Regulatory Compliance in Cloud Computing: An IT perspective

Melanie Viljoen[1], Rossouw von Solms[1] and Vivienne Lawack-Davids[2]
Institute for ICT Advancement[1]and Department of Law Management[2],
Nelson Mandela Metropolitan University, P. O. Box 7700, Port Elizabeth 6031
Tel: +27 41 5043604, Fax: +27 41 9604
email: {Melanie.Viljoen, Rossouw.VonSolms, Vivienne.Lawack-Davids}@nmmu.co.za

Abstract – All well-governed organizations should be able to demonstrate due diligence in ensuring regulatory compliance in applicable fields, including IT. Within the field of IT, a relatively new computing paradigm, cloud computing, is being adopted by organizations around the world. There are concerns regarding compliance with cloud computing. This paper highlights these concerns, and proposes a high-level set of guidelines for cloud computing regulatory compliance.

Index Terms—Cloud Computing, Cloud computing compliance

I. Introduction

The importance of proper IT governance has become more apparent in recent years. There are now well-recognized standards and guidelines for IT governance. It has been highlighted for a number of years that IT governance should be the responsibility of executive managers, and not a task to be undertaken by the IT department of an organization alone.

Compliance is a fundamental component of IT governance. An internationally accepted standard for IT governance [12] lists conformance as one of the six principles of good governance. Organizations should therefore, clearly be concerned with ensuring IT compliance. Well-governed organizations should be compliant with the laws and regulations, as well as with internal policies and practices.

Cloud computing is a development in the field of IT, which is being adopted by organizations today. Cloud computing is a computing paradigm which is associated with many potential business benefits for organizations. There are, however, various concerns about cloud computing. These include concerns about how organizations using cloud computing will be able to demonstrate compliance, which is an integral component of governance, as pointed out earlier.

This paper discusses concerns that organizations have about using cloud computing services in a compliant manner. It then proposes a set of guidelines that could be used to assist in demonstrating due diligence when embarking on the process of deciding on the adoption of cloud-computing services within organizations.

II. Methodology

As stated in the introduction, there are concerns regarding demonstrating compliance when adopting cloud-computing solutions. The objective of this paper, therefore, is to describe research that has been conducted to develop, with a set of guidelines, what could be used to assist IT managers in demonstrating regulatory compliance when adopting cloud-computing services. From a methodological point of view, the design-science paradigm, as described by Hevner, March, Park and Ram [10], for the design of business-oriented solutions by means of artifacts, in this case guidelines, was followed. The guidelines that will be described have been formulated, following a literature review and interviews with IT managers and legal experts.

The legal experts that were interviewed are both professors of law with jointly over 32 years of experience in the field. The IT manager is well qualified in the field of IT management, and has many years of experience in this field.

From the literature review and the interviews described above, a set of guidelines for regulatory compliance in the adoption of cloud computing has been concluded. The guidelines have been verified through a case study at a South African university, which has followed the guidelines in the adoption of cloud-based emails for students at their university. Before the guidelines are explained, however, the importance of IT compliance and the concerns relating to compliance with cloud computing specifically are elaborated on.

III. The Importance of IT Compliance

The word ‘comply’ is a verb that expresses the idea of acting in accordance with something. To comply can also mean to obey, abide by, adhere to, or to conform to [4]. Organizations that are compliant are those which meet the obligations placed on them by regulatory bodies and internally adopted policies and standards.

There are various reasons why organizations would want to demonstrate their compliance. One clear reason for this is that all organizations are under legal obligation to demonstrate compliance with applicable legislation. Failure to do so could result in fines or even imprisonment [9].

Ensuring compliance is also an integral part of good governance [12]. Good governance in organizations is desirable. Research highlights the benefits of demonstrating good governance [12]. A lack of governance can, likewise, disadvantage organizations.

As organizations become more reliant on information technology (IT), it is appropriate that IT governance should receive attention in any organization. IT governance should be an integral part of the overall corporate governance exercised in any organization. Organizations should, therefore, demonstrate compliance with IT-related regulations and internally adopted standards and policies. This article focuses on regulatory compliance.

Countries have shown that they recognize the need for legally enforceable guidelines for the acceptable use of IT. Legislation which addresses these issues, such as the Electronic Communications and Transactions Act [26], the Electronic Communications Act [28] and the USA PATRIOT Act [30] has, therefore, come into existence.

All organizations are, consequently, obliged to be aware of applicable national, international and/or sector-specific regulations relating to the use of IT, and to comply with these regulations.

Cloud computing is a relatively new way of computing that has generated a lot of interest. There are, however, concerns with regard to compliance associated with cloud computing. The next section discusses these concerns.

IV. Cloud Computing and Compliance

Fundamentally, cloud computing has to do with the provisioning of services, platforms and fundamental computing resources (infrastructure) as services over the Internet. Cloud computing can be simply explained by using a utility analogy [6, 18, 19]. Organizations may make use of a resource, such as electricity, from a utility company without much consideration for how the electricity was produced, or where it comes from. Likewise, cloud computing makes it possible for companies to access various IT resources and services from a service provider with only a vague idea of where the resources are, and how they work.

Potential benefits that can be derived from cloud computing, such as increased flexibility and scalability, greener computing, and support for more business innovation, are enticing [2, 21]. Cost reduction is another potential benefit that causes many organizations to be interested in the cloud. Already organizations are making use of various cloud solutions.

A study conducted by Chung and Hermans [5] explains that “The view of a vast majority of decision- makers, is that cloud computing is the future model of IT, and it is definitely not a hype that will subside.” In addition, the study found that a significant percentage (58 percent) of the participating organizations are already using cloud-computing services, or are expecting to adopt cloud computing within the next 12 months.

Cloud computing is being adopted, despite concerns with regard to issues related to compliance in the cloud. Quotes highlighting the concerns of various authors in this regard are shown in Table 1. As can be seen from these quotes, there is often confusion about how existing legislature affects cloud-computing solutions.

One reason why ensuring compliance may be more challenging with cloud computing, is the fact that organizations remain responsible for their own information, regardless of where the information is kept. Organizations with highly controlled environments may feel more confident about ensuring compliance when they have direct control over their information and systems.

When organizations move to a public or hybrid cloud, however, they are likely to lose some measure of control. Information may no longer reside on servers owned and managed by the organization, but by a cloud-service provider that may have a different business model, may be in a different country, and may operate under different laws and regulations.

- “Compliance with regulatory policies on data remains a key hurdle to cloud computing” [14].
- “Continental also determined that compliance is the greatest barrier to moving IT services to the cloud” [17].
- “Courts will need to determine how existing laws may or may not protect electronic communications and content in this new computing model” [23].
- “Despite the growing popularity of cloud computing services, there appears to be little opportunity for judicial or legislative relief in the near future” [23].
- “Whatever regulatory environment is targeted, cloud-based compliance is nearly always a nontrivial task” [32].
- “Cloud computing has ‘unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing,” says Gartner [3].
- “As cloud computing becomes more widely used by individuals and businesses alike and is increasingly viewed as a cheap, convenient, and viable alternative to the traditional desktop-computer platform, the law is unfortunately still trailing behind the development of new technology” [13].

Research has been done concerning applying certain American regulations, such as the Stored Communications Act (SCA) and the Electronic Communications Privacy Act (ECPA) [29] to cloud-computing solutions. Researchers have concluded that “The business model embraced by many cloud-computing providers is incompatible with the requirements of the Stored Communications Act” [23].

It has also been concluded that “there is a great deal of uncertainty in how laws enacted in the mid-80s, such as the ECPA, would apply to cloud computing” [13]. Lanois [13] also reports that countries outside the United States refer to the USA Patriot Act, which gives the USA government the right to demand data, as a hurdle to the international adoption of cloud computing. For lands of the European Union, it is also necessary to take specific measures when adopting cloud computing, to ensure compliance with the EU Data Protection Directive [13]. It is, therefore, clear that regulatory compliance may be a challenge, when adopting some cloud- computing solutions in America and European countries.

There are a multitude of cloud-computing options and solutions; and these may each have different requirements for regulatory compliance. Cloud computing is a very broad term. There are various deployment models and various deployment models that are considered to be cloud-computing solutions [20]. Organizations may use any of many types of software provisioned as a service, deployed on either a public, private or community cloud.

Any of these would be a cloud-computing solution. In addition, organizations may also use Platform as a Service or Infrastructure as a Service. Service models deployed on any cloud deployment model could still be using a cloud-computing solution.

It is easy to see that there is a vast range of cloud-computing solutions which vary in complexity and business importance that can be used. Therefore, organizations need to consider regulatory compliance requirements for each of these potential solutions.

From the above, it is clear that the requirements for regulatory compliance to which organizations would have to adhere, would vary – depending on the regulations specific to the country or countries in which the organization is operating, and the type of cloud-computing solution being used.

All organizations, should however, follow a process to ensure that they will be able to benefit from cloud computing in a compliant manner, before making a decision regarding the adoption of a cloud service. Taking all of the above-mentioned into account, this paper will describe a set of guidelines that have been successfully utilized by a South African university in the process of deciding to move parts of their email service to the cloud.

Before the guidelines are described though, the importance of compliance in the area of company email will be briefly highlighted below.

V. The importance of email compliance

Email is a necessary part of many organizations. As stated by Schadler [25], "email is an entitlement, as ubiquitous and expected as an office chair." This is clearly shown in a report by Radicati [27], which predicts that the number of email users will grow from 1.4 billion users in 2009 to 1.9 billion in 2013. In addition, the report predicts that email traffic will increase from 247 billion messages per day in 2009 to 507 billion messages per day in 2013.

Email is expected to become more pervasive, and to play an ever-increasing role in both the personal and professional lives of employees [1, 22, 25]. It is fair to conclude that, as email loads increase, organizations will become more dependent on this means of communication.

Email is, however, not merely a convenient form of communication on which organizations are dependent. Emails are electronic records for which organizations may have legal responsibilities regarding the retention, destruction and restoration of stored information [15].

There is much work and considerable cost involved in maintaining an in-house email solution [25]. A Forrester report has revealed that firms commonly underestimate the full cost of email [25]. It is not surprising then, that many companies contemplate cloud-based email solutions with their associated potential advantage of lower costs [16].

The idea of email as a service is not new [8, 25]. Email-as-a-Service or cloud-based email is one of the cloud services that some foresee will have a marked impact on organizations [1, 7]. In a recent survey by Forrester Research, 49% of 53 large enterprises who responded to the survey were busy evaluating an alternative option for managing and providing email [31].

This research also asserts that "there aren't many scenarios where an organization could not benefit from hosting some of its email services in the cloud" [31]. According to Schadler [25], for mid-size companies, cloud-based email is often cheaper than an in-house email solution. There are other benefits associated with cloud-based email, such as the ability to rapidly provision users and to assign IT professionals to other business problems [25].

As alluring as cloud-based email may be, organizations still have the responsibility to ensure that email is governed and secured properly, and in such a way that compliance is demonstrated. As mentioned earlier, cloud-based email solutions may decrease the level of control organizations have over their email. It does not, however, decrease the responsibility [18].

It is, therefore, imperative that cloud-based email solutions should be properly governed, in order to ensure compliance.

A detailed discussion of all the regulations pertaining to email for companies in South Africa is beyond the scope of this work. The following section, however, highlights a general process and a set of guidelines that all companies can follow to assist them in addressing compliance, when moving to a cloud-based service.

VI. Guidelines for cloud-computing service adoption

Following the extensive review of the relevant literature and interviews with legal and IT experts, it is possible to deduce the following set of guidelines that could be used to assist in the compliant adoption of cloud-computing services. These guidelines can be summarized into five main phases. Organizations should: 1) Identify cloud-computing services that have real potential benefit for the organization; 2) identify the legal risks related to these services; 3) if possible, negotiate a contract that will allow the organization to demonstrate compliance; 4) if possible, adjust organizational policies and/or procedures to benefit from the service; and 5) identify alternate solutions if compliance is not possible with the identified cloud-computing services.

A South African university (for the sake of brevity hereafter referred to simply as: the University), which provides each of about 25000 students with the necessary IT services, such as email, has been used as a case study to verify the usefulness and validity of the guidelines. According to the University policy, email is an official means of internal communication. In late 2008, the university decided to provide all students with email, using Live@edu. Staff emails are, however, still provided by the University directly.

The decision to provide email in this way was based on various factors. This paper, however, describes how the need to demonstrate legal compliance motivated the decision to use the guidelines above when planning the adoption of cloud-based email.

The following five sub-headings describe the guidelines for compliant adoption of cloud-computing services. In each sub-heading the manner in which the University applied the guideline is also explained.

A. *Identify service benefits*

IT should always be used in a manner that benefits an organization. It would be unwise to invest in a service that does not add value to an organization in some way. Cloud computing, in general, has a number of benefits commonly associated with it. These include cost reductions, more business flexibility and greener computing. The extent that an organization would be able to realize these benefits would obviously depend on various factors. The first step, therefore, is to identify what benefits an organization would expect to receive when adopting a cloud-computing service. The organization would have to determine whether these benefits are likely to be achieved, whether they are worth whatever expense and effort would be involved with the change to using a cloud-computing service, and how they plan on measuring the anticipated benefits.

An immense incentive for using Live@edu to provide email at universities is that Microsoft provides this service for free. Cost reduction is, therefore, definitely a benefit that universities would derive by moving their email to the cloud. There are additional benefits associated with using Live@edu. With Live@edu, users have access to 10 GB inboxes, as compared with the 20 MB inboxes that the University could offer users previously.

Besides offering a free email service Live@edu, provides access to other services for free. These include access to instant-messaging services and the ability to store 25 GB of data online. It is, therefore, clear that there are very significant benefits that the University would achieve by using the Live@edu set of cloud-computing services. In fact, it could be said that the University would be remiss if it did not investigate this propitious solution. Even potential solutions with such tremendous benefits, however, cannot be adopted without considering the legal risks associated with them.

B. Identify legal risks

The law, together with the principles of good governance and ethical considerations all mandate that the legal risks associated with an opportunity are identified and given appropriate consideration. To identify legal risks, organizations might firstly need to identify the pertinent regulations, and investigate these to determine the legal requirements associated with the service. Identified legal requirements can then be compared with how the cloud service providers (CSPs) implement the service to deal with these legal risks. These steps are expounded and made clearer below, by explaining how they have been applied at the University.

1) Identify the legal and regulatory environment

There are several South African laws, which have a bearing on email management in South Africa. These include the Electronic Communications and Transactions Act (ECT), 2002, the Companies Act, 2008, and the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA), 2002, as amended [9].

Giles [9] and Lisa Thornton Inc. [15] highlight various topics of email law. Some of these are summarized below.

- Interception of emails – The RICA and the ECT Act explain when it is lawful and when it is not to intercept emails. Interception of email is, in some cases, required to facilitate the appropriate retention and production of emails.
- Agreements made using email – legally binding agreements can be concluded using email.
- Personal information and email – the Protection of Personal Information Bill requires that personal information be protected. Email addresses are personal information.
- Email as evidence – emails may be used as evidence if the integrity and reliability of the email can be demonstrated.
- Retention of email – the law may require the retention of certain emails. These should be retained, in such a manner, that the integrity of the email may be ensured.

Once an organization is aware of the specific legal requirements that are applicable to the service under consideration, they would then be able to identify the legal risks, by investigating how the potential service is provided by a CSP, and what service level agreement (SLA) the CSP makes available.

2) Determine how the service is provisioned

Based on the legal requirements identified in the previous step, organizations are now able to gather information about how the service is provided by a CSP, in order to determine whether the information is handled in a manner which enables them to demonstrate compliance or not. The information they may need to consider may include, for example, what security measures the CSP have in place. Where will the organization's information be held by the CSP? How long will the CSP hold the information for? Who do they share it with; and how is information destroyed? What type of SLA does the CSP provide?

Live@edu provides universities with a level of control over the email service provisioned by Microsoft. University administrators retain the ability to create and delete accounts via a management interface. University administrators are also able to access reports, such as: service usage and summaries of messages sent, received and failed for the university's domains. In addition, university administrators can carry out searches across multiple mailboxes; they can control who can send emails to specific users; and they can filter emails to users. This is very beneficial, taking into account that messages are stored in data centres around the world.

In completing the above-mentioned steps, the University identified the following potential legal risks:

- There was uncertainty about compliance with laws for the legal retention of emails.
- There was concern about whether emails will have due evidentiary weight in the case where such an email has to be used in an investigation, if the service is provisioned in the cloud.
- There were concerns about how international laws would affect the way the university's information would be able to be accessed.
- Concerns about liability were also highlighted. If email is "hosted" in the cloud, the underlying agreement had to be thoroughly checked, so that problems that could arise would not cause liability on the part of the university.

As shown above, a comparison between legal requirements and the answers to questions about service provisioning by the CSP would help organizations to identify legal risks. Organizations then have the task of attempting to mitigate these risks.

C. Get contract in place

Once an organization has determined, which legal risks would need to be addressed, before outsourcing a service to a CSP, the organization may be able to mitigate some of these risks by negotiating a contract with the CSP. This contract may be able to demonstrate how the organization and CSP would be able to agree to a way of provisioning the service in a manner, which would allow the organization to demonstrate compliance. CSPs may not be willing to negotiate contracts with individual organizations, though. Legal risks may, in such a case, still be mitigated by adjusting the organization's policies, procedures and technical controls, however.

The University chose not to negotiate a contract with Microsoft for the provisioning of their email. They were willing to accept the standard contract provided by Microsoft for the provisioning of students' email. The legal risks identified in the previous step would apply primarily to communication between staff or between university administration and students.

The University, therefore, decided to mitigate these risks by using the following two steps: steps D and E below.

D. Adjust policies and procedures

If organizations are not able to mitigate legal risks to an acceptable level, they would have to find another way of getting the service they want. The solution may be to improve IT services within the organization. Using a hybrid cloud-deployment model could also enable organizations to benefit from some of the benefits associated with cloud computing, while avoiding certain legal risks.

The University chose not to use cloud-based email for all university email. Instead, they chose to use cloud-based email for students, and keep using an in-house solution for the staff. This not only mitigated the legal risks, which were a concern for them, it also provided the university with a chance to evaluate the cloud-based solution with a subset of their users.

E. Reject service where necessary

Organizations may be able to change their policies and procedures to mitigate the legal risks associated with using cloud-based services. They may, for example, adjust how they manipulate information before it is given to a CSP.

In the case of the University, policies where adjusted as follows:

- The ICT core SLA was adjusted to indicate that the availability of email would be: 'As per Service Providers (Live@edu)' for all students.
- All emails to or from students for staff members are retained on internal email servers. As stated earlier, the University has chosen not to outsource staff email. Email sent by staff is therefore, retained on internal email servers. In like manner, emails sent by students to staff are also retained internally. In this way, the matter of important business emails is addressed. There is still, however, the question of whether the University should take vicarious responsibility for emails from students to other parties – for which there would be no record on the university systems.

Although this paper focuses particularly on regulatory compliance, it is worth noting here that the step of adjusting internal policies and procedures, before adopting a cloud-based service, may be essential to ensuring that the company shows internal compliance. Organizations should carefully assess their contracts, to ensure that any legal liability is minimized.

By following the above-mentioned process, organizations should be able to identify and mitigate the legal risks associated with the adoption of cloud-computing services. Although the steps outlined are intuitive and simple, it is advisable to consult with legal experts during this process. IT experts and other staff who have not been trained in the law, may be ill equipped to be able to draw up legally binding contracts and to be able to apply the law in context. By following this process though, business and IT management are able to show that they have demonstrated due diligence, which is important from a modern IT-governance perspective.

Lastly, it is important to note that the guidelines described here are to be used repetitively. It is essential that organizations continue to investigate the opportunities that become available as laws and technologies, since services change and mature.

VII. CONCLUSION

Ensuring IT compliance with legal and regulatory measures is an essential part of ensuring that an organization is well governed. All organizations are required by the law, principles of good governance and principles of ethical behaviour, to take due care in demonstrating regulatory compliance. A set of guidelines that can assist managers in doing this has been concluded and described. The guidelines have proved to be of value in a real-world example of a South African university, which has applied them in the process of deciding whether and how to implement a cloud-based email service. It is believed that these guidelines could be applied in similar instances, where organizations are investigating the use of cloud-computing services.

VIII. REFERENCES

[1] Bauer, P. (2010, January 26). *Email as a Service.* Retrieved March 2, 2010, from CRN: http://www.channelweb.co.uk/articles/print/2256798

[2] Breeding, M. (2009, November/December). The Advance of Computing From the Ground to the Cloud. *Computers in Libraries'*, 22 - 25.

[3] Brodkin, J. (2008, July 2). *Gartner: Seven cloud-computing security risks*. Retrieved June 30, 2010, from Network World: http://www.networkworld.com/news/2008/070208-cloud.html

[4] Collins English dictionary and Thesaurus essential edition. (2007). UK: harpercollins Publisher.

[5] Chung, M., & Hermans, J. (2010). *KPMG's 2010 Cloud Computing Survey.* Netherlands: KPMG.

[6] CSA. (2009). *Cloud Security Alliance*. Retrieved Febuary 8, 2010, from http://www.cloudsecurityalliance.org/

[7] Geer, D. (2008, September 5). Cloud-based Email: Developing technology offers sunny skies to SME IT departments. *Processor, 30(36),* 23. USA: Sandhills Publishing Company.

[8] Georgia, B. L. (2000, April). Drop your e-mail (on someone else). *PC Computing*, pp. 117-122.

[9] Giles, J. (2009, August 14). *Email compliance: email law in South Africa*. Retrieved November 4, 2010, from Michalsons: http://www.michalsons.com/email-compliance-email-law-in-south-africa/print/

[10] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information System Research. *MIS Quaterly, 28*(1), 75-105.

[11] ISACA. (2009). Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives. Rolling Meadows, IL, USA.

[12] ISO/IEC 38500:2008. (n.d.). Coporate governance of information technology. ISO/IEC.

[13] Lanois, P. (2010, November). Caught in the clouds: the web 2.0, cloud computing, and privacy. *Northwestern Journal of Technology and Intellectual Property, 9*(2), 27-49.

[14] Li, J., Singhal, S., Swaminathan, R., & Karp, A. H. (2010). Managing data retention policies at scale. *IFIP/IEEE International Symposium on Integrated Network Management 2011*. Dublin.

[15] Lisa Thornton Inc. (2005). *Guide to achieving Email compliance - a South African perspective.* Retrieved February 21, 2011, from Lisa Thornton Inc: http://thornton.co.za/resources/Email%20Compliance%20-%20a%20South%20African%20perspective.pdf

[16] Liveoffice. (2009). *Cloud Email 101. Cloud Email Buyer's Guide.* Retrieved June 10, 2010, from Cloud Email 101: http://www.cloudemail101.org/home

[17] Loebbecke, C., Thomas, B., & Ullrich, T. (2012). Assessing Cloud readiness at Continental AG. *MIS Quaterly Executive, 11*(1), 11-23.

[18] Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy* (First Edition ed.). (M. Loukides, Ed.) Sebastopol, CA, USA: O'Reilly Media Inc.

[19] Mell, P., & Grance, T. (2009, July 10). *The NIST Definition of Cloud Computing.* Retrieved January 29, 2010, from http://csrc.nist.gov/groups/SNS/cloud-computing/

[20] NIST. (2009, May 11). *Cloud Computing*. Retrieved April 13, 2010, from Computer Security Division: Computer Security Resource Centre: http://csrc.nist.gov/groups/SNS/cloud-computing/

[21] Porta, M., Karimi, A., Plakskon, J., & Sharma, D. (2009, September). Capturing the Potential of Cloud. New York, USA: IBM Corporation.

[22] Ranger, S. (2008, August). Behind the Cloud. *Director*, pp. 50-52.

[23] Robison, W. J. (2010). Free at what cost?: cloud computing privacy under the stored communications act. *The Georgetown Law Journal, 98*, 1195-1239.

[24] Sanborn, S., & Kujubu, L. (1999, August 16). Outsourced e-mail options growing for IT. *Inoworld*. USA: Infoworld.

[25] Schadler, T. (2009). *Should your Email live in the cloud? A comparative cost analysis.* Forrester. Cambridge: Forrester Research, Inc.

[26] South Africa. (2002). Electronic Communications and Transactions Act.

[27] The Radicati Group, Inc. (2009, May 6). *The Radicati Group, Inc. Releases "Email Statistics Report, 2009-2013".* Retrieved August 7, 2010, from Radicati.com: http://www.radicati.com/wp/wp-content/uploads/2009/05/e-mail-statistics-report-2009-pr.pdf

[28] UK. (2000). Electronic Communications Act.

[29] USA. (1986). Electronic Communications Privacy Act.

[30] USA. (2001). USA PATRIOT Act.

[31] Voce, C., Schadler, T., Echols, B., & Burnes, S. (2009, January 5). Should your email live in the cloud? An infrastructure and operations analysis. Cambridge, USA: Forrester.

[32] Wood, L. (2009, January 30). *Cloud computing and compliance: Be careful up there*. Retrieved June 2, 2010, from infoworld: http://www.infoworld.com/d/security-central/cloud-computing-and-compliance-be-careful-there-639

Melanie Viljoen has received her Master’s in Information Technology from the Nelson Mandela Metropolitan University. She is currently studying towards her PHD at the same university.

Prof. Rossouw von Solms holds a PhD-degree from the ex-Rand Afrikaans University. He has been the Head of Department of the Information Technology at the ex-PE Technikon and the Nelson Mandela Metropolitan University for more than fifteen years. Currently, Rossouw is the Director of the Institute for ICT Advancement at the NMMU. Rossouw has published and presented more than one hundred academic papers in journals and conferences, both internationally and nationally. Most of these papers were published and presented in the field of Information Security. He has supervised more than forty M & D students successfully. Rossouw is an executive member of Technical Committee 11 (responsible for information protection) of the International Federation for Information Processing (IFIP). He is also a member of the South African Computer Society. Rossouw is also currently the immediate past-President of the South African Institute for Computer Scientists and Information Technologists (SAICSIT). He is also a Certified Information Security Manager (CISM).

Prof. Vivienne Lawack-Davids is Executive Dean of the Faculty of Law at the Nelson Mandela Metropolitan University. She holds a BJuris LLB

LLD (UPE) LLD (Unisa). Her research fields are payments law, electronic banking law, IT law and consumer protection law.

Acknowledgements:

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 NRF.