EU data protection laws?* The cloud of unknowing, Part 3. Legal Studies Research Paper no 84/2011. Queen Mary University of London, School of Law.

Hsu, W-H.L. 2012. Conceptual framework of Cloud Computing Governance Model: An education perspective. *IEEE Technology and Engineering Education (ITEE)*, 7(2) June 12-16.

Hurwitz, J., Bloor. R., Kaufman, M. & Halper, F. 2009. *Cloud computing for dummies.* Indiana: Wiley.

Institute for Directors (IOD). 2009. *King Report on Corporate Governance in South Africa*. IOD: South Africa.

Institute for Internal Auditors Research Foundation (IIA). 2004. *The Professional Practices Framework for Internal Auditing (PPF).* [Online]. http://www.iadb.org/aug/includes/ProfPracFramework.pdf (Accessed: 28 July 2014).

Institute for Internal Auditors Dallas Chapter (IIA Dallas). 2012. *Cloud computing: A study of internal audit's preparedness in the Dallas area.* Institute of Internal Auditors. [Online]. https://na.theiia.org/iiarf/Public%20Documents/IIA%20Dallas%20Research%20Project%20-%20Final%20Submission.pdf (Accessed: 26 June 2014).

IT Governance Network. 2010. *Privacy & protection of personal information*. [Online]. http://deloitteblog.co.za/2014/01/16/cloud-computing-and-ppi-finding-your-bearing/ (Accessed: 28 June 2014).

Kafouris, D. 2011. Deloitte talks about maintaining privacy and security in the cloud. *Deloitte SA Blog*. [Online]. http://deloitteblog.co.za/tag/protection-of-personal-information-bill/ (Accessed: 27 February 2014).

Kafouris, D. 2014. Cloud computing and PPI: Finding your bearing. *Deloitte SA Blog*. [Online]. http://deloitteblog.co.za/2014/01/16/cloud-computing-and-ppi-finding-your-bearing/ (Accessed: 27 February 2014).

Kolver, L. 2014. SA businesses not ready for POPI implementation – Grant Thornton. Polity.org.za. [Online]. http://www.polity.org.za/article/sa-businesses-not-ready-for-popi-implementation-grant-thorton-2014-03-06 (Accessed: 06 June 2014).

KPMG, 2008. *The evolving role of the internal auditor: Value creation and preservation from an internal audit perspective.* [Online] https://www.kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Risk-Compliance/Documents/The%20Evolving%20role%20of%20the%20Internal%20Auditor.pdf (Accessed 19 June 2014).

Krutz, R.L. & Vines, R.D. 2010. *Cloud security: A comprehensive guide to secure cloud computing.* United Kingdom: John Wiley & Sons.

Kuner, C. 2011. *Regulation of transborder data flows under data protection and privacy law: Past, present and future*. OECD Digital Economy Papers, No. 187, OECD Publishing.

Kuner, C. 2013. *Transborder data flows and data privacy law*. United Kingdom: Oxford University Press.

Lamprecht, I. 2013. *Few organisations ready for Popi.* Moneyweb. [Online]. http://www.moneyweb.co.za/moneyweb-corporate-governance/few-organisations-ready-for-popi (Accessed: 24 February 2014).

Liston, S. 2012. *The cloud: Data protection and privacy whose cloud is it anyway?* GSR Discussion Paper. [Online]. http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/documents/GSR12_Privacy_Liston_6.pdf (Accessed: 24 February 2014).

Marks, N. 2010. *The future of the internal audit profession.* [Online]. http://normanmarks.wordpress.com/2010/06/29/the-future-of-the-internal-audit-profession/ (Accessed: 29 July 2014).

New Zealand Government. 2009. *Government use of offshore information and communication technologies (ICT) service providers: Advice on Risk Management.* New Zealand. [Online] http://ict.govt.nz/assets/Uploads/Drupal/offshore-ICT-service-providers-april-2007.pdf (Accessed: 10 March 2014).

Nicolaou, C.A., Nicolaou, A.I., & Nicolaou, G.D. 2012. Auditing in the cloud: Challenges and opportunities. *The CPA Journal.* New York State Society of Certified Public Accountants. [Online]. http://callcenterinfo.tmcnet.com/news/2012/02/27/6147821.htm (Accessed 28 June 2014).

Noltes, J. 2011. Data location compliance in cloud computing. Masters thesis, University of Twente. [Online]. http://essay.utwente.nl/610421 (Accessed 01 July 2014).

O'Donoghue, C. 2013. New data protection law for South Africa. *Mondaq*. [Online]. http://www.mondaq.com/x/283662/data+protection/New+Data+Protection+Law+For+South+Africa (Accessed: 20 January 2014).

Phakathi, B. 2014. Business 'not ready' for personal information law. *Business Day.* [Online]. http://www.bdlive.co.za/business/2014/03/07/business-not-ready-for-personal-information-law (Accessed: 15 March 2014).

Pieters, M. 2013. Is cross border data transfer prohibited in terms of POPI?' *Bandwidth Blog* 22 January 2013. [Online]. http://www.bandwidthblog.com/2013/01/22/is-cross-border-data-transfer-prohibited-in-terms-of-popi/ (Accessed: 14 January 2014).

Protiviti. 2012. *Internal Audit's Role in Cloud Computing.* [Online]. http://www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/IA-Role-Cloud-Computing-Protiviti.pdf (Accessed 23 April 2014).

PwC. 2011. *Cloud computing and the internal audit function*. [Online]. http://www.pwc.com/us/en/issues/cloud-computing/navigating-the-risks-of-cloud-computing.jhtml (Accessed: 23 June 2014).

PwC. 2012. *Fortifying your defences: The role of internal audit in assuring data security and privacy.* [Online]. http://www.pwc.com/en_US/us/risk-assurance-services/assets/pwc-internal-audit-assuring-data-security-privacy.pdf (Accessed: 23 June 2014)

Sammut, G. 2013. Internal audit takes on emerging technologies. *Mondaq*. [Online]. http://www.mondaq.com/x/216430/technology/Internal+Audit+Takes+On+Emerging+Technologies (Accessed: 28 June 2014).

Senathipathi, K., Chitra, S., Angeline Rubella, J. & Suganya, M. 2013. A cross border access to data stored in the cloud. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 2(10):2707–2714.

Slater, W. 2012. The roles of the internal audit team in cloud computing. *Bellevue University.* [Online]. http://www.billslater.com/writing/CYBR_615_Week_01_Written_Homework_Assignment_from_W_F_Slater_.pdf (Accessed: 23 June 2014).

South African Government. 2013. *Protection of Personal Information Act* 4 of 2013. Pretoria: Government Printer.

Speckman, A. 2014. African rivals pass SA in cloud computing. *Business Report*. [Online]. http://www.iol.co.za/business/companies/african-rivals-pass-sa-in-cloud-computing-1.1669604#.U3k4esuKBjp (Accessed 2 April 2014).

Telavance. 2012. Risk management: How internal audit can play a key role. [Online] http://www.telavance.com/advantage/previous-issues/current-issue/risk-management-how-internal-audit-can-play-a-key-role/ (Accessed 28 June 2014).

Teremi, I. 2012. Privacy, data flows and the cloud. *Practical Advice_ Commercial Outcomes. Kreisson Legal*. [Online]. http://www.kreissonlegal.com.au/wp-content/uploads/2012/08/2-Privacy-Data-Flows-Cloud.pdf (Accessed: 5 March 2014).

The Institute of Chartered Accountants in England and Wales (ICAEW). 2004. *Guidance for audit committees: The Internal Audit function.* The Institute of Chartered Accountants in England and Wales.

The Institute of Internal Auditors. 2013. *International Standards for the Professional Practice of Internal Auditing.* [Online]. http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/full-standards/?search=risk (Accessed: 7 April 2015).

Tomaszewski, J. 2013. A board's legal obligations for the cloud: You have to carry an umbrella. *Business Law Today*. [Online]. http://www.americanbar.org/publications/blt/2013/08/03_tomaszewski.html Accessed: 20 January 2014.

United Kingdom (UK) Government. 1998. Data Protection Act. Information Commissioner's Office (ICO), 2012. *Guidance on the use of cloud computing*. United Kingdom. [Online]. http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx (Accessed: 5 March 2014).

Von Solms, R. & Viljoen, M. 2012. Cloud computing service value: a message to the board. *South African Journal of Business Management* 43 (4):73-81.

Watson, T. 2013. Data sovereignty under the protection of personal information act. *Microsoft Press Article.* [Online]. http://www.microsoft.com/southafrica/press/Pages/Article.aspx?id=44. (Accessed: 10 February 2014).

Watson, T. 2014. Discussion at Microsoft South Africa. Bryanston. February 2014.

Walker, D. & Meiring, I. 2010. *King Code and developments in corporate governance.* Werksmans Attorneys.

Wehler, A. 2013. South African Parliament passes the Protection of Personal Information Bill. *The Chertoff Group*. [Online]. http://safegov.org/2013/9/16/south-african-parliament-passes-the-protection-of-personal-information-bill (Accessed: 10 February 2014).

Wolfe, H.B. 2011. Cloud computing: The emperor's new clothes of IT. *Proceedings of Informing Science & IT Education Conference (InSite)*. [Online]. http://proceedings.informingscience.org/InSITE2011/InSITE11p599-608Wolfe281.pdf (Accessed: 9 January 2012).