A FRAMEWORK FOR ASSURING CONFORMANCE OF CLOUD-BASED EMAIL AT HIGHER EDUCATION INSTITUTIONS

By

Melanie Willett

(nee Viljoen)

December 2013

A Framework for Assuring Conformance of Cloud-based Email at Higher Education Institutions

by

Melanie Willett

(nee Viljoen)

Thesis

Submitted in fulfillment of the requirements of the degree

Philosophiae Doctor

In

Information Technology

in the

Faculty of Engineering, the Built Environment and

Information Technology

of the

Nelson Mandela Metropolitan University

Promoter: Prof Rossouw von Solms

December 2013

Declaration

I, Melanie Willett (20310694), hereby declare that the thesis for the degree PhD: Information Technology is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

Melanie Willett

Abstract

Cloud computing is a relatively immature computing paradigm that could significantly benefit users. Cloud computing solutions are often associated with potential benefits such as cost reduction, less administrative hassle, flexibility and scalability. For organisations to realize such potential benefits, cloud computing solutions need to be chosen, implemented, managed and governed in a way that is secure, compliant with internal and external requirements and indicative of due diligence. This can be a challenge, given the many concerns and risks commonly associated with cloud computing solutions.

One cloud computing solution that is being widely adopted around the world is cloud-based email. One of the foremost adopters of this cloud computing solution is higher education institutions. These higher education institutions stand to benefit greatly from using such services. Cloud-based email can be provisioned to staff and students at these institutions for free. Additionally, cloud service providers (CSPs) are able to provide a better email service than some higher education institutions would be able to provide if they were required to do so in-house. CSPs often provide larger inboxes and many extra services with cloud-based email. Cloud-based email is, therefore, clearly an example of a cloud computing solution that has the potential to benefit organisations. There are however, risks and challenges associated with the use of this cloud computing solution. Two of these challenges relate to ensuring conformance to internal and external (legal, regulatory and contractual obligations) requirements and to providing a mechanism of assuring that cloud-based email related activities are sound. The lack of structured guidelines for assuring the conformance of cloud-based email is putting this service at risk at higher education institutions in South Africa.

This work addresses this problem by promoting a best practice based approach to assuring the conformance of cloud-based email at higher education institutions. To accomplish this, components of applicable standards and best practice guidelines for IT governance, IT assurance and IT conformance are used to construct a framework for assuring the conformance of cloud-based email. The framework is designed and verified using sound design science principles. The utility and value of the framework has been demonstrated at a higher education institution in South Africa. This framework can be used to assist higher education institutions to demonstrate due diligence in assuring that they conform to legal and

best practice requirements for the management and governance of cloud-based email. This is a significant contribution in the relatively new field of cloud computing governance.

Acknowledgments

I owe my sincerest gratitude to many people including the following:

- My supervisor, Prof Rossouw Von Solms, for his support and guidance with this work and throughout my postgraduate career. Thank you for your help and motivation.

- My husband, Sebastian Willett, who has been a constant support and encouragement. Thank you for all your help, understanding and encouragement.

- My father, Stephen Viljoen, for his constant help and encouragement. Thank you for always inspiring me to do my best and for teaching me to love learning dad.

- My brother, sister and gran for their support and love. Thank you for always being ready to listen and give needed pep talks Lau.

- The staff who assisted with the demonstration of my framework. Thank you for your giving of your time and for your support and very helpful feedback and input.

- The staff at the EBEIT faculty at the NMMU for all your help throughout my studies there. A special thanks to Annette, Cheryl and Lynn for all your help and support during the difficult times during the completion of this work.

- The financial assistance of the National Research Foundation (NRF) and the Nelson Mandela Metropolitan University (NMMU) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the NRF or NMMU.

- Lastly, although I cannot thank her now, I owe my deep gratitude to my mother, Barabara Viljoen. It would be amiss not to acknowledge her contribution to this work. My mom has always been one of the greatest sources of motivation, encouragement and support in my life. She has always taken a keen interest in my education and been willing to do anything to help her children succeed in all aspects of life. She is sorely missed.

Table of Contents

DECLARATION I

ABSTRACT II

ACKNOWLEDGMENTS IV

TABLE OF CONTENTS V

LIST OF FIGURES VIII

LIST OF TABLES X

CHAPTER 1 1

INTRODUCTION 1

1.1 Background 1

1.2 Areas of Interest 1

1.3 Problem Statement 12

1.4 Research Questions 13

1.5 Research Objectives 14

1.6 Delineation and Limitations 14

1.7 Research Design 14

1.8 List of Chapters 16

CHAPTER 2 18

RESEARCH METHODOLOGY 18

2.1 Introduction 18

2.2 Research Design 18

2.3 Research Methodology 19

2.4 Research Methods 24

2.5 Conclusion 25

CHAPTER 3 26

IT GOVERNANCE, CONFORMANCE & ASSURANCE 26

3.1 Introduction 26

3.2 IT Governance 26

3.3 Conformance 33

3.4 Assurance 37

3.5 Assuring IT Conformance from a Governance Perspective 42

3.6 Conclusion 45

CHAPTER 4 46

CLOUD COMPUTING 46

4.1 Introduction 46

4.2 Cloud Computing Explained 46

4.3 Cloud Computing Impact *56*
4.4 Cloud Computing Benefits *58*
4.5 Cloud Computing Challenges *60*
4.6 Cloud Computing Guidelines *63*
4.7 Assuring Compliance in Cloud Computing *74*
4.8 Conclusion *75*

CHAPTER 5 ..... **76**

CLOUD-BASED EMAIL AT HIGHER EDUCATION INSTITUTIONS 76
5.1 Introduction *76*
5.2 Cloud-based Email *77*
5.3 Cloud-based Email for Higher Education *80*
5.4 Conclusion *91*

CHAPTER 6 ..... **93**

A FRAMEWORK FOR ASSURING THE CONFORMANCE OF CLOUD-BASED EMAIL 93
6.1 Introduction *93*
6.2 FACCE, A Conceptual Framework *94*
6.3 Design and Development of the FACCE *95*
6.4 Value of the FACCE *110*
6.5 Conclusion *111*

CHAPTER 7 ..... **113**

FACCE VERIFICATION 113
7.1 Introduction *113*
7.2 FACCE Demonstration *113*
7.3 FACCE Evaluation *123*
7.4 Conclusions *133*

CHAPTER 8 ..... **134**

CONCLUSION 134
8.1 Introduction *134*
8.2 Research Objectives *134*
8.3 Research Contributions *140*
8.4 Limitations and Further Research *142*
8.5 Epilogue *144*

REFERENCES **145**

APPENDIX A: FACCE DETAILED GUIDELINES AND DEMONSTRATION INFORMATION 164
Appendix A1 ..... *165*
Appendix A2 ..... *174*
Appendix A3 ..... *186*

Appendix A4 ..... *188*
Appendix A5 ..... *196*
Appendix A6 ..... *196*
APPENDIX B: PUBLICATIONS 197
Appendix B1 ..... *198*
Appendix B2 ..... *215*
Appendix B3 ..... *223*
Appendix B4 ..... *243*
Appendix B5 ..... *268*
APPENDIX C: QUESTIONNAIRES 276
Appendix C1 ..... *277*
Appendix C2 ..... *278*

List of Figures

FIGURE 1.1 CLOUD-BASED EMAIL ADOPTION IN SOUTH AFRICAN UNIVERSITIES....8
FIGURE 1.2 AREAS OF CONCERN FOR CLOUD-BASED EMAIL....11
FIGURE 1.3 NEED FOR CLOUD-BASED EMAIL GUIDELINES....12
FIGURE 1.4 CHAPTER LAYOUT....17
FIGURE 2.1 THE DESIGN SCIENCE RESEARCH METHODOLOGY ADAPTED FROM PEFFERS, TUUNAMEN, ROTHERBERGER & CHATTERJEE....20
FIGURE 2.2 OVERVIEW OF RESEARCH DESIGN FOR THIS WORK....43
FIGURE 3.1 ADAPTED FROM ISO/IEC 38500:2008 MODEL FOR IT GOVERNANCE....31
FIGURE 3.2 COBIT 5'S PROCESS FOR IT GOVERNANCE AND MANAGEMENT (ISACA, 2010B)....32
FIGURE 3.3 MODEL FOR COMPLIANCE AS DESCRIBED BY RAEZ, WEIPPL & SEURF (2010)....36
FIGURE 3.4 THE COMPONENTS AND RELATIONSHIPS NECESSARY FOR ASSURANCE....40
FIGURE 3.5 ISACA'S DEPICTION OF ASSURANCE COMPONENTS (ISACA, 2013)....41
FIGURE 3.6 THE BENEFITS OF A BEST PRACTICE BASED APPROACH FOR ASSURING CONFORMANCE FROM AN IT GOVERNANCE PERSPECTIVE....43
FIGURE 4.1 CSA'S VISUAL REPRESENTATION OF NIST'S CLOUD COMPUTING DEFINITION (CLOUD SECURITY ALLIANCE, 2009B)....49
FIGURE 4.2 EXAMPLE OF A HYBRID CLOUD COMPUTING DEPLOYMENT MODEL (LIU, ET AL., 2011)....52
FIGURE 4.3 LEVEL OF CONTROL AFFECTED BY SERVICE MODEL (ENISA, 2009A)....54
FIGURE 4.4 EFFECTS OF CLOUD COMPUTING DEPLOYMENT MODEL (ENISA, 2009A)....54
FIGURE 4.5 CLOUD COMPUTING HIGH-LEVEL REFERENCE ARCHITECTURE (LIU, ET AL., 2011)....55
FIGURE 4.6 GOOGLE TREND RESULTS FOR CLOUD COMPUTING SEARCHES SINCE 2007....56
FIGURE 4.7 CLOUD COMPUTING MARKET MATURITY (ISACA & CSA, 2012)....59
FIGURE 4.8 DECISION FRAMEWORK (KUNDRA, 2011)....71
FIGURE 5.1 FOCUS AREA OF CHAPTER....77
FIGURE 5.2 CLOUD-BASED EMAIL ADOPTION IN SOUTH AFRICAN HIGHER EDUCATION INSTITUTIONS IN 2012....82
FIGURE 5.3 CLOUD-BASED EMAIL PROVIDERS PREFERRED BY SOUTH AFRICAN HIGHER EDUCATION INSTITUTIONS....83
FIGURE 5.4 HIGHER EDUCATION INSTITUTIONS CLOUD-BASED EMAIL CONCERNS....86
FIGURE 6.1 DESIGN SCIENCE RESEARCH METHODOLOGY USED FOR FACCE....93
FIGURE 6.2 THE THREE STAGES USED TO DESCRIBE THE FACCE....96
FIGURE 6.3 CONCEPT DIAGRAM ILLUSTRATING AN ASSURANCE ENGAGEMENT....97
FIGURE 6.4 ADAPTED FROM ISO/IEC 38500:2008'S MODEL FOR IT GOVERNANCE....99
FIGURE 6.5 SEVEN ENABLERS DEFINED IN COBIT 5 (ISACA, 2010B)....101
FIGURE 6.6 THE GOVERNANCE AND MANAGEMENT PROCESSES THAT FORM PART OF COBIT 5 (ISACA, 2010B)....102
FIGURE 6.7 A FRAMEWORK FOR ASSURING THE CONFORMANCE OF CLOUD-BASED EMAIL (FACCE)....104
FIGURE 7.1 CHAPTER IN RELATION TO THE ACTIVITIES FOR THE DSRM....114

FIGURE 7.2 SAMPLE REPORT BY FACCE PROTOTYPE TOOL 119
FIGURE 7.3 SECOND SAMPLE REPORT OF GUIDELINES RELATED TO CLOUD-BASED EMAIL ACTIVITIES.....120

List of Tables

TABLE 1-1 ISO/IEC 38500:2008 PRINCIPLE OF CONFORMANCE 6
TABLE 1-2 GOVERNANCE AND CLOUD COMPUTING QUOTES 10
TABLE 1-3 PRIMARY RESEARCH QUESTION AND OBJECTIVE 14
TABLE 1-4 SECONDARY RESEARCH QUESTIONS AND OBJECTIVES 15
TABLE 4-1 CLOUD COMPUTING DEFINITIONS 47
TABLE 4-2 MINIMUM PAAS SOLUTION REQUIREMENTS 50
TABLE 6-1 ISO/IEC 38500:2008 PRINCIPLES OF IT GOVERNANCE 98
TABLE 7-1 FACCE GUIDING LIST OF SAMPLE HIGH-LEVEL CRITERIA 116
TABLE 7-4 FACCE EVALUATION IN TERMS OF STRATEGIC FRAMEWORK FOR EVALUATION IN DESIGN SCIENCE (PRIES-HEJE, BASKERVILLE & VENABLE, 2008) 124
TABLE 7-5 SUMMARY OF FEEDBACK FROM FIVE OTHER EVALUATORS 130

CHAPTER 1
Introduction

To be able to effectively solve a problem, it is useful and arguably essential to understand the problem and the objectives of your solution. This chapter introduces the remainder of this work by introducing the problem to be addressed and the objectives of this research. It also describes the delineation and limitations of this work. Additionally, it provides an overview of the structure and content of the remainder of the work by providing a brief description of the remaining chapters. Before highlighting the problem to be addressed by this work, though, the chapter provides background information into the problem by introducing the subjects that inform this work.

1.1 Background

Email has become a crucial technology in the dissemination and storage of business information today (Schadler, 2009a). As information is a vital business asset, it is imperative that email is properly governed to ensure that email-related risk and conformance issues are dealt with in a manner that demonstrates due diligence. Outsourced email as a service in a cloud computing[1] environment introduces additional potential risks to an organisation's email.

The section below provides some background into the concepts of cloud-based email and the important field of governance. The problem to be addressed by this work and the approach to solving the problem is then explained.

1.2 Areas of Interest

As the topic of this work, "*A framework for assuring the conformance of cloud-based email at higher education institutions"*, suggests, this research addresses the fields of cloud-based email and the conformance and assurance aspects of governance. Both of these areas are

[1] Cloud Computing involves the provisioning of services, platforms and fundamental computing resources (infrastructure) as services over the internet as described in Section 2.1

briefly described in this section. The research has been conducted for the South African higher education environment. This environment is, therefore, also briefly presented. Before describing cloud-based email, the concept of cloud computing is briefly introduced.

1.2.1 Cloud Computing

Cloud computing is a term that is currently generating much discussion. A search on Google for the term "Cloud Computing" on 15 July 2010 yielded about 49,100,000 results. Well-respected bodies such as NIST (NIST, 2009), ISACA (ISACA, 2010a) and ENISA (ENISA, 2010) have created groups that focus on cloud computing. Bodies devoted to cloud computing such as the Cloud Security Alliance (CSA) have also formed. Companies such as Microsoft, Google, Novell, Dell, Cisco, Intel, McAffe, Symantec and many others have become CSA members (Cloud Security Alliance, 2009a). These companies have all, therefore, indicated an interest in cloud computing. There are, however, also several companies that are acting as cloud service providers (CSPs). Mather, Kumaraswamy and Latif (2009, p. 214) list some CSPs, including Amazon, Google, Microsoft, Salesforce.com and Sun. The investment that companies like these are willing to make to enter the cloud market suggests that they believe that cloud computing will have a marked impact on the way organisations do business. What exactly *is* cloud computing, though?

Fundamentally, cloud computing has to do with the provisioning of services, platforms and fundamental computing resources (infrastructure) as services over the Internet (Cloud Security Alliance, 2009b, p. 13; Mather, Kumaraswamy, & Latif, 2009, p. 11; Mell & Grance, 2011). Cloud computing can be simply explicated using a utility analogy (Breeding, 2009; ISACA, 2009, p. 4). Organisations may use a resource, such as electricity from a utility company, without much consideration for how the electricity was produced or where it came from. Likewise, cloud computing makes it possible for companies to access various IT resources and services from a service provider with merely an abstract 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 (Porta, Karimi, Plakskon, & Sharma, 2009, p. 3; Breeding, 2009). Cost reduction is another potential benefit that inspires interest in cloud computing. Already organisations are making use of various cloud computing solutions. One cloud computing solution that is being widely

adopted in institutions of higher education around the world is cloud-based email. The following subsection provides more information about this service.

1.2.1.1 Cloud-based Email

Email is a necessary part of many organisations. As stated by Schadler (2009a, p. 6), "email is an entitlement, as ubiquitous and expected as an office chair." This is clearly shown in a report by the Radicati Group (2009), which projects 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 play an ever-increasing role in both the personal and professional lives of employees (Bauer, 2010; The Economist, 2008; Ranger, 2008; Schadler, 2009a). As email loads increase, organisations become more dependent on this means of communication.

There is much work and costs involved in maintaining an in-house email solution (Schadler, 2009a, pp. 2, 4). A Forrester report has revealed that firms commonly underestimate the full cost of email (Schadler, 2009a, p. 4). It is not surprising then, that many companies contemplate cloud-based email solutions with their associated potential advantage of lower-cost (LiveOffice, 2009).

The idea of email as a service is not new (Sanborn & Kujubu, 1999; Georgia, 2000). Email-as-a-Service or cloud-based email is one of the cloud services that some foresee will have a marked impact on organisations (Bauer, 2010; Geer, 2008). 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 (Voce, Schadler, Echols, & Burnes, 2009, p. 2). This research also asserts that "there aren't many scenarios where an organisation could not benefit from hosting some of its email services in the cloud" (Voce, Schadler, Echols, & Burnes, 2009, p. 7). According to Schadler (2009a, p. 11), 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 (Schadler, 2009a, p. 6).

As alluring as cloud-based email may be, organisations still have the responsibility to ensure that email is governed and secured properly and in such a way that conformance is demonstrated. Cloud-based email solutions may decrease the level of control organisations have over their email, but does not decrease the responsibility of managing and governing

this service (Mather, Kumaraswamy, & Latif, 2009). It is, therefore, imperative that cloud-based email solutions are properly governed to ensure conformance and assurance as both are core to good governance.

1.2.2 Governance

There is little question today about the value of good coporate, IT, financial and and other forms of governance (IoDSA, 2009). The lack of good governance in the past has lead to well-reported upon incidents, such as Enron (Healy & Krishna, 2003), Worldcom (Hancock, 2002) and Parmalat (Gumbel, 2004). Good governance is, therefore, expected from organisations today. The King Report on corporate governance states that "if there is a lack of good corporate governance in a market, capital will leave that market with the click of a mouse" (IoDSA, 2002, p. 9). Similarly, research highlights the benefits of demonstrating good governance in all walks of life, and also in any IT environment (ISO, 2008).

The IT Governance Institute defines IT Governance as follows: "IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives" (ITGI, 2003, p. 10). It is vital that all employees, from board-level down, are aware of and able to carry out their responsibilities. According to ITGI (2003, p. 11), "the purpose of IT governance is to direct IT endeavours, to ensure that IT's performance meets the following objectives:

- Alignment of IT with the enterprise and realisation of the promised benefits
- Use of IT to enable the enterprise by exploiting opportunities and maximising benefits
- Responsible use of IT resources
- Appropriate management of IT-related risks."

South Africa uses the ISO/IEC 38500:2008 standard for the governance of IT as a national standard (ISO, 2008). This standard identifies six principles for good governance that should be applied. The principles are: responsibility, strategy, acquisition, performance, conformance and human behaviour. Each of these principles has been identified as necessary for good IT governance. This work, however, focuses on the principle of conformance.

Conformance and compliance are both terms that are used to describe the adherence to rules and standards (ISO, 2008; Linkous, 2008; Schlarman, 2007). For the remainder of this work, the term conformance will be used to describe this principle of governance. Conformance is explained more fully in the next section.

1.2.2.1 Conformance

IT conformance involves ensuring that an organisation can demonstrate that it has met obligations placed on it by regulatory bodies and internally adopted policies and standards (Linkous, 2008; Schlarman, 2007; ISO, 2008). Ensuring IT conformance is more than a matter of good governance practice. Failure to demonstrate conformance can adversely affect organisations. The consequences of non-conformance may include legal action or audit reports that reflect negatively on the organisation.

An extract of the ISO/IEC 38500:2008 standard with regard to the evaluation, directing and monitoring of conformance in IT governance is given in Table 1-1.

As previously stated, conformance is a key principle of good IT governance. An organisation cannot claim to have achieved good IT or corporate governance if the principle of conformance is not ensured. Since email is an important IT service, it is important to identify regulations and internal policies and standards that affect email conformance.

Another important aspect of governance, assurance, is briefly introduced in the next subsection.

1.2.2.2 Assurance

Assurance is another important aspect of governance. Assurance has to do with ensuring that mechanisms and structures are in place that promote confidence and trust that there are appropriate controls in place to ensure that an organisation conforms to internal and external requirements and that risks are appropriately mitigated (ISACA, 2011). Within the field of IT, it is also important to assure that proper governance and management is taking place.

The lack of trust in cloud computing is seen by many as a main inhibitor of the adoption of cloud computing solutions (Ashford, 2011; Kahn & Malluhi, 2010; Ko, et al., 2011; Pearson, 2013; Rashidi & Movahhedinia, 2012). Since assurance is a governance concept that is linked with providing trust, it can be argued that the field of cloud computing would benefit from mechanisms and guidelines for enhancing assurance.

The conformance principle of IT governance

Evaluate

- Directors should regularly evaluate the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines.
- Directors should regularly evaluate the organisation's internal conformance to its system for Governance of IT.

Direct

- Directors should direct those responsible to establish regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.
- Directors should direct that policies are established and enforced to enable the organisation to meet its internal obligations in its use of IT.
- Directors should direct that IT staff follow relevant guidelines for professional behaviour and development.
- Directors should direct that all actions relating to IT be ethical.

Monitor

- Directors should monitor IT compliance and conformance through appropriate reporting and audit practices, ensuring that reviews are timely, comprehensive, and suitable for the evaluation of the extent of satisfaction of the business.
- Directors should monitor IT activities, including disposal of assets and data, to ensure that environmental, privacy, strategic knowledge management, preservation of organisational memory and other relevant obligations are met.

(ISO, 2008, p. 14)

Table 1-1 ISO/IEC 38500:2008 principle of conformance

1.2.3 South African Higher Education

Information and education are closely related. To educate has been defined as to provide someone with "training in or information on a particular subject" (Oxford Dictionaries, 2010).

The introduction of the South African national education information policy (2004) states in part that "the effective gathering, dissemination and analysis of information in the education system of any country is vital for sound education planning, monitoring and delivery."

It is, therefore, not surprising that IT plays an important role in higher education. Much research has been done regarding the use of ICT in Higher education (Dodds, 2007; Noirid & Srisa-ard, 2007; Zhou & Xie, 2010). One of the strategic objectives in the strategic plan 2009 – 2013 by the former South African Department of Education (2009), which is now referred to as the Department of Higher Education and Training, is to support curriculum implementation through the use of ICT. One of the associated targets is to monitor and report on access to the Internet, electronic communication and the use of ICT for the administration and management of education institutions. The importance of email as a form of electronic communication has already been highlighted.

An interesting trend is the rapid adoption of cloud-based email by higher education institutions. A report by Zoe Corbyn remarks on work published by Gartner about the hype cycle for education (2009). According to the report, cloud-based email has seen a "tremendous uptake" in higher education and is a technology that is "firmly ensconced in the sector." This holds true in South Africa as well. The preceding is highlighted by the responses to a questionaire sent out in 2009 as part of a preliminary research for this study. Nine universities responded to the questionaire, all of whom are either already using cloud-based email or are planning on implementing cloud-based email within the next one or two years. This is shown in Figure 1.1. The data collected through a similar questionnaire sent out in 2012 reinforces the fact that cloud-based email is likely to be used by most higher education institutions in South Africa. This survey found that 94 percent of the sixteen institutions surveyed were either already using or planning on using cloud-based email at their respective institutions. The two surveys (conducted in 2009 and 2012) referred to here are discussed in more detail in Chapter 5.

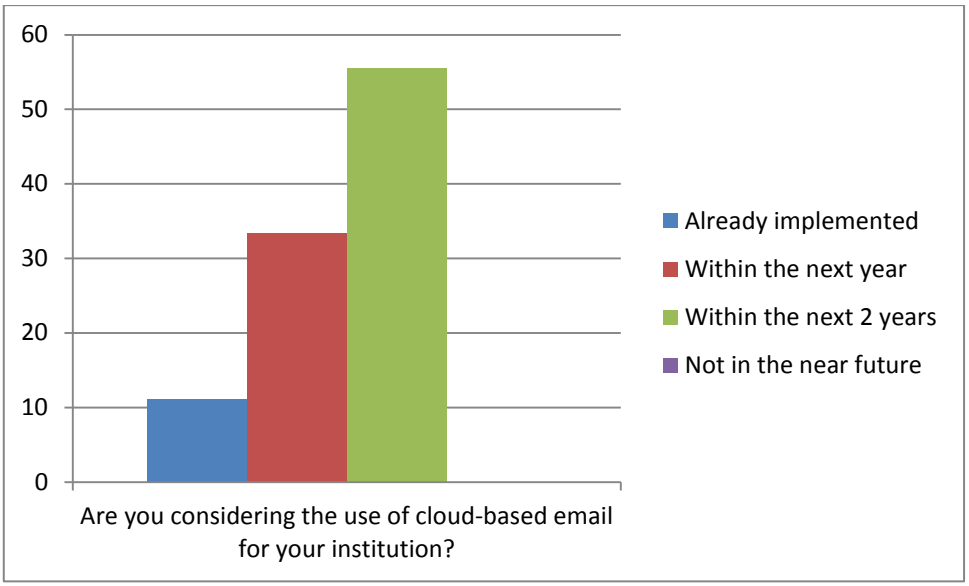


Figure 1.1 Cloud-based email adoption in South African universities

Internationally, universities such as Arizona State University and Bryant University are already using cloud-based email as part of their email solutions (Schadler, 2009b, p. 6).A key reason for the rapid adoption of this technology in higher education institutions may be the fact that some service providers, such as Microsoft (who provided Live@edu, which has now been upgraded to Office365) and Google (Google Apps Education Edition), offer free cloud-based email to universities and other education institutions (Microsoft, 2009; Google, 2009).

As with other organisations, good governance is vital for higher education institutions. In line with this, "support for improved Governance in Higher Education" is another strategic objective of the South African Department of Higher Education and Training (Department of Education, 2009, p. 86).

The following section discusses the areas of interest in the previous sections in relation to one another.

1.2.4 Assuring the conformance of cloud-based email in higher education institutions in South Africa

The preceding areas of interest are integrated in this section; the problem statement for this research will be given in the following section.

Organisations today are not only expected to exercise good governance but benefit from doing so. Two key principles of good governance are conformance and assurance. IT governance is an integral part of good governance. IT governance involves putting in place "the leadership and organisational structures and processes" to ensure that IT resources are used responsibly and securely in a manner that promotes organisational strategy and objectives. Since conformance and assurance are important components of governance, IT governance also involves assuring conformance. It is, consequently, important that an organisation can demonstrate, or provide assurance, that it has used IT resources in a manner that shows that it has met obligations placed on it by regulatory bodies and internally adopted policies and standards. A very important IT service that many organisations are reliant on is email. Governance of email should therefore, be an important part of IT governance. Processes to assure that email is used in a manner that is secure, is compliant and promotes organisational strategy and objectives are, hence, vital. This is true of organisation in general and applies to higher education institutions in South Africa specifically.

Cloud computing is a term which has generated much interest and is expected to affect the way some organisations do business. There are various challenges and risks associated with cloud computing. A risk, in the context of information technology research, can be defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization (ISO, 2004)." There are clear threats relating to the governance, conformance and assurance of cloud computing. Some of these threats are discussed in more detail in Chapter 4 and Chapter 5. Several bodies have been involved in work to identify and explain threats and risks related to cloud computing (Brodkin, 2008; Cloud Security Alliance, 2011; ENISA, 2009a; ISACA, 2012c). Privacy and security concerns with cloud computing are often discussed (Ashford, 2011; Brodkin, 2008; Cloud Security Alliance, 2011). Although these are important areas of concern, there are also critical risks in legal, operational and business areas of cloud computing (Dutta, Peng, & Choudharya, 2013). The CSA has identified thirteen areas of concern for cloud computing and provides guidelines for security in each of these areas (Cloud Security Alliance, 2009b, p. 26). Two areas that this body has identified as areas of concern are 'governance and risk management' and 'compliance and audit.' Moving any system to the cloud often reduces the direct control an organisation has over the system but not the responsibility (Mather, Kumaraswamy, & Latif, 2009). Traditional systems and methods of management and governance may need to be adapted to be effective when using cloud computing (Jackson,

2011; Mircea & Andreescu, 2011; Katz, Goldstein, & Yanosky, 2009). There are also serious concerns regarding legal conformance with cloud computing. There is uncertainty regarding how various international laws and standards will be applied given the geographically distributed nature of cloud computing (Ward & Sipior, 2010). Although cloud computing is being widely and rapidly adopted today, there is a "growing recognition of the substantial risks" associated with cloud computing (Kalyvas, Overly, & Karylyn, 2013a). Given the fact that there are serious vulnerabilities in the areas of governance, conformance and assurance of cloud computing, it can be deduced that failure to address such threats could put the effective use of various cloud computing services, including cloud-based email, at serious risk (Srinivasan, 2011). When moving any system to the cloud, therefore, it is imperative that organisations consider the governance and related conformance and assurance issues involved (Mather, Kumaraswamy, & Latif, 2009; Cloud Security Alliance, 2009b; Computer Weekly, 2009). Table 1-2 lists various quotes highlighting this.

Governance and Cloud Computing
"Business must work with legal, security and assurance professionals to ensure that the appropriate levels of security and privacy are achieved. The cloud is a major change in how computing resources will be utilized, and as such will be a major governance initiative within adopting organisations, requiring involvement of a broad set of stakeholders" (ISACA, 2009, p. 10).
"With Cloud Computing developing as a viable and cost effective means to outsource entire systems or even entire business processes, maintaining compliance with your security policy and the various regulatory and legislative requirements to which your organisation is subject can become more difficult to achieve and even harder to demonstrate to auditors and assessors" (Cloud Security Alliance, 2009b, p.37).
"An organisation's RIM, IT, and legal staff must understand those disadvantages in order to identify possible problems and minimize risks of any SaaS solution that is being considered or has already been implemented. Primarily, they must understand the legal and regulatory environment and risks associated with cloud use" (Gatewood, 2009, p. 34).
"Customers and potential customers of cloud provider services should have regard to their respective national and supra-national obligations for compliance with regulatory frameworks and ensure that any such obligations are appropriately complied with" (ENISA, 2009a, p. 24).

Table 1-1 Governance and cloud computing quotes

Higher education institutions are beginning to use cloud-based email. This trend has been identified internationally and is expected to be true in South Africa as well. When considering:

- the important role that email plays in information transfer and storage,
- the rapid adoption of cloud-based email in higher education institutions,
- the importance of conformance for good governance and
- the increased challenge associated with governance (and conformance in particular) when adopting cloud-based solutions

It becomes clear that the adoption of cloud-based email in higher education is an area of concern.

This is highlighted by the responses to the questionaire previously referred to. Respondents were asked to select three areas that most concerned them with regard to cloud-based email for their institutions. The responses are shown in Figure 1.2. A hundred percent of the respondents chose security concerns as one of their top three concerns. Notably, six out of the nine respondents listed either compliance or regulatory or legal issues as areas of primary concern.

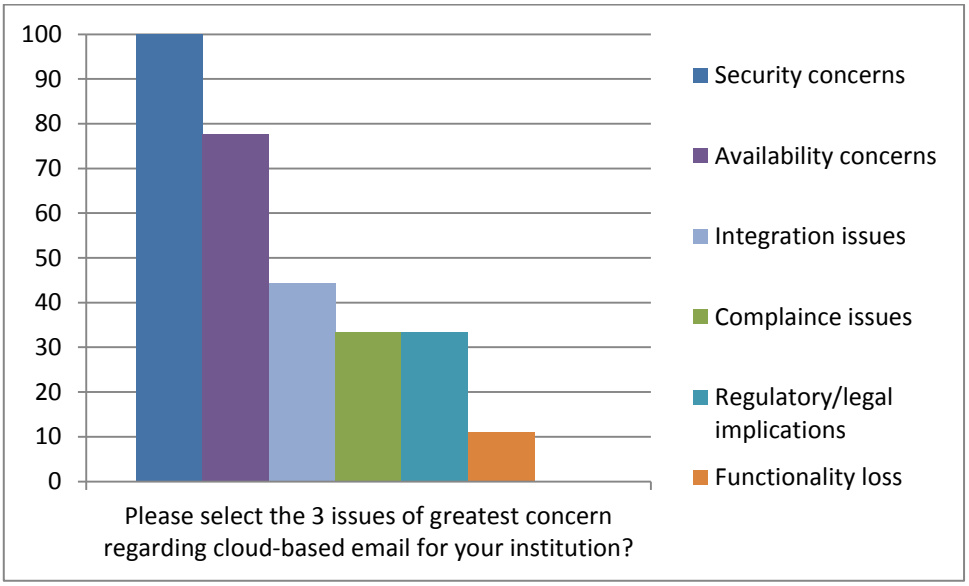


Figure 1.2 Areas of concern for cloud-based email

Eight out of nine respondents either agreed or strongly agreed with the following statement: *I have not been provided with an adequate set of good practice guidelines for the governance, risk and compliance of cloud-based email*. This is shown in Figure 1.3. Interestingly, the one university that disagreed with the statement did not give an indication of any guidelines they would recommend for cloud-based email implementation when prompted to do so. Participants in the 2012 survey were asked "Do you think that South African universities would benefit from a set of guidelines for compliance in the adoption of cloud-based email?" The vast majority of institutions (94 percent) believe that such guidelines would be beneficial.

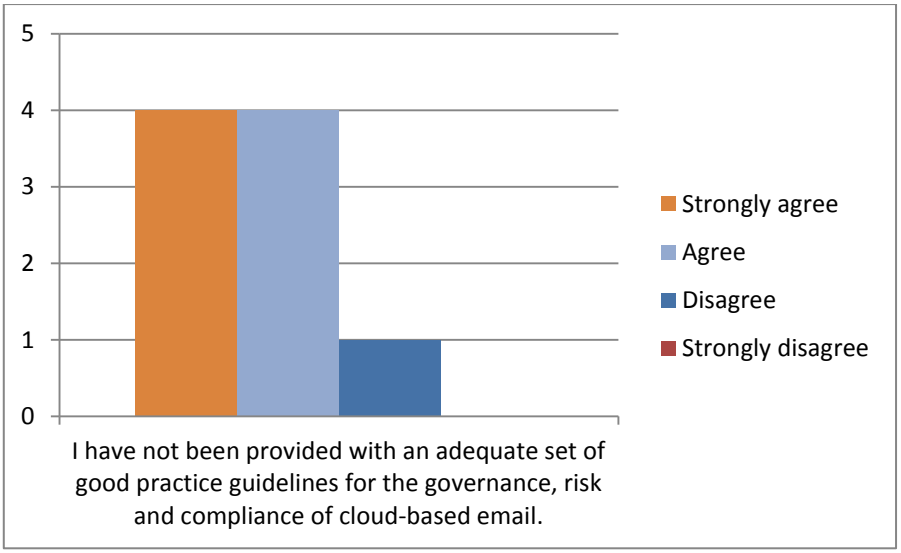


Figure 1.3 Need for cloud-based email guidelines

Considering the important role of email, it is perturbing that IT professionals feel inadequately equipped with regard to the governance, risk and compliance of cloud-based email and are apprehensive about conformance in particular.

1.3 Problem Statement

Taking the background information and discussion above into account, the problem statement for this research study can be expressed as:

The lack of structured guidelines for assurance of cloud-based email conformance is putting this service at risk in higher education institutions in South Africa.

This chapter has introduced some threats and vulnerabilities associated with the use of cloud computing solutions. Chapter 4 and Chapter 5 further emphasise threats and vulnerabilities

associated with cloud computing in general and cloud-based email specifically. As highlighted previously, given the fact that there are serious vulnerabilities in the areas of governance, conformance and assurance of cloud computing, it can be deduced that failure to address such threats could put the effective use of various cloud computing services, including cloud-based email, at serious risk. Without a set of guidelines to address the vulnerabilities and threats related to assuring the conformance of cloud-based email at higher education institutions, such institutions do not have a structured way of ensuring that risks are mitigated. This is likely to affect the level of trust in the appropriate use of cloud-based email. In addition, there may be an increased risk of being unable to demonstrate due diligence in caring for the governance of cloud computing services.

1.4 Research Questions

To address the research problem highlighted above the primary research question becomes:

What framework for assuring conformance should higher education institutions in South Africa consider when implementing a cloud-based email solution?

In answering this question, the following secondary questions are also addressed:

- What conformance and assurance problems are encountered with cloud-based email solutions?
- Which established and accepted standards, frameworks or theories can be used as a foundation for creating a framework for assuring the conformance of cloud-based email?
- What standards, regulations, best practice guidelines, policies and other factors currently influence the management and governance of cloud-based email compliance in higher education institutions in South Africa?
- How should existing standards, regulations, best practice guidelines, policies and other factors influence and/or be changed to accommodate cloud-based email conformance concerns in higher education institutions in South Africa?

Each of the questions above is translated into research objectives in the subsequent section.

1.5 Research Objectives

This section reiterates the research questions listed above and shows the related research objectives. The primary research question and objective are shown in Table 1-3 below. The secondary research questions and associated objectives are shown in Table 1-4.

Research question	Research objective
What framework for assuring conformance should higher education institutions in South Africa consider when implementing a cloud-based email solution?	**To compile a framework to assist South African higher education institutions to assure that cloud-based email solutions are used in a manner that adequately apply the conformance principle of governance.**

Table 1-3 Primary research question and objective

Before explaining the research design used to address these research objectives, the delineation and limitations of this research project is discussed.

1.6 Delineation and Limitations

As suggested in the title of this document, this work investigates only higher education institutions in South Africa. Although much of the work may also be applicable to other types of organisations in other countries, this is not addressed in this work. Additionally, the research is limited to cloud-based email. Some findings of the research may be relevant to other cloud computing solutions, but this is not dealt with. Governance is a primary topic that encompasses many principles. This research focusses primarily on the aspects of conformance (or compliance) and assurance within the area of governance.

1.7 Research Design

This section briefly introduces the research design used to achieve the objectives described in subsection 1.5. The next chapter provides more detail regarding the research design and methodology for this work. In this section the knowledge claims and research strategy are mentioned. This is followed by a description of the research process. In describing the research process, the research methods used are highlighted.

Secondary research question	Secondary research objective
Which established and accepted standards, frameworks or theories can be used as a foundation for creating a framework for assuring the conformance of cloud-based email?	To identify established and accepted standards, frameworks or theories for conformance and assurance that can be used as a foundation for the development of a framework for assuring the conformance of cloud-based email.
What conformance and assurance problems are encountered with cloud-based email solutions?	To devise what conformance and assurance problems currently are encountered with cloud-based email solutions.
What are the shortcomings associated with existing conformance and assurance guidelines that are being used for cloud-based email implementations?	To find out which existing guidelines are currently being used for cloud-based email implementations.
	To determine the shortcomings associated with existing guidelines.
How should existing standards, regulations, best practice guidelines, policies and other factors influence and/or be changed to accommodate cloud-based email conformance concerns in higher education institutions in South Africa?	To formulate how existing standards, regulations, best practice guidelines, policies and other factors should influence or change to accommodate cloud-based email conformance concerns in higher education institutions in South Africa.

Table 1-2 Secondary research questions and objectives

As can be derived from the above, mixed methods were used. A mixed method approach focuses on "collecting, analyzing, and mixing both quantitative and qualitative data in a single study or series of studies. Its central premise is that the use of quantitative and qualitative approaches in combination provides a better understanding of research problems than either approach alone" (Creswell & Plano-Clark, 2007, p. 5).

In line with the above, the following process was used to conduct this research. A ***literature review*** has been conducted to highlight, motivate and provide context for the problem statement. The problem has been triangulated by means of ***surveys*** regarding cloud-based email adoption in higher education institutions in South Africa. Best practice guidelines, standards and other literature have been analysed to determine requirements and implications for a framework for assuring cloud-based email conformance. The information gathered was

used to ***argue*** towards a framework for assuring the conformance of cloud-based email. The practicality of the framework has been demonstrated at a South African higher education institution that is using cloud-based email. The practicality and value of the framework have also been evaluated by IT professionals. The framework and other research findings were published in reputable journals and presented at quality conferences.

How the research is presented is made clear in the following sections, in which this chapter concludes with a description of the chapters that comprise the remainder of this work.

1.8 List of Chapters

This work consists of eight chapters. The basic flow and content of the chapters are described below. Figure 1.4 illustrates the layout of the chapters.

Chapter 1 (Introduction) of the work has introduced the project by describing the research problem, research questions, research objectives and the methodology that has been used to solve the problem. ***Chapter 2 (Research methodology)*** describes the research methodology that informs and motivates this work in more detail. ***Chapter 3 (IT governance, conformance and assurance)*** then describes the fields of governance, conformance and assurance and highlights the relationships between these fields. This is followed by an introduction into the area of cloud computing in ***Chapter 4 (Cloud Computing)***. This chapter defines cloud computing and describes the different cloud service models, including software-as-a-service (SaaS). Attention is drawn to concerns about assurance with cloud computing. The role of standards and guidelines for the assurance of cloud computing are also investigated in this chapter. Guidelines provided by several reputable IT governance bodies regarding cloud computing are described. ***Chapter 5 (Cloud-based email at South African higher education institutions)*** then describes cloud-based email as a SaaS solution. The fact that various international universities and other companies are using or investigating a cloud-based email solution is highlighted. The various conformance considerations of a cloud-based email solution, specifically in South African higher education institutions, are described. ***Chapter 6 (A framework for assuring the conformance of cloud-based email)*** draws on the work described in the previous chapters to describe the framework for assuring the conformance of cloud-based email (FACCE). The validity and value of the framework is defended in ***Chapter 7 (FACCE verification)***. Ultimately, ***Chapter 8 (Conclusion)*** highlights how the work described in the preceding chapters has achieved the research objectives set out in Chapter 1.

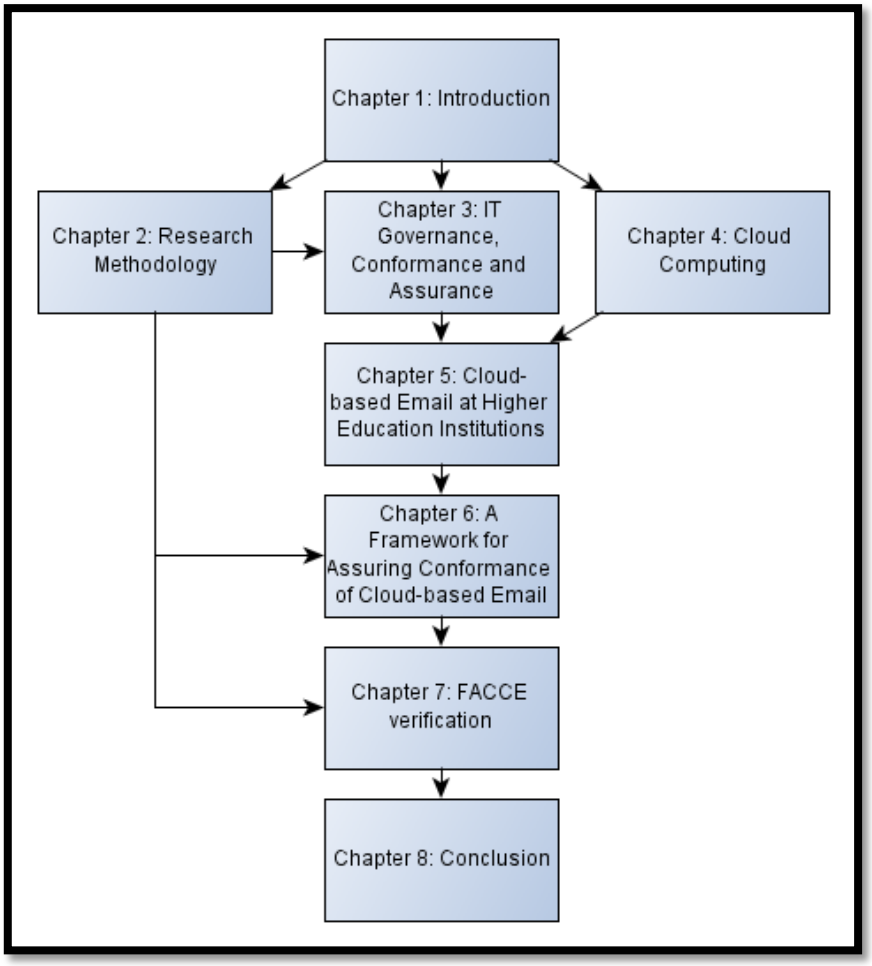


Figure 1.4 Chapter layout

CHAPTER 2
Research Methodology

2.1 Introduction

To research is simply to "investigate systematically", according to the Oxford dictionary. The problem investigated in this work has been introduced in the previous chapter. As stated in section 1.3 of Chapter 1, higher education institutions lack assurance regarding conformance when using cloud-based email, which puts this service at risk. This work aims to systematically investigate this problem with the goal of contributing to a solution.

There are various approaches and methods for conducting an investigation systematically in a structured repeatable manner. These are described in detail by many authors on the subject of research (Hofstee, 2006; Creswell, 2003; Bogdan & Biklen, 1998). This chapter describes how the systematic investigation will be conducted in this study by describing the research design and research methodology employed.

2.2 Research Design

This section briefly explains how this research is designed to provide a solution to assist with the problem of a lack of assurance regarding cloud-based email conformance at higher education institutions in South Africa. The research philosophy of this work is firstly stated though.

It is widely accepted that researchers approach a research project with a certain stance or philosophy (Creswell, 2003; Saunders, Lewis, & Thornhill, 2007; Meyrick, 2006). Identifying and clearly stating this philosophy is seen by some as an important feature of good research (Amis & Silk, 2008; Meyrick, 2006; Saunders, Lewis, & Thornhill, 2007). As stated in the previous chapter, this research will be conducted in a principally pragmatic manner. As such, the researchers acknowledge that problems occur in certain contexts and do not subscribe to either solely a qualitative or quantitative approach. Instead, they focus on solving the problem using methods from both (Creswell, 2003).

As can be easily deduced from the preceding, a mixed method approach will be used. A mixed method approach focuses on "collecting, analyzing, and mixing both quantitative and qualitative data in a single study or series of studies. Its central premise is that the use of

quantitative and qualitative approaches in combination provides a better understanding of research problems than either approach alone" (Creswell & Plano-Clark, 2007, p. 5).

The design and development of an artifact (a framework that can be used in the assurance of cloud-based email conformance) is the main objective of this work. Design science is a field that describes how artifacts should be developed and communicated in a manner that ensures that the resulting work can be seen as rigourous research and not merely as a design activity. The guidelines associated with design science have become clearer and more widely accepted in information systems research (March & Storey, 2008). It is, therefore, fitting that design science is used as the primary strategy of this work.

The development of the artifact (the framework for assuring the conformance of cloud-based email) will be based on the work of two widely referenced authorities regarding the use of design science in information systems: the design science research methodology outlined by Peffers, Tuunanen, Rothenberger & Chatterjee (2008) and the guidelines for design science as explained by Hevner, March, Park, & Ram (2004).

Various research methods will be used to complement the above-mentioned strategy. These will include literature review, argumentation, surveys and a case study. The use of each of these is described and motivated in the next section.

In summary, a pragmatic approach will be used to conduct this research. Design science is used as the primary strategy for conducting the research, and various mixed methods are employed to complement the use of this strategy.

The methodology used for implementing this research design is explained in the next section.

2.3 Research Methodology

Peffers et al. (2008) describe a design science research methodology (hereafter referred to as DSRM) that is used to guide the design of the artifact of this work, a framework for assuring the conformance of cloud-based email, which will hereafter be referred to as the FACCE. The methodology is shown in Figure 2.1. As can be seen in this figure, DSRM involves six key activities. Each of these is discussed in more detail.

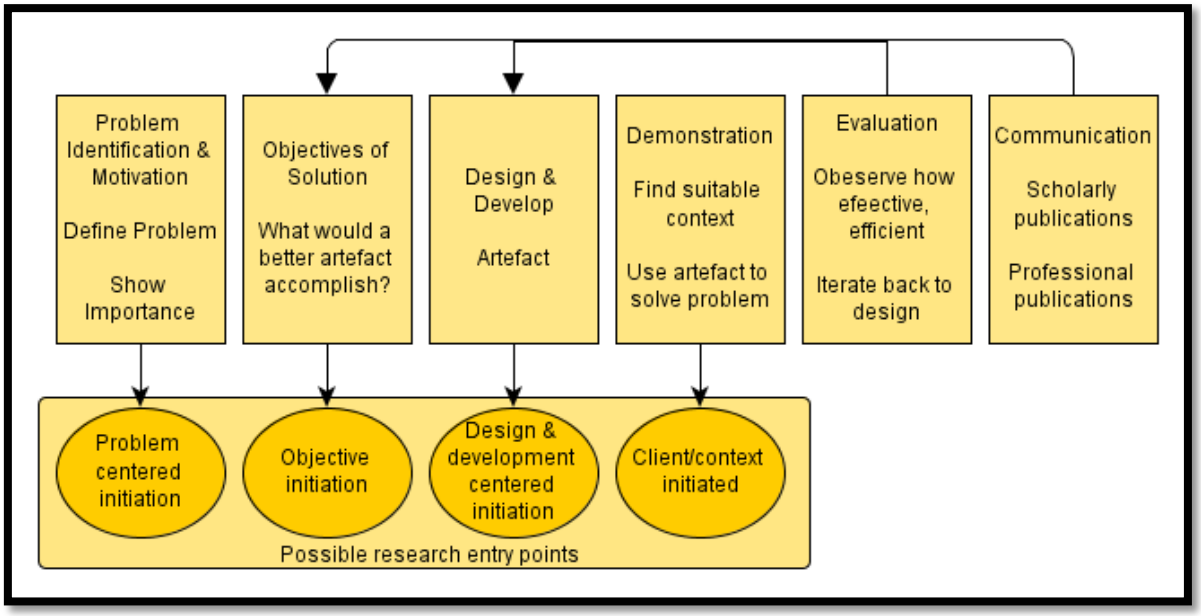


Figure 2.1 The design science research methodology adapted from Peffers, Tuunanen, Rothenberger & Chatterjee, 2008

1. The first activity in this design process involves identifying a problem that is worth solving and motivating the value of a solution to the problem (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2008, pp. 52, 55). The previous chapter has highlighted the ***problem*** that *the lack of structured guidelines for assuring the conformance of cloud-based email is putting this service at risk in higher education institutions in South Africa.* This problem and its importance is further highlighted in the following chapters by means of literature review and questionnaires. The next chapter (Chapter 3) discusses the area of governance, conformance and assurance. It highlights the importance of these subjects being adequately addressed by organisations regarding IT. In Chapter 4, the concerns regarding these subjects (governance, conformance and assurance) regarding cloud computing in general are described. Other challenges commonly associated with cloud computing are also introduced. This provides context to the problem being addressed in this work. Chapter 5 describes how the concerns over governance, conformance and assurance apply to cloud-based email, thereby emphasising the problem being addressed.
2. As the problem areas are analysed by means of a literature review, the desired ***objectives*** of a solution are argued towards. This is the second design science activity (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2008, p. 55). Chapter 3 highlights some objectives of a solution for conformance and assurance. Chapter 5

also summarises a list of objectives for a solution to the problem of assuring the conformance of cloud-based email.

3. Chapter 7 argues towards the ***artifact*** of this work, a framework for assuring the conformance of cloud-based email (FACCE), based on the findings of the literature review. The objectives met by the framework are described. This accomplishes the third activity in the DSRM: design and development of an artifact.
4. Chapter 8 highlights how FACCE has been ***demonstrated*** in a suitable context using a case study at a higher education institution in South Africa.
5. Chapter 8 also describes how FACCE has been ***evaluated*** and refined based on the observations and findings gathered during this case study.
6. The last activity in the DSRM is to ***communicate*** the results of all the previous activities to researchers and other relevant audiences (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2008, p. 56). The results of this work are communicated in various ways. The framework has been communicated to several IT staff through presentations and written explanations during a demonstration at a higher education institution in South Africa. In addition, components of this research have been published in the South African Journal of Business Management (Von Solms & Viljoen, 2012). There is also a paper currently under review at this journal that describes the research done in this study. It is entitled "Towards cloud computing assurance". Another paper entitled "Cloud-based email adoption at higher education institutions in South Africa" also communicates the research done and is under review at the Africa Education Review journal. Further aspects of this work have been presented at the South African Networks and Telecommunications Conference (Viljoen, Von Solms, & Lawack-Davids, 2012). The artifact of this work, FACCE, is also to be presented at the eighth International Conference for Internet Technology and Secured Transactions in December of 2013. A paper entitled "A framework for assuring the conformance of cloud-based email" will appear in the proceedings of this conference.

It is, therefore, clear that the steps outlined as part of the DSRM play an integral part in the design and validation of FACCE. The guidelines for design science likewise guide this work (Hevner, March, Park, & Ram, 2004). The seven guidelines for design science research outlined by Hevener et al. (2004) are listed and explained in terms of this research below. For each of the items in the list, the guideline is bolded and the description of the guideline is

italicized. Each item is followed by a description of how the guideline is applied in this work.

1. **Design as an Artifact -** *A viable artifact in the form of a model, construct, method or instantiation should be produced.*

   A framework for assuring the conformance of cloud-based (FACCE) is designed and described in Chapter 7 of this work in such a manner that it can be implemented in higher education institutions in South Africa.

2. **Problem relevance** - *The solution outlined in the artifact should address any important and relevant problems.*

   The preceding chapter and Chapter 6 of this work highlight the importance and relevance of the problem addressed by FACCE (namely that *the lack of structured guidelines for governance and compliance of cloud-based email is putting this service at risk in higher education institutions in South Africa)* using relevant literature and questionnaire results.

3. **Design evaluation** - *Well-executed evaluation methods should be used to evaluate the utility, quality and efficacy of the artifact.*

   FACCE is verified for utility, quality and efficacy by demonstrating and applying the artifact at a South African higher education institution that uses cloud-based email using a case study like approach. Chapter 8 describes the results of this demonstration.

4. **Research contributions** - *There should be clear and verifiable contributions in the areas of design artifact, design foundation and/or design methodologies.*

   The main artifact of this work (FACCE) will contribute to the area of assurance regarding cloud computing services by addressing the problem that the lack of structured guidelines for governance and compliance of cloud-based email is putting this service at risk in higher education institutions in South Africa. Other contributions of this work are discussed in Chapter 8.

5. **Research rigour** - *Rigourous research methods should be used in both the construction and evaluation of the artifact.*

   An accepted methodology (DSRM) is used in the construction of FACCE. In addition, FACCE is evaluated using a rigourous observational method for evaluation: demonstration of the artifact in a suitable context.

6. **Design as a search process** - *An effective artifact is designed by following an iterative approach where suitable means are used to reach a desired end within the laws of the problem environment.*

   As described in the methodology used for constructing FACCE (DSRM), an iterative approach has been used to design and improve FACCE until this framework meets the objective of providing a manner that can assist in assuring cloud-based email conformance within higher education institutions in South Africa.

7. **Communication of research** - *Research should be presented to technology-oriented and management-oriented audiences.*

   FACCE has been communicated to and used by IT staff members at a higher education institution in South Africa. Additionally, the framework and much of its supporting research has been published in various conferences and journal publications, as described in this chapter.

This section has explained how design science provides a methodology and guidelines that guide systematic investigation for the design of the artifact of this research (FACCE). Figure 2.2 summarises how the design science research methodology (DSRM) and the research methods (which are described next) are used to form the research methodology for this work.

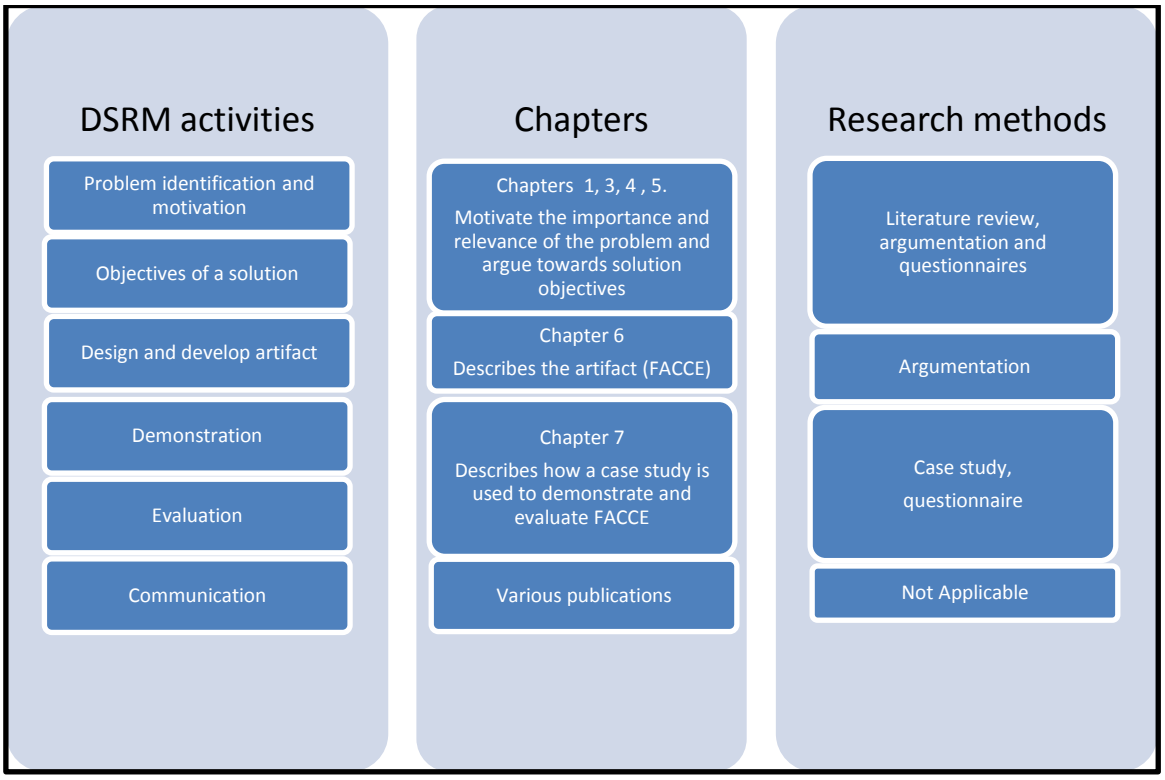


Figure 2.2 Overview of research design for this work

2.4 Research Methods

This chapter has highlighted several research methods that are used as part of the research methodology for this work. They include: case study, questionnaires, literature review and argumentation. These methods are briefly described in this section.

Case study

Case study is a method that allows one to study an artifact in a business environment. It is generally accepted as a method of evaluation in design science (Hevner, March, Park, & Ram, 2004, p. 86). A single-case study will be conducted at a higher education institution in South Africa (hereafter referred to as The University) to investigate the utility, quality and efficacy of FACCE. The University has used cloud-based email for some of their students since 2010. There are various bodies of work that describe approaches to conducting case studies and highlight the advantages and disadvantages of using this specific research method (Merriam, 1998; Yin, 2009; Gerring, 2007). When referring to a case study in this work, however, a simplified approach is followed. A required step in the design science research methodology is that an artifact be demonstrated within a suitable context. In this work, the utility of the artifact is demonstrated at a higher education institution, as described earlier. This higher education institution provides a 'case' that will be studied primarily to answer the question: Can FACCE be used to assist with improving the level of assurance that higher education institutions in South Africa have regarding the conformance of cloud-based email? It is in this sense that the term case study is used in this work (Gillham, 2000). The case study is described in more detail in Chapter 8.

Argumentation

Argumentation is used extensively in this work. In this context, it relates to ensuring that sufficient evidence is provided to support a claim made (Besnard & Hunter, 2008). It is used to argue towards the importance and relevance of the problem being addressed and the relevance of the objectives of a solution proposed. Additionally, argumentation is used to argue towards a framework for assuring the conformance of cloud-based email (FACCE). Argumentation will also be used to argue that there is sufficient evidence to support the claim that FACCE assists in addressing the problem of a lack of assurance regarding conformance related to the use of cloud-based email at higher education institutions in South Africa.

Literature review

A review of relevant literature regarding assurance and conformance in the area of cloud computing will be used to motivate the problem and the solution of this work. The artefact (FACCE) is strongly based on selected best practice guides that are identified as part of the literature review.

Surveys

Surveys are used to gather data regarding the problem area being addressed by this work. The surveys are described in more detail in Chapter 5. This data is used as a source of evidence in arguing towards the relevance and importance of the problem. In addition, a survey is used to gather data regarding IT staff members' perception of the value and utility of FACCE. This data contributes to evidence that is used to argue towards the utility and efficacy of FACCE.

Various research methods are used in conjunction with the design science methodology to develop the artefact of this work: a framework for assuring the conformance of cloud-based email.

2.5 Conclusion

The research philosophy, design, methods and methodology that are used in this research to ensure a systematic investigation that has led to the design of an artefact has been explained in this chapter. This artefact, the FACCE, aims to contribute towards solving the problem of a lack of assurance of conformance for cloud-based email used at higher education institutions in South Africa.

The next chapter begins with a description of the importance of governance, assurance and conformance of enterprise IT. This provides important context and information that will be used to argue towards the relevance and importance of the problem addressed in this work. It is also be used to identify the objectives of a solution.

CHAPTER 3

IT Governance, Conformance & Assurance

3.1 Introduction

The main objective of this work is to provide assistance for *assuring* that, in *governing* cloud-based email, *conformance* can be demonstrated. This chapter provides the context and theoretical underpinnings for the rest of the work by discussing the importance of IT governance, IT conformance and IT assurance. It also highlights the relationship between these areas. Best practice guidance regarding the implementation of IT governance, IT conformance and IT assurance is also described. The discussion in this chapter leads to the identification of high-level objectives and requirements for a framework for assuring the conformance from an IT governance perspective.

This chapter is constructed in the following manner. For each of the main topics discussed in this chapter (IT governance, IT conformance and IT assurance) the following three questions will be discussed: What is it? Why is it important? And how is it achieved? The relationship between governance, conformance and assurance is then highlighted before concluding the chapter.

3.2 IT Governance

IT has become a basic necessity for businesses, and practically every business unit in any organisation depends to some extent on IT to operate appropriately (Weill & Ross, 2004, p. 15). IT is therefore, no longer merely a technical concern that purely involves IT staff. As Peterson points out, business models and IT have become "virtually inseparable", and boards and business executives cannot "delegate, avoid, or ignore IT decisions" since they cannot run a business without "depending on IT and the IT functions at some point in time" (Peterson, 2004, p. 8). The board of an organisation, not the IT staff, is ultimately responsible for ensuring that IT is well-governed within that organisation (Von Solms & Viljoen, 2012). IT governance is, therefore, clearly an important subject. This section discusses exactly what IT governance is and why IT governance is important. How it is implemented and what some of the responsibilities mandated by the principles of IT governance are also addressed.

3.2.1 What IT governance is

Before considering what governance is, it is worth noting the distinction between governance and management. There are similarities when it comes to describing good management and good governance in an organisation. For example, definitions for both governance and management refer to the importance of directing and controlling. Peter Weill and Jeanne Ross (Weill & Ross, 2004, p. 8) highlight the difference between management and governance, claiming that governance entails who makes the decisions, whereas management entails making and implementing those decisions. ISACA highlights the distinction as follows. They describe governance as the mechanism for ensuring "that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives" (ISACA, 2010b, p. 14). Management has to do with planning, building, running and monitoring "activities in alignment with the direction set by the governance body to achieve the enterprise objectives" (ISACA, 2010b, p. 14). Simply put, governance has to do with having mechanisms in place to ensure good high-level decision-making and directives; management has to do with ensuring that those directives are achieved.

The formal definition for IT governance, according to the IT governance institute is: "IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives" (ITGI, 2003, p. 10). This definition will become clearer as the next two sections describe the responsibilities and activities related to achieving IT governance.

3.2.2 IT governance responsibilities

To ensure effective IT governance within organisations, it is important that directors and executive management recognise the importance of IT and its governance and their responsibilities in this regard (Nolan & McFarlan, 2005; Posthumus, Von Solms, & King, 2010; Von Solms & Viljoen, 2012).

According to the *OECD Principles of corporate governance* (2004), a key fiduciary requirement of the board is the duty of care. This requires that the board should always "act on a fully informed basis, in good faith, with due care and diligence." Since information and

IT have become vital to the functioning of most organisations, IT governance is an essential part of all corporate governance (Brown, 2006; Peterson, 2004, p. 9). The board is, therefore, required to practice the duty of care regarding IT (Von Solms & Viljoen, 2012).

The specific responsibilities that the board has with regard to IT governance are highlighted by *The King Report on Corporate Governance for South Africa 2009* (IoDSA, 2009), hereafter referred to as King III, the *Board Briefing on IT Governance* (ITGI, 2003) and the ISO/IEC 38500:2008 standard for C*orporate governance of information technology*. Some of these responsibilities enumerated by Von Solms and Viljoen (2012) are summarised in the list below.

The board of directors should:

- Give strategic direction that is in the best interests of the organisation. Part of this mandate includes the assessment of business opportunities (OECD, 2004; IoDSA, 2009).
- Ensure that opportunities associated with new IT developments are recognised and acted on (ISO, 2008; ITGI, 2003; IoDSA, 2009).
- Ensure value delivery from IT (IoDSA, 2009; ITGI, 2003).
- Ensure that IT risks are adequately addressed (IoDSA, 2009; ITGI, 2003).
- Ensure compliance with applicable IT laws, rules, codes, standard, guidelines and leading practices (ISO, 2008; IoDSA, 2009).
- Remain accountable for enforcing and monitoring effective IT governance, even when the responsibility for the provisioning of IT services has been delegated to another party (IoDSA, 2009).

From the above, it is clear that "the board is responsible for ensuring that opportunities presented by developments in IT are recognised and exploited in a manner that adds value to an organisation and is secure and compliant with regulations, policies, standards and best practice guidelines" (Von Solms & Viljoen, 2012). There is clearly a weighty responsibility entrusted to the board regarding IT governance. The next section discusses why IT governance and these related responsibilities are important.

3.2.3 Why IT governance is important

There are several reasons why ensuring IT governance is important for an organisation. One reason, which has already been alluded to, is the fact that IT is pervasive in modern

enterprises and often plays a critical role in "supporting and enabling enterprise goals" (ITGI, 2003). It is, therefore, important to ensure that IT is properly governed.

Another good reason for IT governance is that, as IT continues to introduce new opportunities and threats to entire enterprises, effective IT governance must be in place so that enterprises can quickly respond to these developments (Weill & Ross, 2004, p. 15; Ali, 2006, p. 71).

In addition, proper IT governance should ensure that money and time spent on IT is spent wisely and produces the intended results. Recognising the importance of IT, many companies invest a great deal of money and time in it (Weill & Ross, 2004, p. 14). Managers are understandably discontented when many IT projects fail, or do not seem to add value to the organisation (Weill & Ross, 2004, p. 17). Managers must, however, recognise the role that they should play in making sure that proper IT governance guidelines are followed so that IT strategy is aligned with business strategy and thereby adds value to the organisation.

Lastly IT governance is important, since it is a critical determinant of a company's success (Brown, 2006). A study conducted by Weill and Ross found that for-profit firms with an above-average ITG performance had higher profits than firms with inferior governance but the same strategy (Weill & Ross, 2004, p. 14). They also found that top-performing firms paid special attention to ITG and used governance patterns that applied to their particular needs (Weill & Ross, 2004, p. 18). Apparent good IT governance can also contribute to stakeholder confidence and a good image with the public (Raghuphati, 2007, p. 98). On the other hand, Ali shows, based on a study of Schwartz and Woodhead's work, that lack of effective IT governance can lead to "business losses, bad reputation, runaway projects, and inefficient operational activities" (Ali, 2006, p. 71).

The foregoing has stressed what IT governance is and why it is important. The definition of IT governance hints at how it is implemented, but more clarity is needed regarding this matter. This is discussed in the next subsection.

3.2.4 How IT governance is implemented

The definition for IT governance, considered earlier in this section, states in part that IT governance "consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives" (ITGI, 2003, p. 10). This describes broadly how IT governance is implemented. Through effective IT governance, organisations aim to align IT with their strategies, thereby

adding value to their organisations (Van Grembergen, De Haes, & Guldentops, 2004, p. 7). This involves a set of leadership, structures, processes, procedures and mechanisms for making and monitoring IT decisions. This section examines the leadership, structures and processes involved in IT governance in more detail. How organisations choose to implement these leadership roles, structures and processes is clearly dependent on various factors within the organisation. Although methods of implementing IT governance will vary, the common factors and principles that influence the development of an IT governance program for all organisations are described here.

Certain managers should always be involved with IT governance to some extent. Since IT governance is an integral part of corporate governance, the ***board*** is ultimately responsible and accountable for IT governance (IoDSA, 2009; Peterson, 2004; ISO, 2008). In addition, ***senior executive managers*** such as the CEOs and Chief Financial Officers (CFOs) play a critical role in the success of IT governance (Brown, 2006; Weill & Ross, 2004). It is understandable that the Chief Information Officer (CIO) will also play an integral part in ITG. Taking into account how critical IT is to companies, Van Grembergen, De Haes and Guldentops suggest that ***IT committees*** be established to oversee this vital area. They refer to the importance of an IT strategy committee at the board level and of IT steering committees at the executive level (2004, pp. 22-23).

Standards and best practice frameworks play a key role in providing guidance regarding how effective IT governance should be achieved in organisations. The International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) have produced ISO/IEC 38500:2008, the *international standard for corporate governance of information technology*. This international standard has also been adopted as the South African national standard for corporate IT governance (SANS 38500). Accordingly, ISO/IEC 38500:2008 provides a framework for effective IT governance that includes a description of principles and a model.

The six principles for IT governance as outlined by ISO/IEC 38500:2008 are:

- Responsibility – staff should be aware of their responsibilities regarding IT and have the skills and authority to do what is required of them
- Strategy – should take into account the current and future IT needs and capabilities

- Acquisition – decisions regarding acquisitions should be made clearly and transparently based on an analysis of benefits, opportunities, costs and risks
- Performance – IT initiatives should be fit for purpose and of acceptable quality
- Conformance – IT should comply with internal (defined by internal policies and practices) and external or legal and regulatory requirements
- Human behaviour – the needs of the people involved should mesh with IT policies, practices and decisions

The model described by ISO/IEC 38500:2008 is depicted in Figure 3.1. As can be seen, it describes three tasks that are seen as essential for IT governance: evaluate, direct and monitor. According to this standard, IT directors should continually *evaluate* the "future current and future use of IT" based on the pressures exerted on the business both internally and externally (ISO, 2008). Directors should "assign responsibility for, and *direct* preparation and implementation of plans and policies" for IT governance (ISO, 2008). Directors should similarly encourage good IT behaviour and a good IT governance culture. Directors are moreover responsible for *monitoring* the performance and conformance of IT. ISO/IEC 38500:2008 described how each of these tasks is to be conducted for all of the six principles of IT governance.

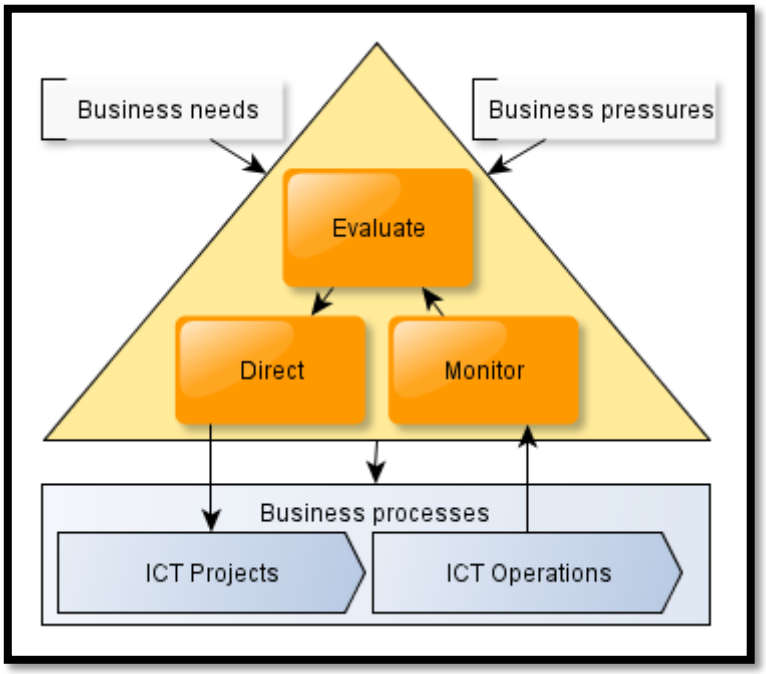


Figure 3.1 Adapted from ISO/IEC 38500:2008 model for IT governance

As described above, ISO/IEC 38500:2008 sets the standard for effective IT governance in South Africa. It describes principles and a model for IT governance that is applicable for all organisations, regardless of size (ISO, 2008, p. 1). This standard purposefully does not provide detailed guidelines regarding the implementation of the standard. IT governance and management frameworks that provide more detail regarding effectively implementing an IT governance program, such as COBIT, are available. Some IT frameworks, which are often seen as IT governance frameworks, address particular concerns (such as information security) or describe guidelines for management, rather than governance. COBIT is a framework that addresses IT governance and management, as can be seen in Figure 3.2 (ISACA, 2010b). The latest version of COBIT, COBIT 5, is based strongly on ISO/IEC 38500:2008.

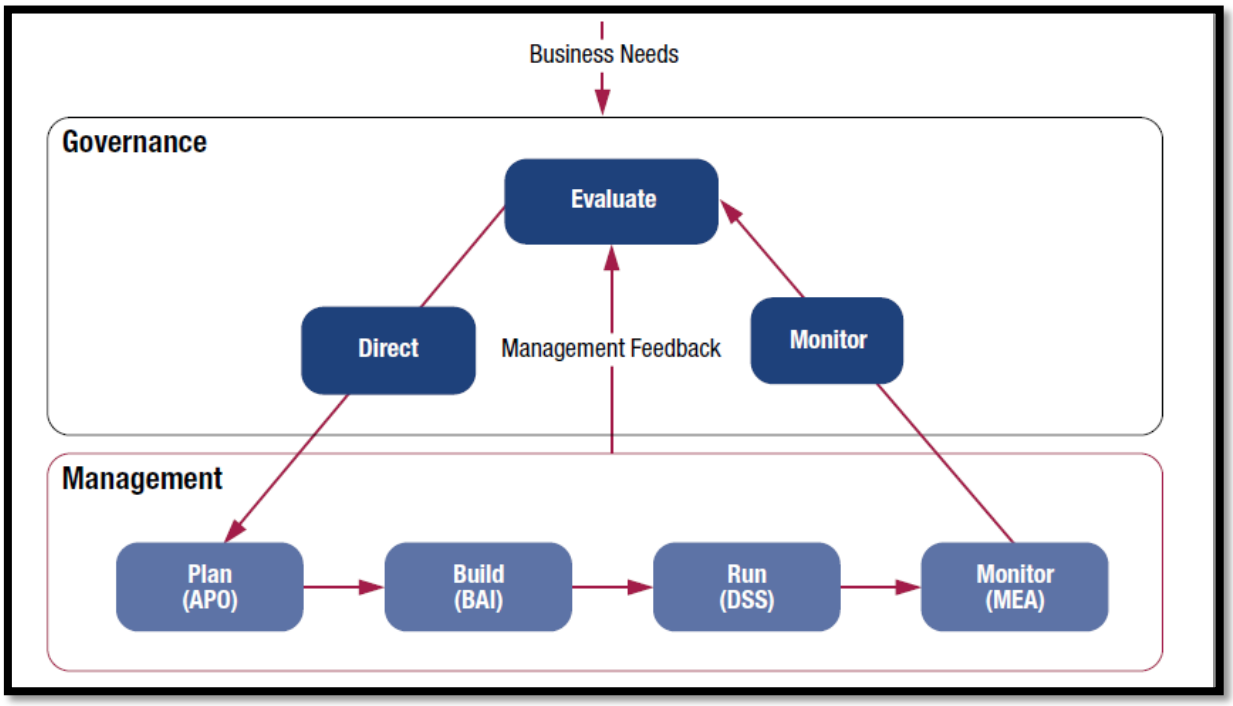


Figure 3.2 COBIT 5's process for IT governance and management (ISACA, 2010b)

COBIT 5 contains guidelines for activities such as establishing business goals and achieving value from IT. In addition, it provides a process reference model that describes a set of best practice activities that can be used for the management and governance of IT. Moreover, COBIT 5 promotes a holistic approach to IT governance and management by identifying and providing guidelines for the effective use of seven enablers for IT governance. Enablers are defined as "factors that, individually and collectively, influence whether something will

work—in this case, governance and management over enterprise IT. … Higher-level IT-related goals define what the different enablers should achieve" (ISACA, 2010b, p. 27).

This section has provided an overview of factors such as leadership roles, principles, and guidelines regarding structure and processes that may influence how organisations achieve IT governance.

The discussion thus far has provided a broad overview of what IT governance is and how it works. This work, however, focusses primarily on one of the six core principles of IT governance: conformance (ISO, 2008). Ensuring conformance with internal and external requirements placed on organisations has also been described previously as an important responsibility for IT governance. After considering some of the responsibilities that the board of directors has regarding IT governance, the following composite responsibility was concluded: "the board is responsible for ensuring that opportunities presented by developments in IT are recognized and exploited in a manner that adds value to an organisation and is secure and compliant with regulations, policies, standards and best practice guidelines" (Von Solms & Viljoen, 2012). The responsibility of ensuring conformance is clearly included in this composite responsibility. The responsibility of assurance can, however, also be identified therein. The function of assurance can assist managers in meeting this responsibility by providing a mechanism for judging the extent to which a certain subject matter complies with criteria based on regulations, standards and best practice guidelines. The next two sections highlight the importance of these two important aspects of IT governance: conformance and assurance.

3.3 Conformance

As described previously, conformance is a crucial aspect of IT governance. This section will follow a similar format to the previous section. It will describe firstly what conformance is, then why it is important and, finally, how it is applied in organisations.

3.3.1 What conformance is

Conformance involves ensuring that IT initiatives comply or conform to internal and external requirements. These requirements include 1) legal and regulatory obligations: regulatory, legislation, common law and contractual and 2) internal requirements as set forth in: internal policies, standards, professional guidelines and systems for IT governance (ISO, 2008, p. 22). As can be seen from this definition, the terms conformance and compliance are often

used interchangeably. In this work both IT conformance and IT compliance are used to mean adherence to internal and external requirements. The term conformance is primarily used though, to indicate alignment with ISO/IEC 38500 which refers to conformance as part of governance.

3.3.2 Why IT conformance is important

Organisations should be interested in demonstrating IT conformance for various reasons. A reason that can be concluded from the description thus far is that it is part of good governance. As is explained in the previous section, modern organisations are expected to demonstrate good corporate and good IT governance. Since IT conformance is essential to IT governance, good IT governance cannot be achieved without ensuring IT conformance.

Similarly, directors of organisations who are responsible for showing due care and due diligence would be unable to fulfill these responsibilities without doing what is "reasonably prudent" with regard to ensuring IT compliance (IoDSA, 2009; Wright, 2008, p. 2).

Another clear reason for this is that all organisations are under legal obligation to demonstrate compliance with applicable legislation. Failure to do so could result in fines or even imprisonment (Giles, 2009; Viljoen, Von Solms, & Lawack-Davids, 2012).

Ethical considerations are an additional reason to be concerned with IT conformance (Viljoen, Von Solms, & Lawack-Davids, 2012). When it comes to business requirements that affect IT that are not covered by the law, self-regulation is required (Van den Bergh & Deschoolmeester, 2010). A culture of moral and ethical behaviour could contribute to compliance with requirements affecting IT.

All organisations are, therefore, required by the law, principles of good governance and principles of ethical behaviour, to take due care in demonstrating IT compliance. This can, however, be challenging (Abdullah, Sadiq, & Indulska, 2010).

3.3.3 How IT conformance is implemented

As with IT governance, organisations decide how to implement IT compliance based on their specific needs and set of circumstances. This section, therefore, concentrates on the general principles for IT conformance that should be in place when implementing IT conformance rather than specifying exactly how it is achieved. It accomplishes this by describing how IT conformance forms part of IT governance and some tasks that are commonly associated with IT conformance.

As highlighted more than once in this section, IT conformance is part of IT governance. It is, like IT governance, not merely a technical concern. It should be supported by executive management and other role players, such as the organisation's legal team (Aumueller, 2010). In addition, since IT compliance is part of IT governance, it is clear that IT compliance initiatives should not be managed and governed in isolation, but as part of a larger IT governance initiative. In the field of governance, risk and compliance (GRC), an integrated approach to governance, compliance and risk management is promoted (ISACA, 2008c). This is clear from the definition of GRC. It is defined as "an integrated, holistic approach to organisation-wide governance, risk, and compliance. This ensures that an organisation acts ethically correct and in accordance with its risk appetite, internal policies, and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness" (Racz, Weippl, & Seufert, 2010). This work does not investigate GRC. The fact that conformance should be viewed as part of a greater IT governance initiative is, nevertheless, important when investigating conformance. This work, therefore, studies conformance in the context of IT governance. Clearly then conformance should be viewed not merely as a technical concern but as a part of IT governance. As such, staff at various levels of the organisation should have responsibilities to support IT compliance, and IT compliance initiatives should be implemented as part of a bigger IT governance program.

There are some tasks for IT conformance that are generally recognised. As described previously, ISO/IEC 38500 describes that the governance tasks of evaluate, direct and monitor should be applied to conformance. When ensuring conformance, these tasks should involve the following:

- Evaluate – evaluating the extent to which an institution is complying with the legal and regulatory obligations and internal requirements
- Direct – direction should be given to ensure that staff is aware of their conformance responsibilities and that policy, plans and mechanisms are in place to ensure conformance
- Monitor – there should be appropriate reporting and assurance practices in place to ensure that IT conformance and related IT activities are adequately monitored (ISO, 2008, p. 22)

Racz, Weippl and Seurfert describe a model for compliance by Rath and Sponholz (2010). This model is depicted in Figure 3.3. As shown in this figure, compliance generally includes the tasks of identifying requirements for internal and external conformance (requirement analysis), evaluating adherence to these requirements by various means, such as audits and/or self-assessment (deviation analysis) and then addressing and managing deviation from what is required by improving or adding controls as necessary (deficiency management). Information gathered during each of these steps should be documented and reported (reporting/documentation) (Racz, Weippl, & Seufert, 2010).

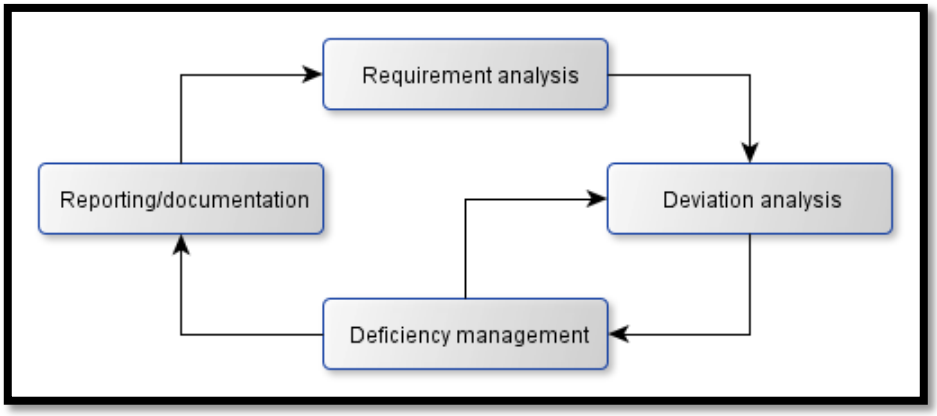


Figure 3.3 Model for compliance as described by Raez, Weippl & Seurf (2010)

Dameri similarly highlights some activities necessary for IT compliance projects regarding financial information systems (2009). These steps are summarised below.

- Define the scope of IT compliance – specify the scope of the IT compliance project by identifying what information systems and regulations are involved in the project.
- Map and document in-scope IT components – "map all the operations composing the processes and document them, outlining the processing regarding each financial data."
- Design controls – identify risks and design controls to mitigate these.
- Evaluate controls – evaluate controls to determine whether they are functioning as required.
- Report on the IT compliance activity – reports documenting IT compliance activities should be available for all relevant parties (Dameri, 2009).

Taking the tasks described for IT compliance from the three works (Dameri, 2009; ISO, 2008; Racz, Weippl, & Seufert, 2010) described in this section we can conclude the following: IT compliance should include activities to:

- Identify requirements for IT compliance within a specific scope.
- Design a set of controls or processes that are to be implemented to meet these requirements.
- Monitor and manage the effectiveness of the controls.
- Document and report on this process.

This section has provided a brief description of conformance as part of IT governance by describing what it is, why it is necessary and how it works. Another aspect of governance that forms a focal part of this study is assurance.

3.4 Assurance

Assurance has become an aspect of governance with increasing scope in organisations. Chambers describes how the view of assurance has progressed over the years. In the early twentieth century (1904) assurance was thought of primarily as auditing business accounting functions. By the end of the twentieth century (1998), however, assurance has been discussed in terms of risk (Chambers, 2009). Assurance is no longer viewed as merely an accounting term but is a concept that applies to other fields that introduce risk to an organisation, including IT. This section once again describes what assurance is, why it is important and what is involved in demonstrating assurance.

3.4.1 What assurance is

Modern definitions of assurance express the broad scope of this subject. According to Business Dictionary.com, assurance is defined as "part of corporate governance in which a management provides accurate and current information to the stakeholders about the efficiency and effectiveness of its policies and operations, and the status of its compliance with the statutory regulations." ISACA similarly defines assurance as an "objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the organisation" (2011). From these definitions it is clear that assurance is concerned with measuring the level of efficiency and effectiveness of controls and processes in place to ensure:

- compliance with both internal (policies) and external (statutory regulations) requirements placed on an organisation and,
- risk management.

The international framework for assurance engagements (hereafter referred to as IFAE) enhances understanding of what is involved with assurance. An assurance engagement is defined as an "engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria" (International Auditing and Assurance Standards Board, 2004).

This definition for an assurance engagement once again highlights the fact that assurance is necessary for a wide array of business functions, not merely for accounting or financial functions. Any identifiable subject for whom one is able to consistently evaluate against identified criteria and for which sufficient appropriate evidence can be gathered to support an assurance conclusion using the IFAE (International Auditing and Assurance Standards Board, 2004, p. 13). Assurance of various cloud computing solutions could, therefore, be gained using the principles outlined in the IFAE.

This definition highlights some of the benefits of assurance. It also gives a brief description of how assurance is accomplished. These two points are described in more detail in the next two sections.

3.4.2 Why assurance is important

There are several reasons that IT assurance is important in organisations. Assurance is a requirement of good corporate and IT governance, and it is associated with significant benefits, such as improved confidence and trust. These benefits are listed and described below.

- *Assurance is mandated by principles of good corporate and IT governance* - Like conformance, assurance is part of governance, and the need for assurance is highlighted numerous times in codes for good corporate governance (IoDSA, 2009; OECD, 2004). Mechanisms for obtaining assurance, such as internal and external audits, are also recommended in such guides. As described earlier, the board is responsible for ensuring that opportunities presented by developments in IT are recognised and exploited in a manner that adds value to an organisation and is secure and compliant with regulations, policies, standards and best practice guidelines" (Von Solms & Viljoen, 2012). The function of assurance can assist managers in meeting this governance responsibility by

providing a mechanism for judging the extent to which a certain subject matter complies with criteria based on regulations, standards and best practice guidelines.

- *Assurance promotes confidence* - The description of assurance by IFAE, quoted earlier, highlights one of the primary benefits and goals associated with assurance: confidence. When it comes to providing assurance within the context of IT governance, assurance assists by providing evidence that criteria is being met (thereby building confidence) or by making the areas where adjustment are needed apparent.
- *Assurance promotes trust* – From an IT perspective, when assurance can be given that an IT system is meeting the requirements or criteria demanded from it, it promotes trust in this system.

The points listed above have highlighted some reasons that assurance is important. The next section discusses how assurance is achieved.

3.4.3 How assurance is achieved

As stated earlier, an assurance engagement is defined as an "engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria" (International Auditing and Assurance Standards Board, 2004).

As can be seen from the definition of an assurance engagement, the IFAE identifies three actors involved: a practitioner, an intended user and a responsible party. A ***practitioner*** is the actor tasked with performing an assurance engagement. The practitioner could, but does not have to be an auditor. The ***responsible party*** is the entity responsible for the subject matter. The ***intended user*** is the group for which the assurance report is prepared. The intended user may include the responsible party and other stakeholders. All three parties may be involved in deciding the requirements of the assurance engagement.

As stated in the definition, a practitioner performs an assurance engagement by evaluating evidence about a certain subject matter against criteria for the subject matter. The relationships between the main components for assurance are illustrated in Figure 3.4. ***Criteria*** are the benchmark against which the subject matter is evaluated. It is essential that criteria are suitable for the assurance engagement to be consistent and reliable. Suitable criteria should be context sensitive, relevant, complete, reliable, neutral and understandable

(International Auditing and Assurance Standards Board, 2004, p. 14). Criteria must be made available to intended users so that they can understand how the subject matter will be evaluated. ***Evidence*** comes in various forms and provides proof of the way the subject matter measures up to the criteria. The practitioner will judge the sufficiency, appropriateness and materiality of the evidence (International Auditing and Assurance Standards Board, 2004, p. 17, ISACA, 2008a). The responsible party will work with the practitioner to make evidence available. After the criteria and evidence have been measured, the practitioner produces an ***assurance report*** that states a "conclusion that conveys the assurance obtained about the subject matter information" (International Auditing and Assurance Standards Board, 2004, p. 21).

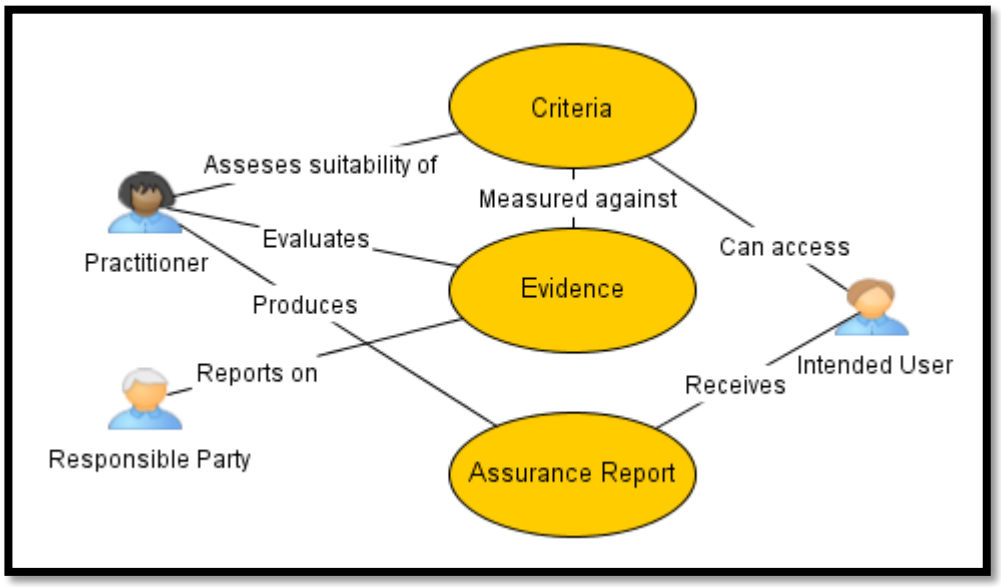


Figure 3.4 The components and relationships necessary for assurance

The ITAF is a professional practices framework for IT assurance that further provides guidelines for implementing an assurance program (ISACA, 2008b). It provides a set of mandatory standards that describe requirements for an audit, such as a code of ethics that should be adhered to during an audit and standards regarding the types of reporting done during an audit. In addition, it provides non-mandatory guidelines and tools and techniques that describe methodologies that can be used for auditing.

ISACA, the same body responsible for producing the ITAF, also provides 'COBIT 5 for assurance' (ISACA, 2013). This document can be used in conjunction with the ITAF. As can

be seen in Figure 3.5, the ITAF is based primarily on the IFAE, describing many of the same components. It describes both how IT governance enablers can be used to assist with providing assurance and how assurance can be provided over such enablers.

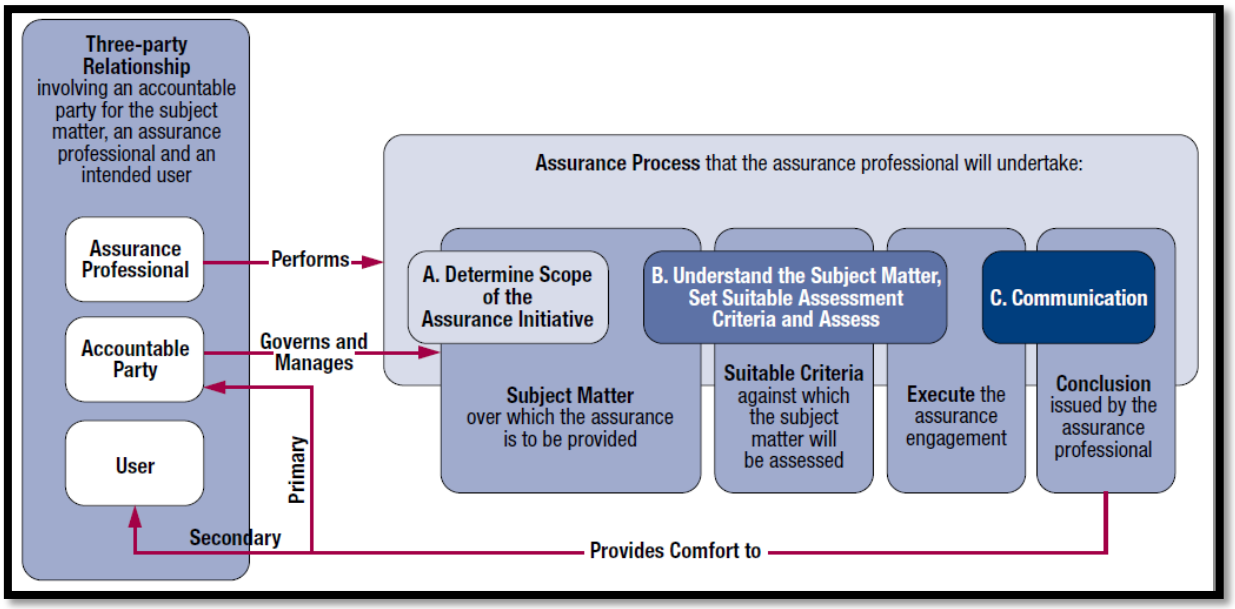


Figure 3.5 ISACA's depiction of assurance components (ISACA, 2013)

There are various types of audits that can be conducted to provide assurance in organisations. Ion, Traian, & Cristian identify several types of audits, listed below.

- External and internal audits - audits can either be conducted by a department within the organisation being audited or by and external auditor
- Preventive or corrective audits – preventive audits evaluate operations before they are done to prevent negative consequences whereas corrective audits evaluate the effectiveness of existing operations
- Conformity, performance or attestation audits - These audits evaluate conformance, performance or attest to the credibility of statements respectively
- Audits of systems and applications, information processing environments, development systems, IT management and/or the Client/Server architecture – these are some of the areas that can be covered in an IT audit (Ion, Traian, & Cristian, 2008).

The guidelines highlighted in this section can be applied to all these types of audits. Governance frameworks often mandate the use of both internal and external audits to provide IT assurance (ISACA, 2010b; IoDSA, 2009). These audits are formal and are guided by the strict standards described by frameworks, like the ITAF. The high-level activities for assurance, such as those described in IFAE and the principles for IT assurance described in *COBIT 5,* can also be effectively applied to less formal initiatives within organisations that are aimed at providing a level of assurance. Methods of self-assurance and continuous auditing fall into this range of activity (Nelson & McCollum, 2004; Best, Mohay, & Anderson, 2004). Using automated systems to aid with this is also a popular and beneficial means to improve the assurance available to organisations (McCollum, 2011; Nelson & McCollum, 2004).

The subjects of IT governance, IT conformance and IT assurance have now been described. For each of these subjects, the topics of what, why and how have been discussed. In each instance, best practice standards and/or frameworks have been used to describe how the subject is achieved. The relationships between IT governance, IT conformance and IT assurance have been alluded to throughout this chapter; the following section highlights the relationships further.

3.5 Assuring IT Conformance from a Governance Perspective

The aim of this work is to provide a way to assist with addressing the problem of a lack of structured guidelines for assurance and compliance of cloud-based email, which puts this service at risk in higher education institutions in South Africa. It aims to do this by proposing a framework that can be used for assuring the conformance of cloud-based email. This chapter provides the context for this study by describing the areas of assurance and conformance from an IT governance perspective. The areas have been described separately so far, but this section draws them together to highlight the importance of assuring conformance in IT.

Figure 3.6 highlights the relationships between the subjects discussed in this chapter. Firstly, it is important to note that both conformance and assurance are mandated and governed by IT governance as part of corporate governance. As such, IT conformance has to do not only with conforming to external requirements (such as legal obligations) but also with conforming to the internal requirements described in the IT governance structure of the

organisation. Assuring conformance therefore entails more than just assuring legal and regulatory compliance. Rather, it also has to do with assuring that criteria for conformance with IT governance guidelines are achieved as well. Accordingly, throughout the remainder of this work, IT conformance and assurance are studied in terms of their strong relation to IT governance.

Another important feature of Figure 3.6 is to note that a best practice approach for guiding the achievement of IT governance, IT conformance and IT assurance is described and promoted in this work.

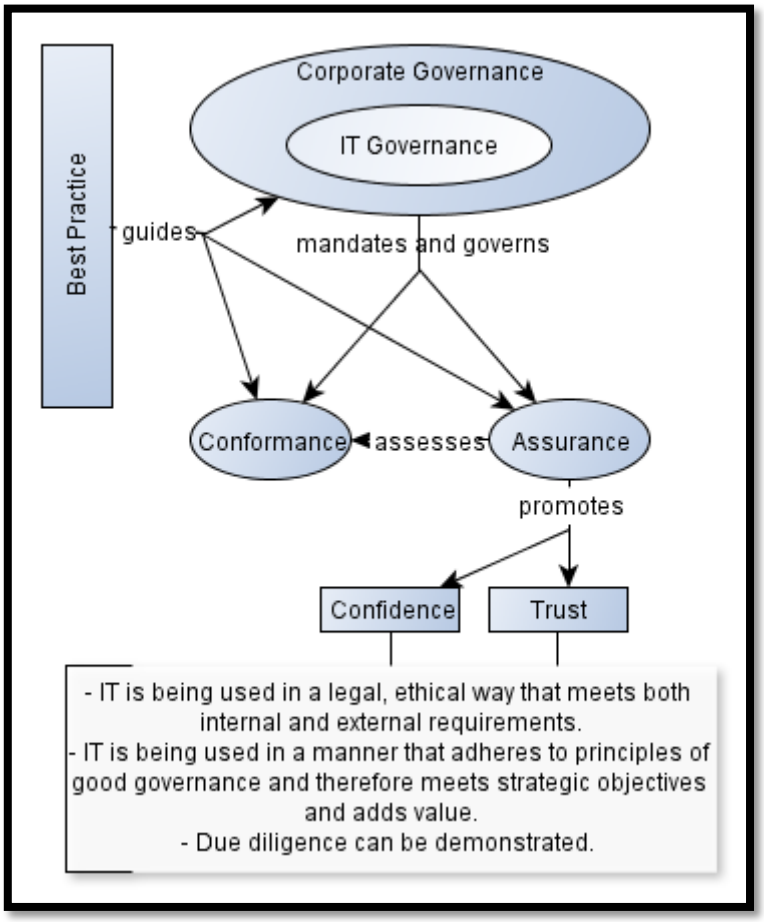


Figure 3.6 The benefits of a best practice based approach for assuring conformance from an IT governance perspective

Assuring conformance therefore, ensures that a best practice based approach is used for assuring that IT conforms to its internal and external requirements, where the internal requirements are often informed by the IT governance structure used by the organisation.

When assuring conformance is conducted in this manner, the following benefits can be derived:

- *Assurance builds confidence and trust that IT is being used in a legal, ethical manner that meets both internal and external requirements.* The section describing the importance of conformance in this chapter highlighted that conformance is needed to meet legal obligations and to meet ethical obligations. Assuring conformance provides evidence to show to what extent this is being done and, therefore, either asserts the claim that IT is being used in a legal, ethical manner that meets both internal and external requirements, or highlights areas of concern that should be addressed.
- *Assurance builds confidence and trust that IT is being used in a manner that adheres to principles of good governance and meets strategic objectives and adds value*. Since both assurance and conformance are mandated by IT governance and form an important part of governance, using best practice as a guide to providing assurance that conformance is being properly implemented assists with demonstrating IT governance. Furthermore, IT strategic alignment and ensuring that IT adds value are two key goals of IT governance. Assuring conformance with internal requirements in well-governed organisations with a well-defined governance structure should therefore build confidence that IT meets its strategic objectives and adds value.
- *Assurance assists with demonstrating due diligence more confidently.* Best practice provides reputable guidance from experts in a field. It describes not only what reasonably prudent behaviour in a field is but what the best way of approaching a subject is. By using best practice to guide assurance and conformance, it makes it easier to argue that due diligence has been shown to ensure conformance.

There are clear benefits associated with adopting a best practice based approach for assuring conformance from an IT governance perspective.

The following high-level objective and associated requirements for a framework for assuring conformance associated with an IT related subject matter can be concluded:

- Objective: Assist with promoting trust and confidence in the conformance of subject matter
    - Requirement: Provide assure conformance by using accepted assurance and conformance methods and techniques.

- Objective: Assist with demonstrating due diligence
    - Requirement: Promote a best practice/standards based approach for assuring conformance.
- Objective: Assist with achieving the goals of IT governance (strategic alignment and value optimization) for the subject matter
    - Requirement: Ensure that the conformance and assurance activities promoted by the framework are strongly guided by best practice guidelines for IT governance.

An investigation of the related areas of IT governance, IT conformance and IT assurance has aided in identifying high-level requirements for a framework to assist with assuring the conformance. The principles and information described here inform the remainder of work done for assuring cloud-based email conformance.

3.6 Conclusion

This chapter has described the related areas of IT governance, IT conformance and IT assurance. In doing so, it has identified and described several well-accepted best practice standards and frameworks that provide guidelines for effectively creating and executing programs in each of these areas. Furthermore, this chapter has highlighted the importance of IT governance, IT conformance and IT assurance. It has also highlighted how these subjects work together, and it shows the importance of having a system for assuring conformance of IT subject matters. The benefits of such an approach have been described. Some high-level objectives requirements for a framework for assuring conformance of an IT related subject matter have also been identified.

This work aims to provide a way to assist with addressing the problem that a lack of structured guidelines for assurance and compliance of cloud-based email is putting this service at risk in higher education institutions in South Africa. This chapter has contributed to an understanding of the importance and relevance of this problem by highlighting the importance and benefits related to assuring conformance of IT related subject matters in an appropriate manner. The IT-related subject matter that is being investigated in this work is cloud-based email, a cloud computing solution. The importance of this problem is made clearer in the next chapter.

CHAPTER 4

Cloud Computing

4.1 Introduction

The previous chapter has highlighted the importance of good IT governance, compliance and assurance in all fields of information technology (IT). Cloud computing is an IT solution that in many respects highlights the importance of addressing these issues adequately. This chapter highlights this. Firstly though, this chapter introduces cloud computing as a concept or paradigm. It discusses what cloud computing is, why it is important and some of the opportunities and challenges associated with it.

4.2 Cloud Computing Explained

For cloud computing to be successfully researched, managed, implemented or used, it must be understood. In its infancy in 2009, cloud computing was a term many were attempting to define. Table 4-1 provides a sample of definitions of cloud computing from that year. As seen from a statement in an InfoWorld article, cloud computing was still an indistinct term to some: "As a metaphor for the Internet, 'the cloud' is a familiar cliché, but when combined with 'computing' the meaning gets bigger and fuzzier" (InfoWorld, 2009, p. 10). In late 2009, though, Mell and Grance published a definition that would eventually become the most widely referenced NIST definition of cloud computing (Mell & Grance, 2011; Mell & Grance, 2009; Celar, Seremet, & Turic, 2011). Work by NIST has largely clarified the term cloud computing by providing not only a definition, but also a reference architecture and case studies that describe it. The rest of this section will consider both the NIST definition and reference architecture in order to explain what cloud computing is.

Before considering this more technical definition of cloud computing though, a simplified explanation is offered here. There are various ways of describing cloud computing (Fingar, 2009, p. 26). At times it is useful to be able to provide non-IT management and staff with a high-level, non-technical description of cloud computing.

Cloud computing definitions
• "Another way to describe services offered in the cloud is to liken them to that of a utility. Just as enterprises pay for the electricity, gas and water they use, they now have the option of paying for IT services on a consumption basis" (ISACA, 2009, p. 4). • "Cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption" (Cloud Security Alliance, 2009b, p. 13). • "Boiled down to a phrase, it's using information technology as a service over the network. We define it as services that are encapsulated, have an API, and are available over the network. This definition encompasses using both compute and storage resources as services" (Sun Microsystems, 2009, p. 1). • "Cloud computing is a style of computing whose foundation is the delivery of services, software and processing capacity using private or public networks. The focus of cloud computing is the user experience, and the essence is to decouple the delivery of computing services from the underlying technology. Beyond the user interface, the technology behind the cloud remains invisible to the user, making cloud computing incredibly user-friendly. Cloud computing is an emerging approach to shared infrastructure in which large pools of systems are linked together in private or public networks to pro-vide IT services" (IBM, 2009, p. 3).

Table 4-1 Cloud computing definitions

Cloud computing can be understood as follows: "cloud computing is a computing model which allows one to access an IT service over a network, as or when it is needed, without worrying about the technical details of how the service is provided" (Von Solms & Viljoen, 2012). It can be likened to using a shared form of transport (for example, public transport) instead of private transport (such as one's car), when needed (Von Solms & Viljoen, 2012). To illustrate, it may be more convenient for one to ride to work in one's car; however, if one is planning a trip from one city to another one may decide to use a means of public transport, such as an airplane, a train or a bus. In this case, one would merely pay for that particular service while using it. In the same way, at times it is best for one to have one's own programs installed on a computer. There are, however, cases when one would derive

substantial benefit from accessing IT resources, such as certain programs or services, over a shared network. This could be done by using cloud computing. As can be seen from Table 4-1, cloud computing has been similarly explained using the utility analogy (ISACA, 2009, p. 4; Breeding, 2009).

4.2.1 Cloud Computing Defined

The preceding provides a simplified explanation of cloud computing. There are "many approaches and nuisances to cloud computing" (ISACA, 2009, p. 6). Various organisations will use cloud computing in different ways. The common description of cloud computing as a collection of essential characteristics, service models and deployment models is, therefore, more accurate (Mell & Grance, 2009; Cloud Security Alliance, 2009b, pp. 13-23; Mather, Kumaraswamy, & Latif, 2009, pp. 4, 7-8). The Cloud Security Alliance provides the visual representation of NIST's widely referenced definition for cloud computing, as shown in Figure 4.1 (Cloud Security Alliance, 2009b, p. 14). The three aspects of cloud computing – characteristics, service models and deployment models – depicted in Figure 4.1 are each explained subsequently.

4.2.1.1 Cloud essential characteristics

Mell and Grance (2009) lists the following essential characteristics for cloud computing:

- On-demand self-service – users are able to self-provision resources (such as processing capabilities or storage) made available by various service providers without interacting personally with each service provider (Mather, Kumaraswamy, & Latif, 2009, p. 8; Porta, Karimi, Plakskon, & Sharma, 2009, p. 3).
- Broad network access – services are accessed through standard mechanisms over the network (Porta, Karimi, Plakskon, & Sharma, 2009, p. 3).
- Resource pooling – cloud service providers' resources are pooled, making multitenancy (the sharing of resources by multiple users or 'tenants') possible (Mather, Kumaraswamy, & Latif, 2009, p. 8; Porta, Karimi, Plakskon, & Sharma, 2009, p. 3).
- Rapid elasticity – resources are quickly made available and released so that resources can appear unlimited to the user (Mather, Kumaraswamy, & Latif, 2009, p. 8; Porta, Karimi, Plakskon, & Sharma, 2009, p. 3).
- Measured service – metering capabilities are used to control and optimise resource usage.

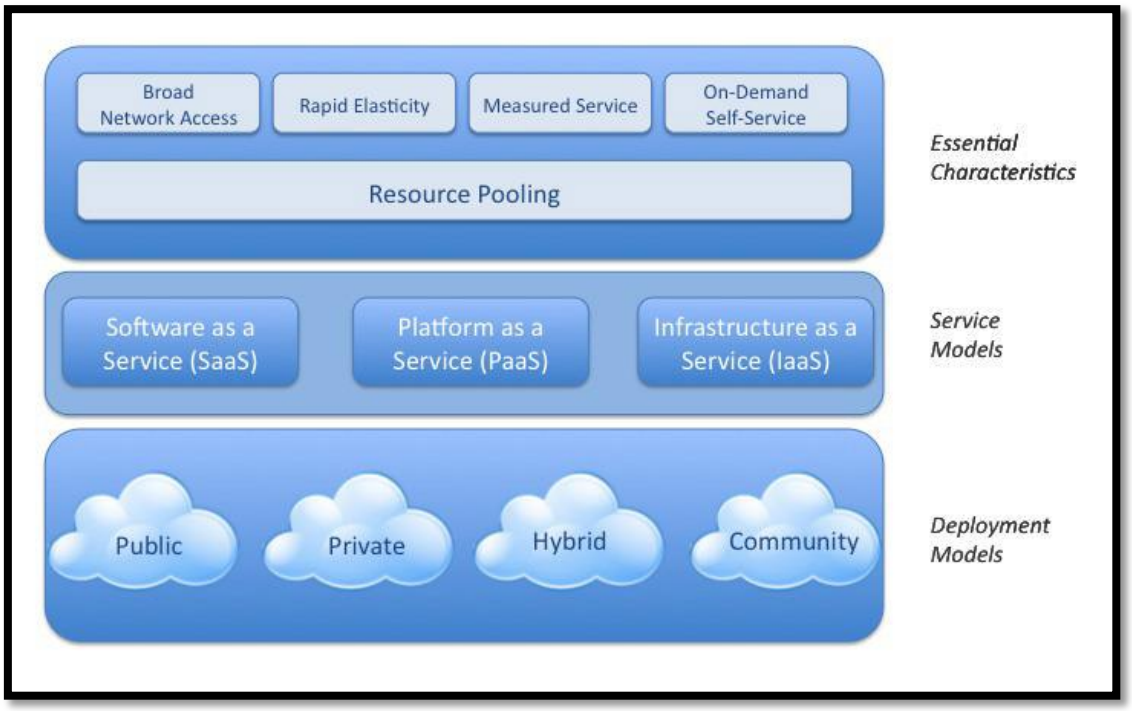


Figure 4.1 CSA's visual representation of NIST's cloud computing definition (Cloud Security Alliance, 2009b)

Although not listed by NIST as essential, the following characteristics are often used to describe cloud computing: massively scalable (Mather, Kumaraswamy, & Latif, 2009, p. 8) and pay-as-you-go (Mather, Kumaraswamy, & Latif, 2009, p. 8; Porta, Karimi, Plakskon, & Sharma, 2009, p. 3).

4.2.1.2 Cloud service models

NIST defines cloud computing as being composed of three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (PaaS). The SPI (an acronym referring to the three service models) framework is used to describe these cloud computing services (Mather, Kumaraswamy, & Latif, 2009, p. 11). The three service models are discussed below.

1. Cloud Software as a Service – CSPs make software available to users on the cloud infrastructure. The software can be accessed by various authorised devices using a thin client interface (ISACA, 2009, p. 5). SaaS differs from application service provider (ASP) solutions in that it is designed to run in a multitenant architecture, whereas ASP solutions are single-tenant applications hosted by a third party. SaaS applications are, in addition, designed to run on the web, whereas ASP applications are not written as

Net-native applications (Mather, Kumaraswamy, & Latif, 2009, p. 19). Cloud-based email can be considered a SaaS application.

2. Cloud Platform as a Service – CSPs make development platforms available to users using the cloud. The CSP will typically make 'toolkits, standards for development and channels for distribution and payment' available to users. The users are, therefore, able to build and deploy applications on the platform provided by the CSP, often without being required to install any tools on their computer (Mather, Kumaraswamy, & Latif, 2009, p. 19; ISACA, 2009, p. 5). Table 4-2 lists the minimum criteria for a PaaS solution according to Mather, Kumaraswamy & Latif (2009, p. 20).
3. Cloud Infrastructure as a Service – CSPs provision fundamental computing resources on the cloud. These resources can include processing power, storage, networks and other resources. Details of the resources, such as location, security and scaling, are abstracted from the user. This model is similar to utility computing. With the IaaS model, however, the CSP is in full control of the infrastructure. With utility computing, the user may control the geographic location of the infrastructure and what runs on each server (Mather, Kumaraswamy, & Latif, 2009, p. 22).

Minimum PaaS solution requirements

At minimum, a PaaS solution should:

- Be browser based.
- Provide a high-productivity IDE (Integrated Development Environment) running on the actual target delivery platform so that debugging and test scenarios run in the same environment as production deployment.
- Provide integration with external web-services and databases.
- Provide comprehensive application and user activity monitoring to enable developers to make informed application improvements.
- Automatically provide built-in scalability, reliability, security and multitenancy capabilities.
- Support collaboration throughout the software development life-cycle in a manner that is secure and protects associated intellectual property.
- Support pay-as-you-go metered billing.

(Mather, Kumaraswamy, & Latif, 2009, p. 20)

Table 4-2 Minimum PaaS solution requirements

The various service models discussed above have different levels of security responsibilities and capabilities for users (Cloud Security Alliance, 2009b, p. 19). The type of cloud computing service model implemented by an organisation is, therefore, likely to impact the degree of control the organisation has over the resources associated with the solution. This is also true for the various cloud computing deployment models discussed in the next subsection. The implications of this are further highlighted at the end of the next subsection.

4.2.1.3 Cloud deployment models

The way clouds are deployed can typically be categorised into one of the following four deployment models:

- Private cloud – a cloud that is operated for a single organisation. The cloud will be managed either by the organisation or by a third party (outsourced private clouds) and can exist either on or off premise (Liu, et al., 2011). The organisation will carry the costs for implementing and managing the cloud. This does, however, provide a high level of control and transparency and can, therefore, make it simpler to effectively govern the cloud (Mather, Kumaraswamy, & Latif, 2009, p. 24; ISACA, 2009, p. 5).
- Community cloud – a cloud that supports a community of users. Like a private cloud, it can be managed either by the organisations or by a third party of their choice. It can also be on or off premise.
- Public cloud – a cloud that can be used by the general public or a large industry group. The cloud is owned and managed by a third-party vendor. A user, therefore, has limited control.
- Hybrid cloud – two or more clouds that are bound in a manner that allows data or applications portability. An organisation may, for example, decide to run certain applications in a public cloud but keep others that use more sensitive information or are more central to the operation of the organisation in a private cloud (Mather, Kumaraswamy, & Latif, 2009, p. 25). Figure 4.2 depicts an example of a hybrid cloud.

The choice of deployment model and service model will affect an organisation's security considerations and the level of control that it can directly exercise over resources. With SaaS, the cloud user has a certain level of control at the application level. The CSP has control over the middleware and operating system (OS) layers. With IaaS, cloud users have control over the virtualized OS that they run on the cloud, as well as over whatever middleware layer and

application layer resources run on the OS. The CSP controls the environment that hosts the virtual operating systems (Liu, et al., 2011).

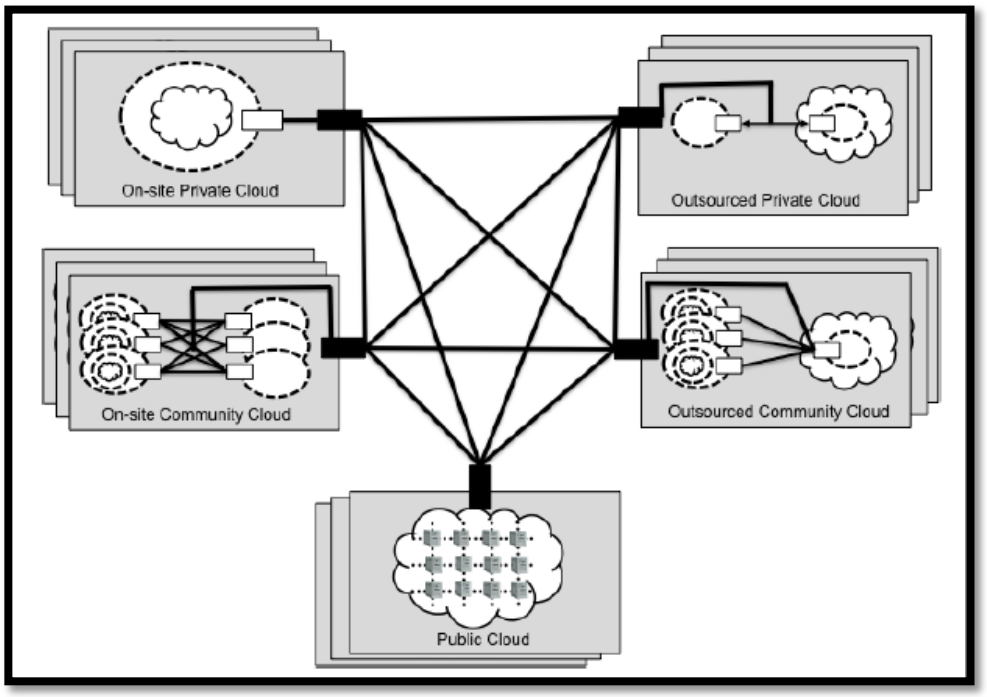


Figure 4.2 Example of a hybrid cloud computing deployment model (Liu, et al., 2011)

Similarly, Figure 4.3 illustrates the effect that the choice of cloud computing deployment model has. Cloud users obviously have more direct control over resources when using private clouds than when using public clouds. As can be seen from Figure 4.4, the level of direct control correlates with the level of assurance.

This section has clearly defined cloud computing and has shown that cloud computing can be explained from either a technical or non-technical perspective. In addition, cloud computing has been explained in terms of its essential characteristics, service models and deployment models. From this description it should be clear that cloud computing is a broad term that can encompass many different types of applications deployed in various ways. The service and deployment models that are used to implement a cloud computing solution at a specific organisation will have significant implications regarding the levels of direct control that such an organisation has over the resources associated with the solution. Making wise choices regarding how cloud computing solutions are to be implemented at organisations is, therefore, important in managing the information and other resources associated with the cloud computing solution.

To further promote a clear understanding of cloud computing, NIST provides a reference architecture for cloud computing. This is discussed in the next section.

4.2.2 Cloud computing reference architecture

In addition to providing a widely accepted definition for cloud computing, NIST also has produced a reference architecture and taxonomy for cloud computing. The reference architecture aims to provide a basis from which characteristics, uses, requirements, structures and standards for cloud computing can be discussed and explored (Liu, et al., 2011, p. 2).

A high-level overview of the reference architecture is depicted in Figure 4.5. As can be seen from the diagram, the architecture depicts five main actors in cloud computing and their roles and activities.

The actors and some of their key roles and activities are listed and explained as follows:

- Cloud consumers – a cloud consumer is either a person or organisation that uses cloud computing services. The cloud consumer can access these services either from a cloud provider directly or through a cloud broker. The consumer enters into a business relationship with a cloud provider and should have a service level agreement (SLA) with the cloud provider. The consumer can access various types of cloud computing services in the form of SaaS, PaaS or IaaS.
- Cloud providers – a cloud provider is a person or organisation that makes cloud computing services available to cloud consumers. Figure 4.5 highlights some of the main roles and responsibilities of cloud providers. These include service orchestration, service management and providing security and privacy. These will be briefly listed here, but a full description is beyond the scope of this work. Service orchestration is depicted in the first, white rectangle inside the cloud provider rectangle in Figure 4.5. Service orchestration "refers to the composition of system components to support cloud providers activities in arrangement, coordination and management of computing resources in order to provide cloud services to Cloud Consumers" (Liu, et al., 2011, p. 12). Cloud providers must also conduct service management. As can be seen in Figure 4.5, this involves more than provisioning and configuring cloud computing services. Rather, it also includes business support activities (such as pricing and customer management) and ensuring interoperability and portability of services. Cloud providers must also ensure the security and privacy of the services they offer. Both cloud consumers and cloud providers, though, have some responsibility for ensuring the

privacy of cloud consumer information. Cloud consumers remain ultimately responsible for the security and privacy of their organisation information.

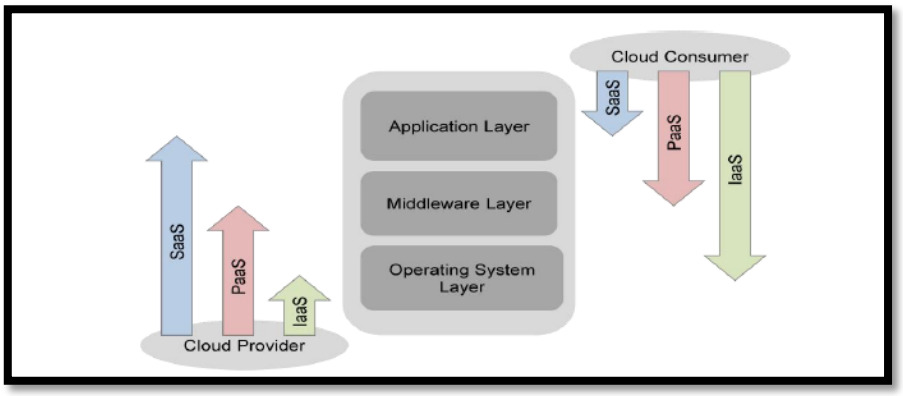


Figure 4.3 Level of control affected by service model (ENISA, 2009a)

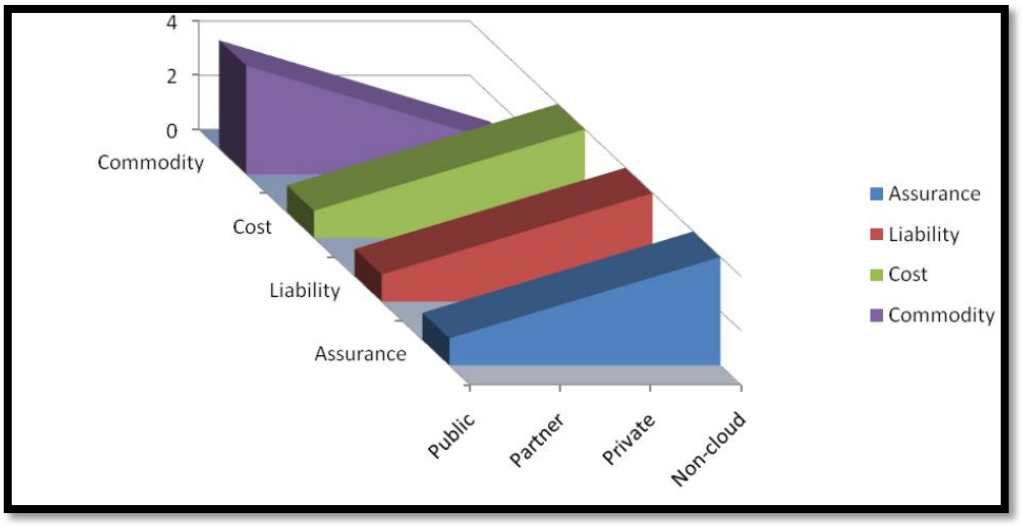


Figure 4.4 Effects of cloud computing deployment model (ENISA, 2009a)

- Cloud brokers are entities that can act as intermediaries between cloud consumers and cloud providers. NIST describes three categories of service offered by cloud brokers: 1) service intermediation - where a broker sits between the consumer and provider and enhances the service in some way. Examples of enhancements could include access to management or performance reporting. 2) Service aggregation and 3) service arbitrage both have to do with a broker aggregating services from different cloud providers into a new service.

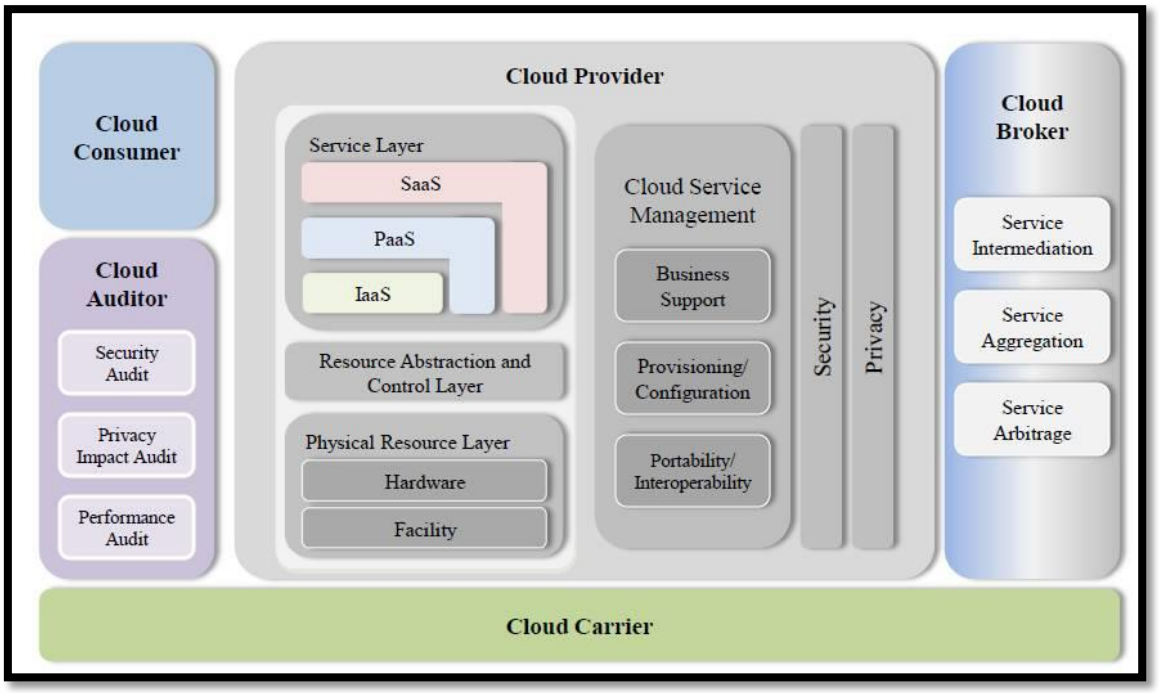


Figure 4.5 Cloud computing high-level reference architecture (Liu, et al., 2011)

- Cloud auditors are tasked with evaluating whether cloud computing controls are adequate to meet the requirements placed on an organisation by standards, policies or regulations. As shown in Figure 4.5, various types of audits can be conducted. These include security, privacy and performance audits.
- Cloud carriers are entities that provide connectivity between cloud consumers and providers. These are usually network and telecommunication carriers or organisations that provide "physical transport of storage media such as high-capacity hard drives" referred to as transport agents (Liu, et al., 2011, p. 9).

The information in the chapter so far has defined and explained cloud computing and the various ways that it can be used in organisations. It has also highlighted terms associated with cloud computing that will be used throughout the rest of this work. Now that it has been established what cloud computing is, the next part of this chapter describes the impact of cloud computing.

4.3 Cloud Computing Impact

"Like the Internet itself, the Cloud is a disruptive technology that challenges existing business models, institutions, and regulatory paradigms" (Nelson, 2009, p. 76). This quote illustrates the marked impact that some expect cloud computing to have on organisations. Although there may have been much hype regarding cloud computing, this section discusses several factors that highlight the real impact of cloud computing on organisations internationally.

Cloud computing has been generating a lot of interest for some time already. Figure 4.6 shows that since 2010 there have been more searches for "cloud computing" than for "information security", "mobile computing", or even "Barak Obama" on Google. Cloud computing is clearly a term that people are interested in, and organisations around the world are adopting cloud computing.

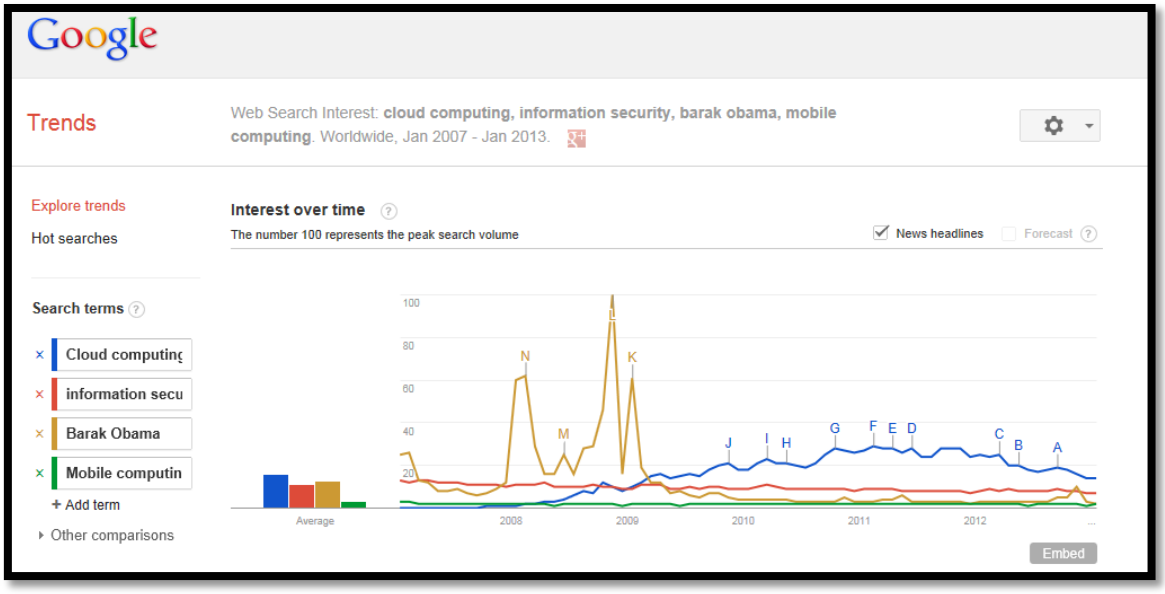


Figure 4.6 Google Trend results for cloud computing searches since 2007

Surveys and analyst predictions about cloud computing indicate that it is a computing model that should not be overlooked as a mere new hyped technology. According to the results of a survey by KPMG (Chung & Hermans, 2010) "…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." Many organisations are already using some form of cloud computing or have plans to do so within the next year (Chung & Hermans, 2010; Pricewaterhouse Coopers,

2012; Focus Market Research, 2011). According to a survey by Norhtbridge, 82 percent of participating organisations are already using SaaS (2012). The Cloud Industry Forum "expect that by the end of 2013, over 75 percent of UK businesses will be using at least one cloud service formally and 80 per cent of current cloud users will have increased their spend in this model of IT delivery" (Cloud Industry Forum, 2012, p. 2). Michael Pearl, the US cloud computing leader at PwC, estimates that the global market for cloud computing will be more than $241 in 2020 (Pearl, 2012).

Not only are individual organisations using cloud computing, but government initiatives are also promoting its use. The American government has adopted a "cloud first policy" encouraging agencies to assess whether they could achieve the benefits of cloud computing before looking for other potential solutions (Kundra, 2011). In addition, Europe is driving the use of cloud computing by government agencies and includes plans for it in the "Digital Agenda for Europe" (European Commission, 2012). The Australian government also has a strategy for promoting the use of cloud computing (Australian Government, 2013).

The work done by reputable international authorities may also indicate the influence that cloud computing is expected to have on organisations. For example: The National Institute of Standards and Technology (NIST) is involved with a cloud computing project (NIST, 2009). As seen previously in this chapter, it has published, amongst other things, a comprehensive cloud computing definition (Mell & Grance, 2009). The European Network and Information Security Agency (ENISA, 2009a), ISACA (2009) and the Jericho Forum (2009) have been involved with cloud computing research. Furthermore, this chapter has quoted work by the Cloud Security Alliance (CSA). The mission statement of this group is: "to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing" (Cloud Security Alliance, 2009a). Much of the work by bodies such as these regarding cloud computing guidance will be highlighted later in this chapter. Would all these reputable groups be involved with cloud computing research if they didn't believe that it will have an impact?

A glance at the CSA's list of corporate members is also insightful. Companies such as Microsoft, Google, Novell, Dell, Cisco, Intel, McAffe, Symantec and many others are CSA members (Cloud Security Alliance, 2009a). This signifies that these companies are all, at a minimum, interested in cloud computing. There are, however, also several companies that are acting as cloud service providers (CSPs). Mather, Kumaraswamy and Latif list some

CSPs. These include Amazon, Google, Microsoft, Salesforce.com and Sun (Mather, Kumaraswamy, & Latif, 2009, p. 214). The investment that companies like this are willing to make to enter the cloud market suggests that they too believe that cloud computing will have a marked impact on the way organisations do business.

It is impossible to predict what will happen with cloud computing. Cloud computing is not necessarily a computing paradigm, which is going to single-handedly transform organisations. Using cloud computing services may not even be a viable option for some organisations. Research by reputable bodies, work by well-known IT companies, like Microsoft and Google, and analyst predictions and survey results are, however, some of the factors that seem to indicate that cloud computing is and will continue having an impact on organisations. Cloud computing is, therefore, a relatively new IT development worthy of consideration (Von Solms & Viljoen, 2012).

Cloud computing is in its infancy, though. According to a survey by ISACA and CSA, the potential of cloud computing for organisations is widely recognised, but PaaS and IaaS are still in the early stages of market maturity (as shown in Figure 4.7). SaaS is just emerging from the infancy stage and it is believed that it will still be about two years before it will be firmly in the growth stage of market maturity. The report about the survey concludes that, for cloud computing to reach market maturity, there needs to be a thorough understanding of what "benefits are provided, what risk must be understood and addressed, and what basic concerns about the offering need to be mitigated" (ISACA & CSA, 2012). The following two sections discuss some opportunities and risks associated with cloud computing.

4.4 Cloud Computing Benefits

This chapter has thus far discussed what cloud computing is, how it works and how it is affecting organisations. Understanding the potential benefits of cloud computing helps to clarify the importance of this computing model for organisations. Some of the opportunities related to cloud computing are briefly listed in this section.

There are many benefits purportedly associated with cloud computing. Some of these include ubiquitous access (Iyer & Henderson, 2010), greener computing (Breeding, 2009), improved information sharing (Porta, Karimi, Plakskon, & Sharma, 2009, p. 3) and improved security (Du & Cong, 2010; Nawrocki, 2011). This section does not discuss all of these potential opportunities. Rather, it highlights three general benefits that have been found to be greatly

influential in promoting the adoption of cloud computing (Pricewaterhouse Coopers, 2012, p. 19; ISACA; CSA, 2012, pp. 16,17). They are listed and discussed below.

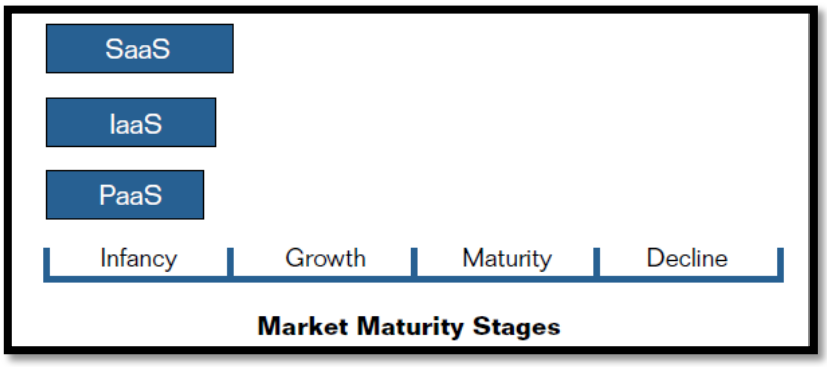


Figure 4.7 Cloud computing market maturity (ISACA & CSA, 2012)

- Cost saving – with cloud computing organisations pay only for the IT resources they use. Organisations do not have to invest in costly hardware and software, which they may not always use fully. Instead, they can use the resources provided by CSPs on a pay-as-you-go basis, or even free services. This model also reduces the costs associated with resource wastage (ISACA, 2009, p. 6; Nelson, 2009; Fingar, 2009, p. 27; Porta, Karimi, Plakskon, & Sharma, 2009, p. 3; Mather, Kumaraswamy, & Latif, 2009, p. 26; Horwath, et al., 2012; Farber, 2009).
- Increased business responsiveness and efficiency – with cloud computing some administrative concerns (such as licensing, updates and hardware maintenance) may become the CSP's responsibility. This allows in-house IT personnel to focus more on business problems and opportunities (ISACA, 2009, p. 6). The reduced costs associated with new projects may make them less risky. This may lead to better business responsiveness, flexibility and innovation (ISACA, 2009, p. 4; Porta, Karimi, Plakskon, & Sharma, 2009, p. 3; Phillips, 2009; ISACA, 2012b; Shivakumar & Raju, 2010).
- Scalability – because of rapid elasticity, resources are automatically provisioned according to need. This allows organisations to access resources through cloud computing extensively during periods of high demand without resource wastage or additional capacity planning costs (Porta, Karimi, Plakskon, & Sharma, 2009, p. 3; ISACA, 2009, p. 6; Fox, 2009, p. 158; Phillips, 2009; Iyer & Henderson, 2010).

This section has listed some of the potential benefits of cloud computing. Whether or not organisations reap these benefits will depend much on factors such as the cloud computing solutions they choose and how they implement such a cloud-based solution.

As concluded by Von Solms and Viljoen (2012), cloud computing "users will have to experience real benefits associated with cloud computing for this computing model to be widely adopted." Surveys show that organisations generally perceive a high likelihood of constraints (such as cost and rigidity) being reduced by the use of cloud computing. If organisations do not achieve any of the real benefits they are anticipating while truly implementing cloud computing solutions, it would negatively impact the perceived value of cloud computing. This would negatively impact cloud computing adoption in general (Von Solms & Viljoen, 2012).

As noted earlier, the adoption of cloud computing is likely to depend largely on how important cloud computing challenges are dealt with. The following section addresses cloud computing challenges.

4.5 Cloud Computing Challenges

As has been made clear in the previous two sections, the advantages associated with cloud computing, the rate at which it has already been adopted and the analyst predictions for future cloud growth, makes it apparent that cloud computing is a paradigm that is likely to affect many organisations in the near future. As a nascent system, there are, nevertheless, many challenges that still need to be addressed for cloud implementation to be used in a secure and optimal manner, with a true, wide scale and sustainable impact (Mather, Kumaraswamy, & Latif, 2009, pp. 30, 245; Schmelzer, 2009; Cloud Security Alliance, 2010; Cloud Security Alliance, 2009b; Modi, 2009; Wang, 2009).

There are various significant concerns regarding the use of cloud computing. The CSA has categorised some of these areas of concern. It also provides guidelines for security in each of these areas (Cloud Security Alliance, 2009b, p. 26). The domains of concern identified by the CSA are listed and discussed below.

- Governance and risk management: Cloud computing results in a loss of direct control of information by organisations, affecting the way their governance mechanisms (structures, processes, systems and controls) are implemented. Organisations making use of cloud computing should ensure that appropriate adjustments are made when

using cloud computing (Cloud Security Alliance, 2009b; Kobielus, 2009). As will be highlighted in the following points of concern, cloud computing introduces many potential risks to an organisation. Organisations must ensure that these risks are properly managed (Horwath, et al., 2012).

- Legal and electronic discovery: There is a need to consider potential legal issues associated with the use of cloud computing. There are legal questions pertaining to cloud computing, such as questions about legal liability and how different laws in diverse geographic areas affect cloud computing (ISACA, 2009, p. 7). The CSA discussion in this domain includes topics such as security breach disclosure laws, regulatory requirements, and international laws (Cloud Security Alliance, 2009b, p. 27).
- Compliance and audit: An important challenge organisations using cloud computing face is that of ensuring and proving compliance or, as it is referred to in this work, conformance (Mather, Kumaraswamy, & Latif, 2009, p. 167; ISACA, 2009, p. 7; Wood, 2009). Audit (or assurance) and conformance requirements are usually met by monitoring whether there are policies, procedures, processes and systems in place and being implemented to satisfy requirements that may be driven by, amongst other things, business requirements and laws and regulations (Mather, Kumaraswamy, & Latif, 2009, p. 167). This area is one of the main challenges addressed in this work. As described in Chapter 3, meeting the challenges of conformance and assurance of cloud computing forms an important part of improving the overall governance of cloud computing. As seen earlier in this list, governance of cloud computing is also commonly regarded as a challenge.
- Information lifecycle management: Issues of concern in this domain include identification and control of data in the cloud, controls for data loss and issues of determining responsibility for data confidentiality, integrity and availability.
- Portability and interoperability: Independence from CSPs, interoperability and portability of data are important characteristics that can influence organisational cloud adoption (Mather, Kumaraswamy, & Latif, 2009, pp. 31-32). As stated earlier in this chapter, organisations may choose to use a hybrid deployment for the cloud. With this model, various business applications may reside on different cloud implementations. One application may be deployed on a private cloud. Another may be hosted by a certain CSP and a third may be hosted by another CSP, for example. Standards of

interoperability will be necessary to ensure that the integrity and consistency of an organisation's information and processes are maintained (Mather, Kumaraswamy, & Latif, 2009). Users should also be free to easily change from one CSP to another for various reasons. A customer may, for instance, find that they are not happy with the level of service provided by a certain CSP. The ability to port information from one CSP to another then becomes important. Many CSPs use unique application programming interfaces (APIs), making interoperability and portability between clouds difficult. There are efforts to standardise APIs, but it is worth noting that market incentives for CSPs tend to cause them to lock customers into their clouds (Mather, Kumaraswamy, & Latif, 2009, pp. 16-17).

- Traditional Security, Business Continuity and Disaster Recovery: Cloud computing will likely introduce new risks to organisations and will influence processes and procedures to implement security, business continuity and disaster recovery (Cloud Security Alliance, 2009b, p. 27; Pacella, 2011). Better enterprise risk management models are therefore necessary (Cloud Security Alliance, 2009b, p. 27). CSPs should understand the role that they are required to play in terms of disaster recovery, and recovery time objectives should be stated in contracts (ISACA, 2009, p. 7).
- Data center operations: Cloud users will have the challenge of evaluating CSPs data center architecture and operations to identify characteristics that could influence the ability to offer long-term on-going services (Cloud Security Alliance, 2009b, p. 27).
- Incident response, notification and remediation: Organisations using the cloud also have the challenge of adjusting their incident handling program to ensure proper incident detection, response, notification and remediation to include incidents within the cloud (Cloud Security Alliance, 2009b, p. 28).
- Application security: Organisations have to decide which applications are suitable for cloud deployment and ensure that all such applications are secure (Cloud Security Alliance, 2009b, p. 28; Lanois, 2010).
- Encryption and key management: There are issues involved in both protecting access to resources and protecting data.
- Identity and access management: Before moving to the cloud, organisations have to consider issues related to identity control in the cloud and evaluate their readiness to "conduct cloud-based identity and access management" (Cloud Security Alliance, 2009b, p. 28).

- Virtualization: There are various security issues associated with virtualization. The CSA addresses items such as risks associated with multitenancy, VM isolation and VM co-residence.

As stated earlier, it is vital that these issues are dealt with properly if cloud computing is to deliver the benefits people hope for (Mather, Kumaraswamy, & Latif, 2009, pp. 30, 245; Schmelzer, 2009; Cloud Security Alliance, 2010; Cloud Security Alliance, 2009b; Modi, 2009; Wang, 2009). In this regard, much work has been done by various bodies to provide guidelines to address some of these concerns.

The remainder of this chapter will highlight some guidance provided by reputable bodies that can assist with addressing various cloud computing related concerns. Firstly though, the importance of such standards is discussed in the next section.

4.6 Cloud Computing Guidelines

Guidelines for cloud computing can assist managers with the task of deciding how to proceed with cloud computing in their organisation confidently. The sheer volume of guidance becoming available for cloud computing may make the task of finding and selecting guidelines for the adoption and implementation of cloud computing more complicated than it may seem. There are numerous cloud computing standards and guidelines available and under development. There are also numerous bodies working on these standards and guidelines, including government bodies, standards organisations and academics. NIST hosts a wiki that lists and describes work on cloud computing standards. Here the work of about fourteen bodies is listed. Another wiki that lists cloud computing standards names an additional three bodies. In addition to these bodies, academia, industry and government bodies are also involved in research for cloud computing standards and guidelines. A Google search for "cloud computing guidelines" on 25 January 2013 resulted in about 83,300 results in 0.22 seconds. A similar search for the phrase "cloud computing standards" resulted in 437,000 results and a search for "cloud computing framework" resulted in about 540,000 results.

This section summarises some guidance that is provided by reputable IT governance bodies. Before doing this, though, the next subsection briefly highlights the importance of standards and guidelines for IT in general and cloud computing in particular.

4.6.1 Value of guidelines

Carrying out a complicated task is often less daunting when provided with a clear set of guidelines. In the field of IT, when organisations adhere to best practice guidelines and standards they avoid wasting time and resources reinventing the wheel with their approach to handling IT. By adhering to best practice guidelines, organisations can be more confident that they are following an approach that is effective and efficient. Effectively being guided by best practice thereby increases assurance that things are being done the right way. The previous chapter highlighted the relationship between best practice, assurance and governance in more detail.

Following best practice guidance also enables managers to demonstrate due diligence. Due diligence is defined as "reasonable steps taken by a person to avoid committing a tort or offence" (OECD, 2004). As explained in the OECD principles for governance, a person can show due diligence by demonstrating that he or she has behaved in a way that "a reasonably prudent person would exercise in similar circumstances" (OECD, 2004). Properly following a set of guidelines by a group of experts gives directors and managers the ability to claim due diligence. A standards-based, best practice approach to the governance of IT is, therefore, the wise course to follow.

As with IT in general, in the relatively new field of cloud computing, standards and reputable guidelines can also help management carry out their responsibilities. As with other IT standards and guidelines, cloud computing guidelines help management understand cloud computing, its implications for organisations and their responsibilities regarding cloud computing. In addition, standards and best practice guidelines provide aid in the process of deciding about the adoption and implementation of cloud computing solutions. Not only would managers benefit from guidelines that assist them with these tasks, but they would also benefit from guidelines that promote confidence in adopting a relatively new IT paradigm. Guidelines that provide assurance for cloud computing are, hence, also beneficial for organisations.

Standards and guidelines for cloud computing have clear value for organisations. There are, however, a plethora of cloud computing standards and guidelines available. The next subsection highlights this fact and describes some reputable guidance available for cloud computing.

4.6.2 What is available?

There are various types of cloud computing guidelines available. These guidelines range from very specific to very general, from very technical to very conceptual. Guidelines can be broadly categorised into two types for the purpose of this discussion, though. Borenstein and Blake highlight these two types of standards: prescriptive and evaluative (2011). They describe prescriptive standards as those which give exhaustive details about how things work. SMTP and TCP are examples of prescriptive standards. Evaluative standards, on the other hand, provide a uniform manner of assessing how well something works. An example of an evaluative standard is ISO/IEC 27001. This work will describe some evaluative cloud computing guidelines.

As stated previously, there are various bodies (such as academia, industry and governance bodies) involved in producing guidelines for cloud computing. This work does not attempt to review the works of all of these bodies. Neither does it attempt to provide an exhaustive list of cloud computing standards that may be relevant to directors or management. It only discusses the influential work about cloud computing by some reputable IT governance and cloud computing bodies. The following subsection motivates this decision by explaining some of the benefits of this approach. Firstly though, the remainder of this subsection briefly describes some of the findings of a review of academic literature regarding frameworks for cloud computing.

On 9 March 2014 the online research database EBSCOhost, was used to search scholarly (peer reviewed) publications for papers with the keywords "cloud computing" and "framework." This search yielded 210 results. Many of these papers describe frameworks for aspects of cloud computing that are not related to areas of research covered in the scope of this work. In order to illustrate this, some of these are listed below:

- Rana and Fakrudeen (2011) propose a cloud computing framework and service model which aims to assist visually impaired computer users to work with services and applications made available over the internet.
- A framework for personal genome analysis in the cloud describes how cloud computing can be used to conduct genomic analysis in a manner that has not been feasible for smaller research laboratories without vast resources at their disposal (Evani, et al., 2012). There are a number of other frameworks that similarly describe how cloud computing can be used to provide new opportunities for

developing or improving applications and solutions ranging from games to analysis of massive data (Shea, Liu, Ngai, & Cui, 2013; Ding, Xu, & Yang, 2013; Bahga & Madisetti, 2012; Arora, Millman, & Neville, 2013; Brandic, et al., 2011; Fujioka, et al., 2012).

- There are some papers that apply cloud computing to specific contexts such as human resources (Yeh, 2012), small and medium enterprise (Wei, 2010) and business intelligence (Gash, Ariyachandra, & Frolick, 2011).

The preceding list of papers, clearly does not directly relate to the topic of assuring the conformance of cloud computing. The search also yielded papers describing frameworks for cloud computing that could contribute to aspects of assuring the conformance of cloud computing though. In order to illustrate this, two such works are described below:

Kalyvas, Overly and Karlyn (2013a, 2013b) provide a "practical framework for managing cloud computing risk." This framework essentially consists of various recommendations for managing risks associated with cloud computing. The recommendations focus on making sure that contracts with CSPs are properly managed. Although valuable, this work does not fully address the problem of assuring the conformance of cloud computing. Managing contracts is an important part of the governance of cloud computing. Similar issues regarding the management and negotiation of contracts with CSPs are addressed by reputable IT governance bodies. Some of these recommendations are highlighted in Section 4.6.5.

Abbadi (2013) describes a "framework for establishing trust in cloud provenance." Trust and assurance are closely linked subjects. Abbadi's framework however, does not address the field entire of trust in cloud computing but rather focusses on trust in cloud provenance. Provenance has to do with data about where other data originates.

Although not yielded as part of the results from the search of EBSCOhost, Martens and Teuteberg (2011) describe a reference model to be used for risk and compliance management in cloud computing that can be linked with this work. This reference model addresses several of the same areas of interest as this work. It describes how cloud-computing-related risk and compliance issues can be perceived and explained. It also hints to mechanisms (such as key performance indicators and dashboards) that can be used to manage risk and compliance in cloud computing. The purpose of the reference model is to "to present a first proposal for the focused research field" (Martens & Teuteberg, 2011). Although it provides a good theoretical overview of the field of risk and compliance management in cloud computing,

it does not provide a complete solution for the problems in this area. The reference model also addresses the field of management, rather than the more overarching field of governance.

The frameworks described in the preceding paragraphs contribute to the field of cloud computing governance and can contribute to the overall task of assuring the conformance of cloud computing. Although addressing part of the problem of assuring the conformance of cloud computing, such frameworks do not address the problem as a whole. In addition, none of the existing frameworks provide specific and detailed guidelines for cloud-based email at South African higher education institutions. Guidance found in these frameworks can also often be found in best practice guidelines from reputable IT governance bodies. There are benefits associated with using guidelines from reputable IT governance bodies instead of guidance from academic work as a foundation for a framework for assuring the conformance of cloud computing in general, and cloud-based email specifically. Some of these benefits are discussed in the next section.

4.6.3 Value of guidelines by reputable IT governance bodies

Guidance for cloud computing from recognised and established IT governance bodies may be valuable for organisations for some of the following reasons:

- Various IT governance bodies have been producing guidelines that have been used successfully for a number of years by organisations internationally. They have, therefore, become reputable and trustworthy advisors in the field of IT, and it would be wise to monitor any work that these bodies would be involved in with cloud computing specifically.
- An additional reason that cloud computing guidance from such bodies is useful is that these guidelines can be used in conjunction with the existing guidelines for IT governance, which many organisations may already be using when considering the adoption of cloud computing services.
- Guidelines form reputable IT governance bodies assist and are relevant to the board and top management. They help these individuals ensure that adoption and use of cloud computing is properly governed. Although more detailed, technical guidelines specific to certain technologies are vital, they are not necessarily of direct interest or concern to the board of directors or top management. What should be of concern to these individuals is that they direct and monitor the use of high-level guidelines and

standards for the governance of IT. These guidelines in turn direct that there are processes in place to make sure that standards and guidelines at a more specific level of detail are used and enforced. The guidelines from these bodies are, therefore, not technical or technology or vendor specific.

- In addition, guidelines from these bodies are most likely to be adopted by organisations. Adherence to guidelines from these bodies may even be a mandate for the organisation.
- Finally, as explained earlier, adherence to guidelines from such reputable bodies facilitates due diligence.

From the above, it should be clear why it is worth considering the work on cloud computing by reputable bodies involved in the promotion of IT governance guidelines and frameworks. The approach to base the framework for assuring the conformance of cloud-based email on guidelines from these bodies has thus been chosen for this work. There are a number of reputable IT governance bodies involved in producing guidelines for cloud computing. Only the cloud computing specific guidance from the bodies listed below will be analysed in this work, though.

- ISACA - ISACA provides guidance for IT governance, information security and IT audit and assurance. Well known governance frameworks such as COBIT and Val IT are developed by ISACA (ISACA, n.d.).
- ISO – International Organisation for Standardization. ISO develops voluntary international standards through global consensus (ISO, n.d.).
- NIST - National Institute of Standards and Technology. NIST is a federal agency within the United States of America's Department of Commerce. It promotes the use of standards and technology to promote industrial competitiveness of the USA (NIST, 2012).
- COSO – Committee of Sponsoring Organisations of the Tradeway Commission. COSO develops "frameworks and guidance on enterprise risk management, internal control and fraud deterrence" (COSO, n.d.).

Within the guidance from the bodies listed above, reference is made to guidance from the following bodies: CSA, ENISA, CIO council and Commission of the European Communities, Expert Group on Cloud Computing. Some guidance from the above-mentioned bodies will be highlighted in the next subsection.

Since cloud computing is a relatively new field in IT, it is not surprising that a good deal of the information presented by these bodies serves to clarify what cloud computing is and its potential benefits and risks. This information has already been discussed.

Several areas in which cloud computing related guidance is provided will be discussed in this section. These areas include guidance regarding the selection of cloud computing solutions and the governance of cloud computing.

4.6.4 Selecting cloud computing solutions

Although there are significant opportunities attributed to the use of cloud computing, each organisation has the responsibility to investigate whether the adoption of a cloud computing solution would be appropriate for an organisation's specific circumstances and requirements.

A number of the cloud computing guidelines researched in this work include processes and models to help managers of organisations make decisions regarding the adoption of cloud computing. Some of these include:

- The CSA provides a ***simple framework for assessing initial cloud risks.*** The framework aids with making security decisions for cloud computing implementations (Cloud Security Alliance, 2011, pp. 8-9).
- ENISA provides a ***model for choosing resilient and secure*** cloud computing solutions (Cattedu, 2011).
- Additionally, ISACA describes a ***four step process*** to assist with a decision regarding the use of cloud computing (ISACA, 2012c). This process includes some of the recommendations highlighted in the other guidelines. It is described in the following few paragraphs in more detail.

Although each of the above-mentioned methodologies for selecting cloud computing solutions differ in their approach, they all cover similar aspects that should be considered. The four step approach described by ENISA is, therefore, described below as an illustrative example of a methodology for cloud computing solution selection.

The four steps include:

- Preparation of the internal environment - It is recommended that an organisation assess how a move to the cloud would affect and be affected by: existing organisation principles, policies and frameworks; processes; organisational structures; culture, ethics

and behaviour and people skills and competencies. They also recommend a consideration of the costs and benefits of moving to the cloud.

- Selection of the cloud service model - A decision tree is presented to help managers decide which service model (SaaS, PaaS or IaaS), if any, would best suite their organisation.
- Selection of the cloud deployment model - Provides a decision tree to assist in deciding whether a public or private cloud would best meet needs or whether the organisation may be in a better position not using a cloud computing solution.
- Selection of the cloud provider - It is recommended that established, trusted CSPs are considered and that the location of the CSP be taken into account, as this may affect laws pertaining to the decision. The standards and business needs must also match the service provided by the CSP.

Various other guidelines may enable managers to weigh up the cost and benefits of cloud computing adoption. ISACA also assists in making a decision regarding the potential value of a cloud computing solution in the form of a framework for the calculation of return on investment (ROI) of cloud computing (ISACA, 2012a). It describes why it is difficult to calculate ROI with cloud computing and lists and explains tangible and intangible costs and benefits of cloud computing. In addition, it provides a framework that outlines guidelines for various phases that assist managers in calculating ROI.

The guidance referred to thus far has assisted managers in understanding cloud computing and selecting an appropriate cloud computing solution for their organisation. NIST refers to and elaborates upon a decision framework that goes beyond the selection of a solution and touches upon aspects of provisioning and managing a cloud computing solution. This high-level framework, originally described by the CIO Forum, is shown diagrammatically in Figure 4.8 (NIST, 2011b; Kundra, 2011). The three steps in the decision framework for cloud migration are mapped to areas that are described as priority areas of interest for cloud computing by NIST. From this mapping, NIST has determined a number of considerations in each of the steps given in the decision framework. In addition to the considerations, NIST also provides a set of case studies that refer to the steps in the framework.

This subsection has highlighted some guidance provided by reputable bodies related to making decisions about the adoption of a cloud computing solution. The next two

subsections now highlight the more overarching topics of governance and assurance in cloud computing.

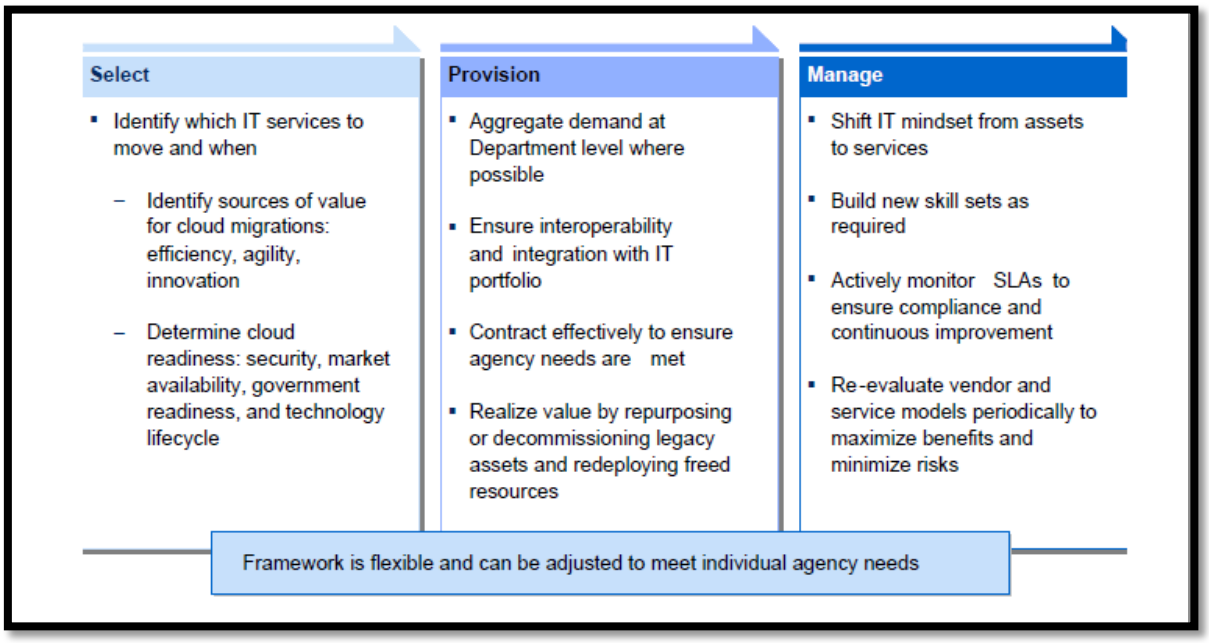


Figure 4.8 Decision framework (Kundra, Federal cloud computing strategy, 2011)

4.6.5 Governance and cloud computing

As seen in Chapter 3, governance is defined by ISACA as "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved and ascertaining that risks are managed appropriately" (ISACA, 2011). ISACA states that the two key objectives of IT governance ensure that IT adds *value* to the business and that IT related *risks* are properly managed. This subsection will highlight various guidelines regarding enterprise governance of cloud computing. The previous subsection has highlighted several guidelines and models that organisations can use to ensure that they select cloud computing solutions that add value to organisations. This subsection, therefore, focusses primarily on the second main objective of IT governance for cloud computing – risk management. Firstly, though, more general governance guidelines for cloud computing are described.

- *Cloud computing must be governed within context of enterprise IT governance program using standards and best practice guidelines.*

Many of the bodies considered here, which are responsible for producing IT governance frameworks, recommend and describe how existing IT governance frameworks can be

tailored and applied to cloud computing. ISACA describes how ***COBIT 4.1 can be applied to cloud computing*** (ISACA, 2011). Likewise, COSO recommends that the ***COSO ERM framework*** be used when dealing with cloud computing (Horwath, et al., 2012).

ISO is also developing standards based on ISO/IEC 27002, specifically for cloud computing. These will be ***ISO/IEC 27017*** (ISO, 2012b) and ***ISO/IEC 27018*** (ISO, 2012a). The CSA also explains a "***Trusted Cloud Initiative Reference Architecture***" which is based on various best practice frameworks for IT (CSA, 2011). The CSA defines the architecture as "both a methodology and a set of tools that enable security architects, enterprise architects, and risk management professionals to leverage a common set of solutions" (CSA, 2011).

- *To ensure cloud computing is properly governed, roles and responsibilities should be assigned to different levels of management.*

In the definition for governance given previously, the importance of this requirement is highlighted. If governance is, in part, "the set of responsibilities and practices exercised by the board and executive management …" it is clear that, for proper governance of cloud computing, these managers will need to be aware of their responsibilities. COSO provides a ***list of the responsibilities*** of various managers, such as the board of directors, the chief executive officer, chief financial officer, chief legal officer, chief information officer and the chief internal auditor (Horwath, et al., 2012). COSO also provides ***a list of questions that the board of directors and managers should consider*** regarding cloud computing.

- *Organisations should establish business goals and business cases for cloud computing.*

ISACA provides a set of steps that organisations can use to determine their cloud computing business goals (ISACA, 2011). This includes activities such as ensuring that the use of cloud computing aligns with the business strategy, determining the benefits and risks that are anticipated from a cloud computing solution and evaluating the value that is to be achieved by implementing such a solution.

- *There should be a set of controls for cloud computing*

ISACA defines a control as "The means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of an administrative, technical, management or legal nature. Also used as a synonym for safeguard or countermeasure" (ISACA, 2010b).

Some of the guidelines listed above have already highlighted controls that organisations should use for cloud computing. In fact, the guidelines themselves are controls. ISACA has **mapped control objectives from COBIT 4.1 for cloud computing** (ISACA, 2011). The CSA has also released a **matrix of control objectives,** which refers to controls that can be relevant to cloud computing from various other standards and guidelines, such as HIPAA, ISO/IEC 27001:2005, NIST SP800-53 R3, FedRAMP Security Controls, PCI DSS v2.0 and others (CSA, 2012a). It is also worth mentioning that ENISA has produced an **Assurance framework** for cloud computing (ENISA, 2009b). It provides a list of questions that organisations can ask to help them in the assurance process.

- *Ensure that a system is in place to ensure that enterprise risks introduced by cloud computing are managed.*

Cloud computing introduces a multitude of new opportunities and risks. All of the bodies considered in this work describe various opportunities and risks associated with cloud computing and emphasise the need to address risks.

Much of the work described in the section regarding the selection of cloud computing solutions referred to various means of analysing risks. A decision framework by ENISA, described earlier in this chapter shows how a **SWOT analysis** can be used in such a risk evaluation. As stated previously, the CSA also outlines a "**simple framework** to help evaluate initial cloud risks…" (Cloud Security Alliance, 2011). ENISA also explains a more complete, **standards-based risk assessment process** that organisations can use (ENISA, 2009a). They categorise several common cloud computing risks according to probability, impact and how the risks compare with the risks associated with more traditional solutions.

Once a risk assessment has been conducted, organisations need to decide on a risk response for cloud computing. Once again, there is an abundance of guidelines and recommendations regarding how various cloud computing risks should be addressed from the bodies considered in this work. The CSA provides a document describing and providing recommendations for cloud computing risks in thirteen different domains (Cloud Security Alliance, 2011). NIST provides a description of various risks and recommendations (NIST, 2011a). ENISA (2009), and the Commission of the European Communities, Expert Group on Cloud Computing, also provides guidance on risk mitigation, especially as it relates to contracts and legal risks.

- *Ensure that cloud computing complies with legal, regulatory and contractual requirements.*

The guidance considered in this work, as it pertains to cloud computing, deals largely with ensuring compliance using contracts.

ENISA gives a **list of areas to pay attention** to when assessing agreements in various forms (such as service level agreements and terms of use) with CSPs (ENISA, 2009a). ENISA also provides extensive guidance on cloud computing contracts. The guidance includes a **checklist** that organisations can follow to assess and evaluate cloud computing contracts with CSPs (ENISA, 2011). The guidelines focus primarily on security issues (such as availability, incident response and data lifecycle management) of the contracts from the customer's perspective. The CIO Council also gives **guidelines and a checklist** of questions that organisations can use regarding SLAs and CSP and End-user agreements (CIO Council & Chief Acquisition Officers Council, 2012).

ENISA also provides a **methodology for legal analysis** regarding the use of cloud computing (Cattedu, 2011). The methodology includes three steps that help organisations identify legal risks related to the use of cloud computing. A list of six fundamental questions regarding organisations' use of cloud computing aids in conducting this analysis. The methodology is applied to scenarios within the European Union.

4.7 Assuring Compliance in Cloud Computing

This chapter has highlighted the work by various reputable bodies regarding guidelines for cloud computing. As can be seen in the preceding sections, various useful guidelines have been provided to assist with making decisions about the selection, implementation and running of cloud computing. This work is primarily concerned with guidelines about assurance and conformance.

This chapter has highlighted several guidelines that have been produced for cloud computing conformance or compliance. This has included guidance regarding how to evaluate contracts and agreements with CSPs and a methodology for analysing legal risks. It has also highlighted the fact that organisations should govern the use of cloud computing in the context of the organisation's IT governance program. This approach would facilitate internal compliance. ISACA has provided guidelines about using control objectives from COBIT 4

for cloud computing. **No guideline found by the researcher holistically addresses internal and external conformance issues for cloud computing in detail.**

This chapter has also highlighted guidelines regarding cloud computing assurance. According to ISACA, however, there is no single framework that can be used for cloud computing assurance (ISACA, 2011). ISACA lists various common frameworks that can be used by CSPs for assurance and highlights the shortcomings of each (ISACA, 2011). Many of these have been referred to in this work, including the CSA cloud control matrix. Additionally, ENISA provides an ***assurance framework*** that has also been referred to in this work (ENISA, 2009b). One shortcoming of this framework, as described by ISACA, is that it is limited to the risks associated with cloud computing.

In the field of cloud computing, in general, there is much work done to produce guidelines to assist with this subject (Chris, 2010; Ovum, 2010; Reilly, 2011). In the fields of conformance and assurance, there is still a need for further guidance. One of the reasons that complicates producing guidelines for cloud computing is that, as we have seen in this chapter, it is a very broad term that can encompass a great variety of IT solutions. Guidelines for cloud computing would, therefore, have to be quite broad to be applicable to such a range of possible IT solutions. More granular guidance addressing issues for assuring conformance for specific cloud computing solutions are, therefore, also important.

4.8 Conclusion

"Cloud computing is not going away. It can be a valuable tool to an organisation. But, it's a tool that needs to be understood and managed" (Gatewood, 2009, p. 36).

In order to be able to understand the problem of assuring the conformance of cloud-based email in context, this chapter has explained the concept of cloud computing. In defining cloud computing, it has shown that there are various service and deployment models that can form part of a cloud-based solution. Additionally, this chapter has stated that each of these service and deployment models have varying risks and opportunities associated with them. Cloud computing has a large potential to positively impact organisations. To reap benefits from cloud computing, however, it is vital that the challenges and risks coupled with such solutions are adequately addressed. Issues regarding assuring the conformance of cloud-based solutions impact the success and adoption of these solutions.

CHAPTER 5

Cloud-based Email at Higher Education Institutions

5.1 Introduction

The main objective of this work, as identified in Chapter 1, is to **compile a framework to assist higher education institutions in South Africa with assuring that cloud-based email solutions are governed and managed in a way that adequately complies with the conformance principle of governance.** As shown in Figure 5.1, the preceding chapters of this work have provided a basis for solving this problem by discussing the areas of assurance and conformance as part of governance and the field of cloud computing. A broad overview of what cloud computing is, how it is being used by organisations and both the tremendous opportunities and significant challenges presented by this form of computing has been provided. The challenges and concerns regarding conformance and assurance when using cloud computing have been especially highlighted. This chapter and the rest of this work focuses specifically on the *problem of assurance and conformance* guidelines for *cloud-based email* used in *higher education* in *South Africa,* as depicted by the asterisk in Figure 5.1.

Before emphasising the problem of insufficient assurance guidelines for cloud-based email in higher education in South Africa, this chapter defines exactly what cloud-based email is, the impact that it is having on organisations in general and on higher education institutions in particular and the potential benefits of cloud-based email for higher education institutions.

Cloud-based email is one of the earliest and most widely adopted forms of cloud computing (Cloud Industry Forum, 2011; Focus Market Research, 2011). Individuals having being using email provided over the internet by service providers, such as Google and Hotmail, for some time already. This form of email was referred to as webmail. It became widely available to the public in the mid-1990s (Fleishman, 2012; Goldsborough, 2012).

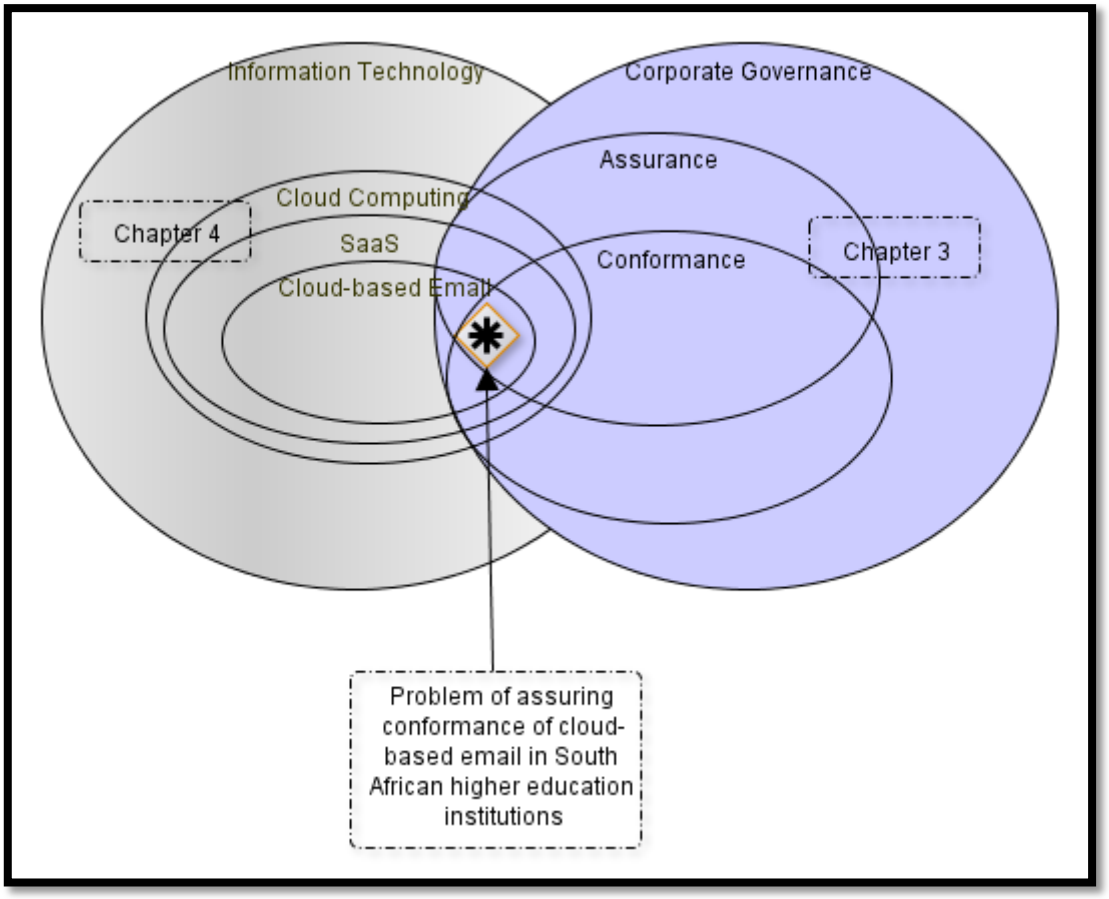


Figure 5.1 Focus area of chapter

5.2 Cloud-based Email

Although cloud-based email for individuals has been used widely for almost two decades now, the use of cloud-based email for organisations is a relatively new concept. This section highlights exactly what is meant by cloud-based email and the impact that this manner of email provisioning is having on organisations.

5.2.1 What is cloud-based email?

It is important to understand what cloud-based email is. Hosted email, SaaS email, email as a service, web-based email, cloud email and cloud-based email are terms that seemingly describe the same thing. This section highlights some definitions found in literature and proposes a definition of cloud-based email that will be used for this work. Firstly though, a distinction is made between personal and business email. Individuals have been accessing email as a service that has been provisioned and maintained by a service provider over the internet for some time already. This work discusses the use of cloud-based email for an

organisation and how this affects the organisation's ability to implement governance and assurance controls and not personal email.

As was shown in the definition for cloud computing in chapter 4 of this work, there are four main cloud deployment models: private, community, public and hybrid. An organisation's email can be deployed using these models.

A *private cloud* is one which is provisioned for a single organisation by a third party and can exist either on or off premise. This model for provisioning email where there is a dedicated server for each customer may also be referred to as *hosted email* (Conry-Murray, 2010) or *cloud email* (Schadler, 2009b).

*Community cloud*s support a community of users and can be managed either by the organisations or by a third party of their choice. It can also be on or off premise. With this model the community has a fair amount of ownership and control of the cloud. This is a less common deployment model for email in general. Email services provided specifically for education institutions by providers such as Microsoft (which offers email as part of Office 365) and Google (which offers email as part of Google Apps for education), may appear to be examples of community clouds. Although this email implementation may be like a community cloud in some respects, the community of users (educational institutions) does not have ownership or a high-level of control of the cloud and, therefore, is not truly a community cloud.

Public clouds are used by the general public or a large industry group and are owned and managed by a third-party vendor. Email provided over the internet by service providers such as Google, Microsoft and Yahoo are examples of public deployments for email. Email provided in this manner is also referred to as *Software as a Service (SaaS) email* or *email as a service* (Conry-Murray, 2010; Redmond, 2008). It is usually built on a multitenant architecture (Conry-Murray, 2010). This public deployment of email as a service is likely what many think of as cloud-based email. Sometimes, the characteristic of multitenancy is disregarded and this email deployment is also referred to as hosted email (Schadler, 2009a).

Organisations may choose to use a combination of public and either private or completely in-house deployment models for an email solution. This can be referred to as a *hybrid* system for cloud email (Redmond, 2008).

Based on the above, for the remainder of this work an *organisation will be said to use cloud-based email whenever it relinquishes a degree of control over all or part of its email by*

engaging in a contract with a CSP for the provisioning and management of email using a multitenant architecture.

5.2.2 Impact of cloud-based email

As stated at the outset of this chapter, cloud-based email is one of the earliest and most widely adopted forms of cloud computing. Surveys indicate that email is one of the IT systems that organisations are most likely to move to the cloud. They also show that there is a significant percentage of organisations already using or considering the adoption of cloud-based email. According to a survey by the Radicati Group 29% percent of organisations now use either cloud-based email entirely or use partly cloud-based email and partly in-house email (The Radicati Group, Inc, 2012). Research suggests that the vast majority of organisations (83%) expect to have at least part of their email provisioned using cloud computing by 2014 (PR Newswire, 2012). Popular cloud-based email providers such as Google and Microsoft already have a significant customer base. Google Apps, which provides email and other collaboration services, is already being used by over five million businesses, governments in over 45 states and millions of students and teachers at educational institutions.

The fact that cloud-based email and related cloud computing services are and will continue having a marked impact on organisations seems indisputable. The benefits that an organisation may derive from using this form of email provisioning is a motivating factor for its adoption.

There are several potential benefits associated with cloud-based email that contribute to the interest in this form of email provisioning for organisations. Potential cost reduction is the largest motivator (Business Wire, 2011; Conry-Murray, 2010; Schadler, 2009a). A report by Schadler for Forrester Research concluded that most types of companies could make significant cost reductions on their email spending by moving at least some staff email to the cloud. According to the report, if a company with 100,000 users were to move 20,000 occasional email users to the cloud they could save between $750,000 (with Google Apps Premier Edition) and $1.3 million (with Microsoft Exchange Online Deskless Worker license) annually (2009b, p. 5).

Another benefit related with cloud-based email includes the fact that the CSP becomes responsible for proper maintenance and administration (including tasks such as configuration

and upgrades of the email system), thereby freeing up company IT staff to focus on other, possibly more business-centric tasks (Schadler, 2009a; Business Wire, 2011).

There are, however, concerns about the use of cloud-based email by organisations. The adoption of cloud-based email is being slowed by these concerns.

Some issues include concerns over ensuring security and privacy of cloud-based email. Problems with warranting availability with cloud-based email may also pose a problem for organisations. In addition, there are various concerns related to ensuring compliance when using cloud-based email. Compliance issues include uncertainty as to how laws and internal organisational policies regarding e-discovery and document retention are affected with cloud-based email.

As has been highlighted in this section, organisational cloud-based email is an area that merits interest and research. It can enable organisations to provide users with access to email and related communication and collaboration services with less administrative hassle and less money. There are, however, serious issues related to cloud-based email that organisations must be cognizant of. These issues have to be adequately addressed before organisations can adopt cloud-based email in a manner that meets the requirements of proper governance. Organisations should, therefore, have a system in place that allows for the evaluation, adoption, implementation and governance of cloud-based email that provides assurance that this is done in an effective and compliant manner. This is true of all organisations. One sector which has seen a tremendous uptake of cloud-based email and in which this is outstandingly the case is the higher education sector.

5.3 Cloud-based Email for Higher Education

As has been highlighted, cloud-based email is a cloud solution that has become prevalent in many industries. Higher education is an area where there has been an especially rapid adoption of this technology. This section discusses the marked impact that it is having on higher education institutions, both globally and in South Africa. It discusses some of the factors that make the use of cloud-based email especially appealing for higher education. The significant concerns related to the use of cloud-based email by higher education institutions are also highlighted.

Cloud-based email is already widely used among higher education institutions around the world, and it is expected to continue having a marked impact on the way email is provisioned and thought of in this sector (Carnevale, 2008). A report published by Gartner about the hype cycle for education indicates that cloud-based email has seen a "tremendous uptake" in higher education and is a technology that is "firmly ensconced in the sector" (Corbyn, 2009). According to the NMC Horizon Report, the increased use and acceptance of cloud-based technology is one of the key trends in technology adoption between 2012 and 2017 that changes the way institutions use, configure and conceptualise certain functions (Johnson, Adams, & Cummins, 2012). The popularity of cloud-based email solutions for education is evident when the websites for two of the most popular providers of cloud-based services for education are examined. Microsoft (Office 365 formerly Live@edu) and Google (Google Apps for Education) both provide education institutions with free email and collaboration tools. Google (2011) claims to have "more than fourteen million students and teachers" using Google Apps. Microsoft (2012) states that, "Thousands of educational institutions in more than a hundred countries around the world use Live@edu services, accounting for tens of millions of users." Some institutions using services provided by Google include Yale University (Carter, 2011), the University of Nebraska (Goulart, 2012) and Harvard College (Kumar & Weinberg, 2011).

There has clearly been a remarkable adoption of cloud-based email for higher education internationally. Research suggests that higher education institutions in South Africa are also rapidly adopting cloud-based email. Two surveys of IT directors (or their representatives) of higher education institutions in South Africa have been conducted as part of this work. Both surveys were carried out at a general meeting of the Association of South African University Directors of Information Technology (ASAUDIT). The surveys were conducted in 2009 and 2012. The aim of the surveys was to twofold: 1) to establish the extent to which cloud-based email is being used at higher education institutions in South Africa and 2) to gauge the general attitude of managerial IT staff at these institutions regarding the risks and benefits of cloud-based email. In 2009 representatives of nine South African universities responded. In 2012 there were participants from sixteen higher education institutions. The South African Department of Education lists 22 South African universities (Department of Basic Education). Therefore although not all higher education institutions were surveyed, the data collected represents a significant percentage (73 percent) of higher education institutions in South Africa. The questionnaires used in 2009 and 2012 are found in Appendix C1 and

Appendix C2 respectively. The survey of sixteen higher education institutions in South Africa in 2012 found that half of the respondents had already started using or were currently implementing cloud-based email. As can be seen from Figure 5.2, three out of the seven institutors planning on using cloud-based email were aiming to begin implementation by 2012. It is expected, therefore, that soon most South African higher education institutions will be using cloud-based email in some form.

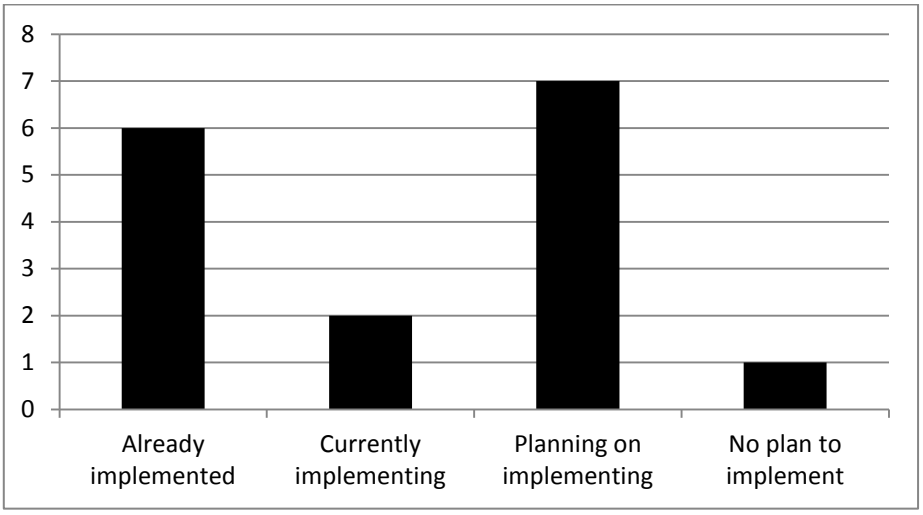


Figure 5.2 Cloud-based email adoption in South African higher education institutions in 2012

The survey also found that Live@edu is currently the most popular cloud-based email provider for South African higher education institutions. As shown in Figure 5.3, nine out of fifteen (60%) of the institutions that are currently using or intending to use cloud-based email indicate Microsoft's Live@edu solution as their preferred solution. Interestingly, five out of the six institutions already using cloud-based email (83%) are using Live@edu.

It is clear that cloud-based email is transforming the way higher education institutions are provisioning email. There are various factors that make cloud-based email especially appealing for higher education. Understanding the potential benefits that higher education institutions could derive from cloud-based email makes it clear why this cloud computing solution should be carefully examined by such institutions (Geer, 2011). The next subsection discusses some of these opportunities.

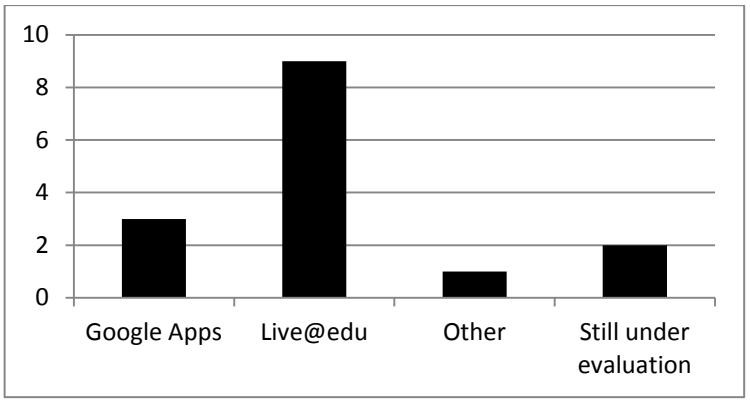


Figure 5.3 Cloud-based email providers preferred by South African higher education institutions

5.3.1 Cloud-based email benefits for higher education

There are several factors that make cloud-based email especially appealing to higher education institutions. The fact that education institutions can receive ***tremendous cost savings*** using cloud-based email is foremost of these.

The budgets of many higher education institutions internationally have been adversely affected by recent economic pressure (Britto, 2012). The NMC Horizon Report for 2012 to 2017 lists economic pressures as one of the biggest challenges facing higher education institutions globally (Johnson, Adams, & Cummins, 2012, p. 5). This is true in South Africa as well.

Despite the pressure to cut costs at higher education institutions, there is a demand for these institutions to provide staff and students with easy access to various IT services. Like most organisations today, higher education institutions rely on information technology to function. Not only is information technology critical to the functioning of the business of higher education, but it is also a feature expected by the students of these institutions. Students at higher education institutions generally come from a generation of people that uses information technology and the internet. They view information technology and the internet as a normal part of life and not as an outstanding new invention. Students from this generation are at times referred to as digital natives, reflecting this fact (Prensky, 2001). Students from this generation characteristically expect easy access to information technology services, including email, from the educational institutions they attend (Britto, 2012; Johnson, Adams, & Cummins, 2012, p. 4).

Economic pressure, coupled with demand for continuous access to IT services, makes it essential for higher education institutions to investigate and find new ways of provisioning services (Mircea & Andreescu, 2011; Suess & Morooney, 2009). Cost reductions associated with the use of cloud computing make this computing model an obvious contender as part of a possible solution. This is especially true for cloud-based email. Google Apps for education, Live@edu and Office 365 from Microsoft and Zimba from Yahoo all make cloud-based email and its related services available to students ***free*** of charge. Considering the tremendous value that a free cloud-based email service would have for cash-strapped higher education institutions, it would be irresponsible not to seriously investigate the use of this technology.

Another factor that may make cloud-based email and other cloud computing solutions seem ideally suited for higher education is that some characteristics of cloud computing match the desired characteristics of a modern educational institution. The NMC Horizon Report, mentioned previously in this chapter, claims that people expect access to services "whenever and wherever they want" as a key trend for the adoption of technology in higher education (Johnson, Adams, & Cummins, 2012, p. 4). As seen in chapter 3, cloud computing provides on demand self-service (Mircea & Andreescu, 2011). Cloud-based email allows ***instant access*** to email at any time, ***from various types of devices*** and ***from anywhere*** in the world.

CSPs are also often able to provide ***additional features and functionality***. For example, CSPs can often provide *larger inboxes* than higher education institutions would be able to provide. Cloud-based email providers also allow access to a number of *other communication and collaboration services* for free. These commonly include access to services, such those that provide cloud-based storage and instant messaging (IM) functionality. This is especially important to digital natives who view email, the internet and instant messaging as an integral part of their lives and expect access to networks and social media (Johnson, Adams, & Cummins, 2012; Prensky, 2001; Britto, 2012).

The above makes it clear that cloud-based email has the ability to greatly benefit higher education institutions. Chapter 2 highlighted that it is the responsibility of the board to ensure that opportunities presented by developments in IT (such as those discussed here) are recognised and exploited in a manner that adds value to an organisation and is secure and compliant with regulations, policies, standards and best practice guidelines. By not recognising and investigating the potential opportunities associated with cloud-based email,

higher education institutions could be thought of as not fully carrying out their IT governance responsibilities.

Higher education institutions, however, also cannot be said to fully carry out their IT governance responsibilities if the risks and challenges are not thoroughly addressed before adopting a technology, such as cloud-based email, so that this is done in a compliant manner. The following subsection highlights some of these risks and challenges.

5.3.2 Challenges

Various concerns have been highlighted in literature regarding the adoption of cloud computing by organisations in general and by higher education institutions in particular. These include concerns regarding privacy, security, availability and interoperability. Chapter 3 discusses some of these concerns.

Figure 5.4 shows the results of a survey of South African higher education institutions. As can be seen in this figure, South African higher education institutions also have several concerns regarding the use of cloud-based email.

This work, however, focusses on the more overarching concerns of assurance and conformance with regard to cloud-based email. As explained in chapter 3, an assurance engagement is defined as an "engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria" (International Auditing and Assurance Standards Board, 2004). The criteria of an assurance engagement will test compliance with internal policies and procedures, external laws and regulations and best practice guidelines and standards related to the subject matter. Ensuring that controls are in place and risks are identified and mitigated is an integral part of the assurance process.

This subsection, therefore, highlights some of the concerns regarding assurance of cloud-based email in the areas of legal compliance, internal compliance and conformance with principles set out in relevant best practice guidelines and standards.

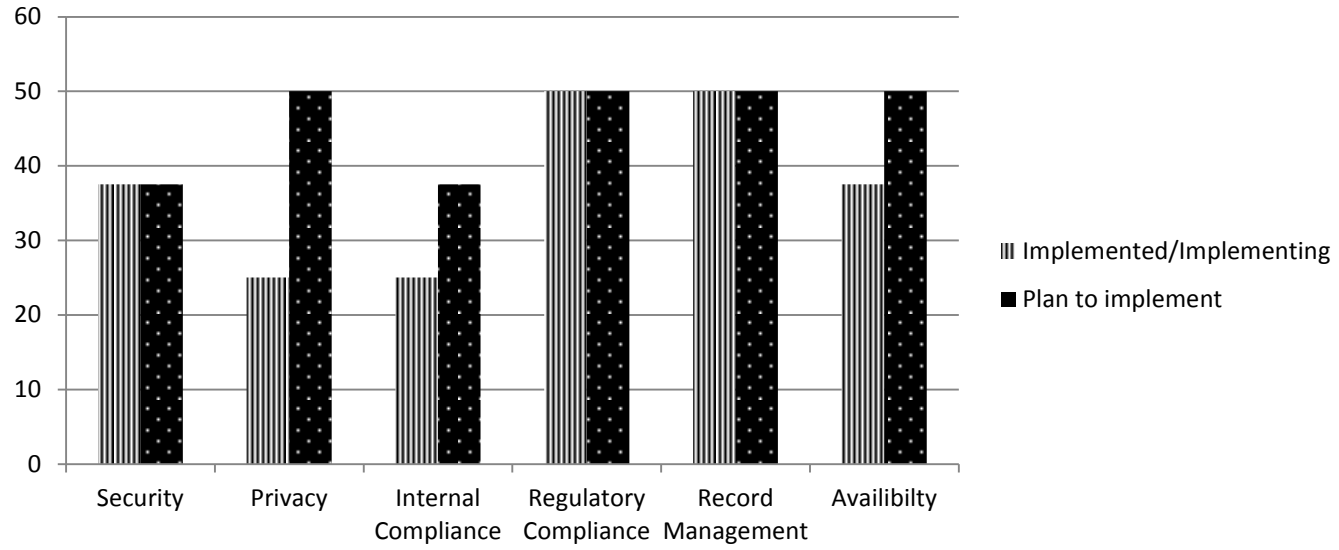


Figure 5.4 Higher education institutions cloud-based email concerns

5.3.2.1 Legal compliance

As discussed in Chapter 3, ensuring IT compliance with legal and regulatory measures is an essential part of ensuring that an organisation is well-governed. All organisations are required by the law, in accordance with principles of good governance and principles of ethical behaviour, to take due care in demonstrating regulatory compliance. All organisations are, consequently, obliged to be aware of applicable national, international and/or sector-specific regulations related to the use of IT, and to comply with these regulations (Viljoen, Von Solms, & Lawack-Davids, 2012, Robinson, 2010). Cloud computing is nonetheless being adopted despite concerns about legal compliance in the cloud. Chapter 4 highlighted some of the concerns regarding ensuring legal compliance when using cloud computing in general. Some of these concerns are highlighted here, particularly those pertaining to cloud-based email.

Email is not merely a convenient form of communication on which organisations are dependent. Emails are electronic records for which organisations may have legal responsibilities regarding the retention, destruction and restoration of stored information (Lisa Thornton Inc, 2005). Whether higher education institutions house these electronic records in-house or store them on the cloud, they remain responsible for them, regardless of where the information is kept.

When higher education institutions use public or hybrid cloud deployment models for provisioning email, though, they are likely to lose some measure of control. Information may

no longer reside on servers owned and managed by the organisation, 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. Higher education institutions then have the responsibility of finding means other than traditional controls such as internal policies and procedures to ensure that they are still legally compliant with relevant laws and regulations.

As mentioned in the previous paragraph, CSPs are often based in different countries than the higher education institutions for which they provision email and related services. This complicates the matter of legal compliance, since the higher education institution may be affected by laws not only from their own country, but also from the country in which the CSP operates. A study into the affects that US laws, such as the US Patriot Act, could have on research institutions in the Netherlands found that information stored in the cloud by foreign higher education and research institutions could be accessed by American authorities regardless of whether the server provisioning the services is situated in the Netherlands or not (van Hoboken, Arnbak, van Eijk, & Kruisjen, 2012). A CSP is considered subject to U.S. jurisdiction when "the entity is based in the United States, has a subsidiary or office in the United States, or otherwise conducts continuous and systematic business in the United States" (van Hoboken, Arnbak, van Eijk, & Kruisjen, 2012). All the CSPs that currently provide free cloud-based email to higher education institutions would, therefore, be subject to U.S. jurisdiction. Information owned by higher education institutions could be accessed even without the knowledge of these institutions.

The report also highlights the legal principles of 'reasonable expectation of privacy' the 'Third Party Doctrine'. Essentially the 'Third Party Doctrine' implies that if private information is handed over to a third party (such as a CSP) one can no longer, in principle, have any reasonable expectation of privacy with regard to this information (van Hoboken, Arnbak, van Eijk, & Kruisjen, 2012). This could evidently be a concern for higher education institutions contemplating the use of cloud-based email.

Another potential legal concern for higher education institutions contemplating the adoption of cloud-based email has to do with service level agreements (SLAs) and contracts with CSPs. Higher education institutions that receive email and related services free of charge from CSPs may not be in a position to negotiated contracts and relate terms of use and SLAs with CSPs. In institutions where there are not yet clear policies regarding cloud computing adoption, such contracts could also be entered into without the appropriate scrutiny by top management and legal staff.

From the above it is clear that there are noteworthy legal risks associated with the adoption of cloud-based email that higher education institutions are obliged to carefully examine before adopting and implementing such services in a manner in which they can assure legal compliance.

5.3.2.2 Internal compliance

Internal compliance refers to compliance with policies, practices and guidelines that govern institutions. Higher education institutions considering the adoption of cloud-based email or other cloud computing services will have to determine what requirements related to such services are mandated by these internally adopted rules and guidelines. For example, higher education institutions may ask questions such as: Will our SLA with our staff and students need to be adjusted when using cloud computing? Will we still comply with policies regarding such matters as document retention, privacy and availability when using cloud-based email? What policies will need to be adjusted when using cloud-based email? If our IT governance strategy is best practice based, how will we be able to apply best practice guidelines to cloud-based email?

Internal compliance may, however, involve more than just determining organisational requirements based on existing internal policies, practices and guidelines. Cloud computing may necessitate a fundamental shift in an organisation's views of management and leadership for certain services. It calls for a different approach to the traditional tactic of centralised control (Jackson, 2011; Yanosky, 2010; Mircea & Andreescu, 2011). Traditionally, higher education institutions have largely been able to control their information and IT resources directly. With cloud computing, this changes (Osterman Research, 2011). Old policies, standards, best practice guidelines, management practices and controls that focussed on providing assurance and confidence through direct control need to be updated.

Katz suggests that failure of higher education institutions to properly govern and manage cloud computing could lead to a scenario where they are forced to use an 'accidental' approach where attempts are made to "rope in" cloud computing solutions (Katz, 2008, p. 23).

5.3.2.3 Assurance and confidence

As has been highlighted in the previous chapter, a lack of confidence or trust in cloud computing in general is a point of concern that seems to affect the widespread adoption of

cloud computing solutions. As highlighted in this chapter, however, there is a widespread adoption of cloud-based email amongst education institutions. This seems to indicate that there is generally a high-level of trust in the cloud-based email service providers. This was also apparent during the case study at the University (described in more detail in Chapter 7). Staff at the University highlighted that the institution had a long standing, good relationship with Microsoft. This influenced the University's decision to use Microsoft as the CSP for the email service, as they felt confident that proper services would be provided. The fact that cloud-based email has been successfully used by several higher education institutions may also foster trust in this service (Lockheed Martin, LM Cyber Security Alliance & Market Connections, Inc., 2010). Despite confidence in the CSP's ability to provide good levels of service for free, institutions do lack confidence regarding their own ability to assure internal and external conformance.

This section has made clear from literature that internationally, despite the tremendous uptake of cloud-based email, there are serious concerns regarding the use of this service at higher education institutions. This is true in South Africa as well. A survey of IT managers from sixteen higher education intuitions in South Africa in 2012 found that, although the majority of intuitions will use cloud-based email in the future or are currently using it and are satisfied with the service, they still have many noteworthy concerns regarding the use of this service (Tout, Sverdlik, & Lawver, 2009). This is troubling. The survey also found that ***South Africa higher education institutions feel that they would benefit from a set of guidelines for compliance when using cloud-based email.***

In 2009, seven out of eight respondents either agreed or strongly agreed with the following statement: I have not been provided with an adequate set of good practice guidelines for the governance, risk and compliance of cloud-based email. Interestingly, the one university that disagreed with the statement did not give an indication of any guidelines they would recommend for cloud-based email implementation when prompted to do so. Further emphasising the important role of a set of guidelines for compliance using cloud-based email, participants in the 2012 survey were asked "Do you think that South African universities would benefit from a set of guidelines for compliance in the adoption of cloud-based email?" Only one out of seventeen institutions responded "no". The vast majority of institutions (94%) believe that such guidelines would be beneficial.

Considering the important role of email, it is perturbing that IT professionals feel inadequately equipped with regard to the governance, risk and compliance of cloud-based email and are apprehensive about ensuring compliance in particular.

It can be concluded that ***the lack of structured guidelines for assuring the conformance of cloud-based email is putting this service at risk in higher education institutions in South Africa.***

This work aims to assist with addressing this problem. Based on the facts described in this chapter, the following subsection derives some objectives of such a solution.

5.3.3 Solution objectives

In Chapter 3, a list of basic objectives of a framework for assuring conformance was concluded. These objectives are modified and expanded based on the findings described in this chapter. The objectives for a framework to assist with assuring the conformance of cloud-based email are listed below:

- Objective: Assist with promoting trust and confidence in the internal and external conformance of cloud-based email
    - Requirement: Assure conformance by using accepted assurance and conformance methods and techniques.
    - Requirement: Ensure that the framework addresses legal and regulatory conformance risks.
    - Requirement: Ensure that the framework addresses internal conformance requirements, including requirements in policies and internal governance structures.
    - Requirement: The framework should assist higher education institutions by promoting confidence that they are governing and managing cloud-based email in a manner that conforms to internal and external requirements.
- Objective: Assist with demonstrating due diligence
    - Requirement: Promote a best practice/standards based approach to assure conformance.
- Objective: Assist with achieving the goals of IT governance (strategic alignment and value optimization) for cloud-based email

- Requirement: Ensure that the conformance and assurance activities promoted by the framework are strongly guided by best practice guidelines for IT governance.

A solution that meets these objectives should assist with addressing the problem motivated in this chapter: the lack of structured guidelines for assuring the conformance of cloud-based email is putting this service at risk in higher education institutions in South Africa.

5.4 Conclusion

As with cloud computing in general, cloud-based email is associated with both potentially significant opportunities and noteworthy risks. Cloud-based email provides cash-strapped higher education institutions that are expected to cater to the ICT needs and wants of both staff and students (a generation of digital natives) with the opportunity to provide an email service with less administrative hassle and with additional functionality and features than most of them could provide in-house for *free*. Not recognising and investigating the potential opportunities associated with cloud-based email higher education institutions could, therefore, be not only foolish but negligent. The principles of IT governance, however, place a dual responsibility on managers. Principles of good IT governance not only require managers to *ensure that opportunities presented by developments in IT (such as those discussed here) are recognised and exploited* but that they also do so *in a manner that adds value to an organisation and is secure and compliant with regulations, policies, standards and best practice guidelines.* The second part of this responsibility should contribute to a sense of assurance in the adoption of cloud-based email. This chapter has highlighted some of the challenges that plague higher education institutions in giving assurance regarding the adoption of cloud computing. It has shown that, although the majority of intuitions will use cloud-based email in the future or are currently using it and are satisfied with the service, there are still many noteworthy concerns regarding the use of this service. One significant concern is that IT professionals feel inadequately equipped to handle the governance, risk and compliance of cloud-based email. They are apprehensive about compliance in particular and feel that they would benefit from a set of guidelines. It has been concluded that ***the lack of structured guidelines for governance and compliance of cloud-based email is putting this service at risk in higher education institutions in South Africa.***

The following chapter will present a framework which will assist in addressing this problem.

Higher education institutions are among the early adopters of cloud-based email, and research regarding the effective assurance of cloud-based email may be used effectively to benefit other sectors (Britto, 2012; Suess & Morooney, 2009; Mircea & Andreescu, 2011).

CHAPTER 6

A Framework for Assuring the Conformance of Cloud-based Email

6.1 Introduction

The previous chapters have highlighted and examined the fields of cloud computing, assurance and conformance and have shown that *the lack of structured guidelines for assuring the conformance of cloud-based email is putting this service at risk in higher education institutions in South Africa.* This chapter introduces a *Framework for Assuring the Conformance of Cloud Email* (hereafter referred to as FACCE), which can be used to assist in addressing this problem.

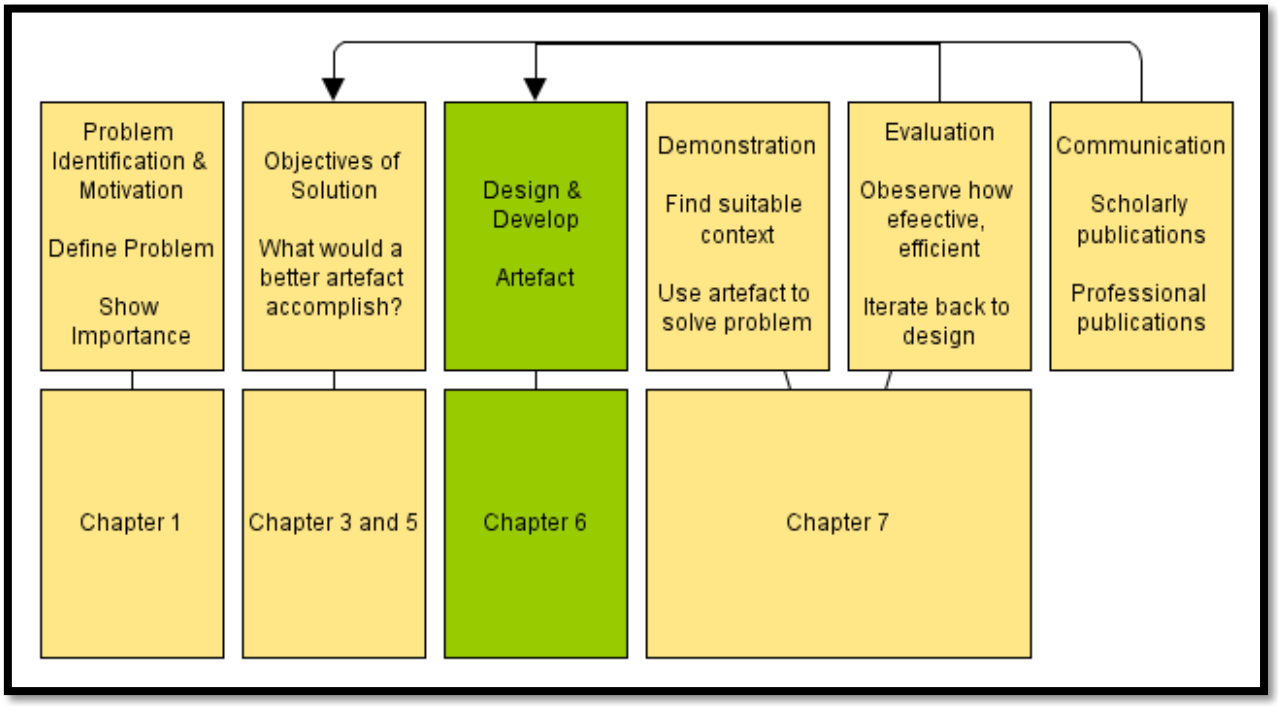


Figure 6.1 Design science research methodology used for FACCE

As described previously, the FACCE is designed using the design science research methodology (DSRM) outlined by Peffers et al. (2008). The steps of this methodology are shown in Figure 6.1. As this figure highlights, the problem, the importance of the solution and the objectives of the framework have been discussed in previous chapters.

The primary focus of this chapter, though, is to describe the design and development of this artifact. This is accomplished in the remainder of this chapter.

6.2 FACCE, A Conceptual Framework

Before describing a framework for assuring cloud-based email conformance (FACCE), it is important to clearly understand what is meant by the term framework as used in this chapter. This section, therefore, explains how and why FACCE can be described as a framework.

The term framework is a broad and possibly ambiguous term. The Encarta World English Dictionary defines a framework as an "underlying set of ideas: a set of ideas, principles, agreements, or rules that provides the basis or outline for something intended to be more fully developed at a later stage." There are various kinds of frameworks. Conceptual frameworks are commonly used in research. A conceptual framework can be defined as "a visual or written product that explains, either graphically or in a narrative form, the main aspects to be studied. It includes key factors, concepts, variables and the presumed relationships among them" (Miles & Huberman, 1994). A framework is a flexible tool that can be used to apply ideas presented directly or as an outline that can be modified or added to (Lethbridge & Laganiere, 2005). Conceptual frameworks can be further divided into various types. Shields and Tajalli identify five "micro-conceptual frameworks":

- Working hypotheses – this type of conceptual framework is usually associated with exploratory or preliminary research. It is expressed as a statement of expectation; research collects evidence that either supports or fails to support the hypothesis.
- Descriptive categories – with this micro-conceptual framework, the findings of a study are classified or categorised. It is used primarily for describing a field.
- Practical ideal type – this type of micro-conceptual framework is used to model components that would be used, or criteria that would be met, in a nearly ideal process. It does not prescribe a perfect solution, but it can be modified and revised. Frameworks that aim to describe best practice and that can be used as guides to improve reality are practical ideal type micro-conceptual frameworks. "The practical ideal type is just the best components that the student could find after engaging in a careful review of literature, tempered by his or her experience" (Shields & Tajalli, 2006, p. 324).

- Models of operations research – this type of micro-conceptual framework is usually used for decision making; it describes the best decision or the approach to follow to make such a decision.
- Formal hypotheses – here a hypothesis is usually stated in the form of "if x then y." Whereas working hypotheses are usually for exploratory research and are related with qualitative research techniques, formal hypotheses are used for explanation and are usually associated with quantitative research techniques.

Essentially, a conceptual framework provides an outline of the key components and relationships related to a field. The various types of micro-conceptual frameworks describe different goals that can be achieved by frameworks. Conceptual frameworks can aim to facilitate tasks, such as explaining, exploring or assisting with improving practice or decision making in a certain field.

A framework for assuring the conformance of cloud-based email (FACCE) will convey the main *components* (including ideas, principles and rules) regarding the subjects of assurance and conformance and apply these to the area of cloud computing in general and cloud-based email in particular. It will also describe the *relationships* between these components.

The FACCE is, therefore, clearly a conceptual framework. It aims to assist staff in higher education institutions in South Africa to improve the level of assurance of conformance related with cloud-based email. The components that comprise the FACCE are based on best practice guidance regarding the fields of assurance and conformance. The FACCE is, therefore, a practical ideal type micro-conceptual framework. This will become apparent in the following description of the FACCE.

6.3 Design and Development of the FACCE

The FACCE is explained in three stages in this section. Firstly, the main components that make up the core of the framework are identified, explained and motivated. Secondly, the manner in which these components interact to assure conformance is explained. Thirdly, more detailed guidelines for the implementation of the FACCE, which apply specifically to cloud-based email at higher education institutions, are explained. This progression forms the outline for the rest of this section, and is shown in Figure 6.2.

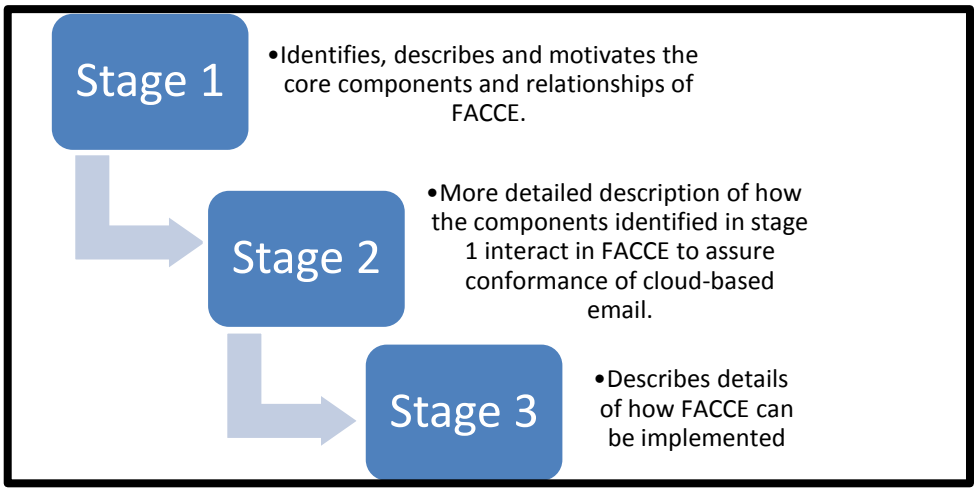


Figure 6.2 The three stages used to describe the FACCE

6.3.1 Stage 1: Identifying the core components and relationships of the FACCE

As stated previously, FACCE is a practical ideal type micro-conceptual framework. As such, the components that make up FACCE have been identified by carefully examining literature regarding what is considered as best practice in the areas of assurance and conformance as part of IT governance. This subsection provides the first stage of FACCE description. It aims to identify and explain the main components and relationships that form the core of FACCE. The components that are essential for providing assurance and then conformance are highlighted in the next two subheadings respectively.

6.3.1.1 Key components and relationships for an assurance framework

One of the main objectives of FACCE is to assist with improving assurance regarding the use of cloud-based email at higher education institutions. To identify components that are necessary for providing assurance, an existing conceptual framework for assurance has been analysed. This fits the standard approach for developing a practical ideal type micro-conceptual framework (Shields & Tajalli, 2006, p. 325). The *International Framework for Assurance Engagements* (hereafter referred to as IFAE), informs the components and relationships for assuring the conformance of cloud-based email in the FACCE. The IFAE is an internationally accepted framework designed by the International Federation of Accountants (IFAC). It describes the primary components, actors and relationships involved in an assurance engagement. This generic assurance framework can be expanded and adapted for the assurance of various types of 'subject matter', including IT.

Chapter 3 has described the core components of the IFAE. The components and relationships of this framework are, therefore, merely summarised here. An assurance engagement typically involves three actors: a *practitioner* (who performs the audit), a *responsible party* (who is responsible for the subject matter) and the *intended user* (who receives the assurance report). There are also three other components that are essential in an assurance framework: a set of suitable *criteria*, *evidence* collected and evaluated against the criteria and an *assurance report* that reports on the findings of the evaluation.

From the above, the core assurance framework that is illustrated in Figure 6.3 is concluded. The components identified here are used for assurance in the FACCE.

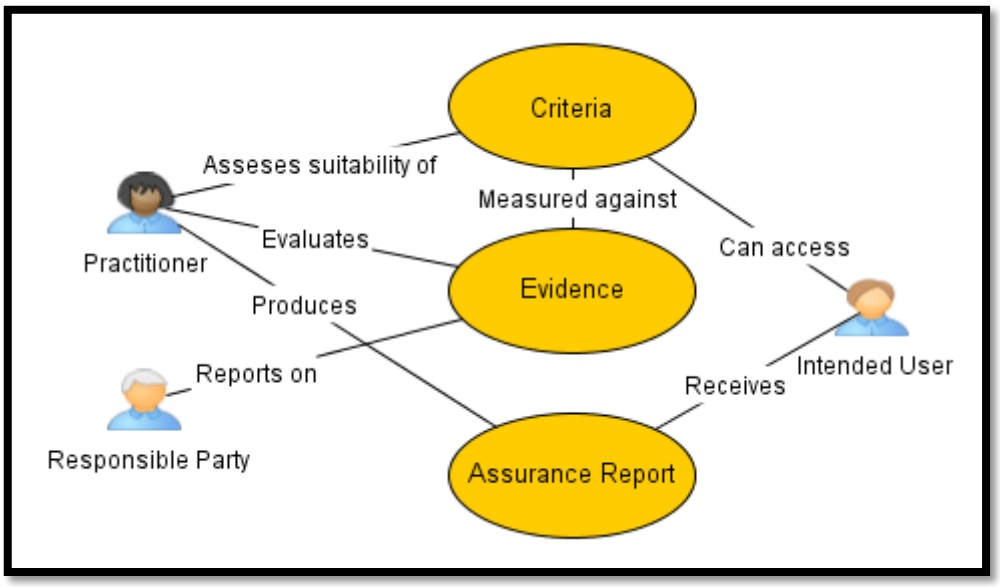


Figure 6.3 Concept diagram illustrating an assurance engagement

6.3.1.2 Key components and relationship for a framework for conformance

In addition to assisting with the problem of assurance, the FACCE aims to ensure conformance from an IT governance perspective with regards to cloud-based email. *ISO/IEC 38500:2008* is an internationally recognised standard for corporate governance of IT that is used as a basis for identifying components for the FACCE that assist with demonstrating conformance. According to ISO/IEC 38500:2008, conformance is a key principle of IT governance. All six principles deemed necessary for IT governance in most institutions are summarised in Table 6-1. Examining the principle of conformance, as detailed in ISO/IEC

38500:2008, assists with identifying and explaining components that form part of the FACCE.

ISO/IEC 38500:2008 Principles of IT governance
• Responsibility – staff should be aware of their responsibilities regarding IT and have the skills and authority to do what is required of them • Strategy – should take into account the current and future IT needs and capabilities • Acquisition – decisions regarding acquisitions should be made clearly and transparently based on an analysis of benefits, opportunities, costs and risks • Performance – IT initiatives should be fit for purpose and of acceptable quality • Conformance – IT should comply with internal (defined by internal policies and practices) and external or legal and regulatory requirements • Human behaviour – the needs of the people involved should be taken into account with IT policies, practices and decisions

Table 6-1 ISO/IEC 38500:2008 principles of IT governance

As described in Table 6-1, conformance involves assuring that IT initiatives comply with internal and external requirements. These requirements include 1) legal and regulatory obligations: regulatory, legislation, common law and contractual obligations and 2) internal requirements as set forth in: internal policies, standards, professional guidelines and systems for IT governance (ISO, 2008, p. 22).

For each of the principles of IT governance, ISO/IEC 38500:2008 outlines three main tasks (evaluate, direct and monitor) involved in adhering to the principle. ISO/IEC 38500:2008 represents the interaction of these three tasks in the model for corporate governance of IT, as shown in Figure 6.4.

When ensuring conformance, these tasks should involve the following:

- Evaluate – evaluating the extent to which an institution is complying with legal and regulatory obligations and internal requirements.
- Direct – direction should be given to ensure that the staff is aware of conformance responsibilities and that policy, plans and mechanisms are in place to ensure conformance.

- Monitor – there should be appropriate reporting and assurance practices in place to ensure that IT conformance and related activities are adequately monitored (ISO, 2008, p. 22).

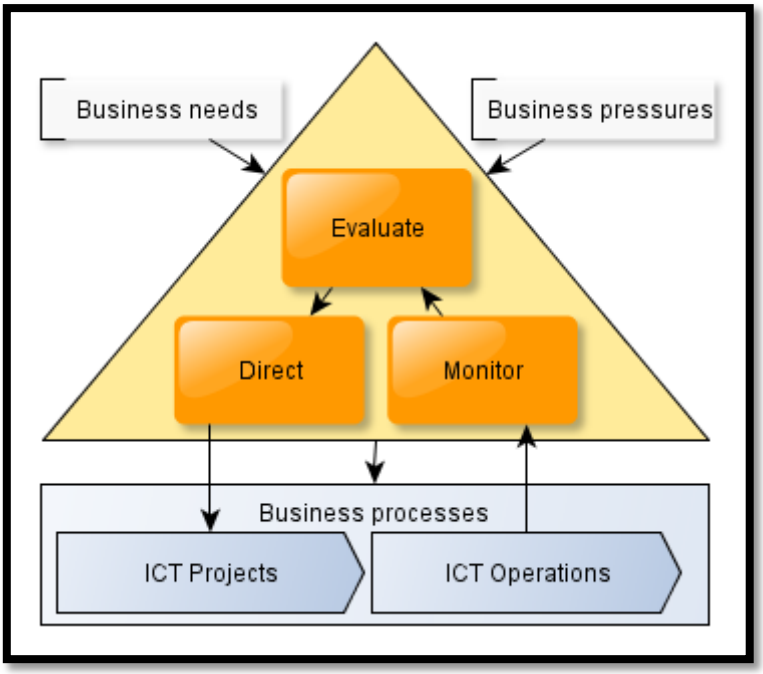


Figure 6.4 Adapted from ISO/IEC 38500:2008's model for IT Governance

These tasks should be carried out iteratively to facilitate demonstrating conformance with IT related matters at institutions.

An examination of ISO/IEC 38500:2008 provides an overview of what conformance is, how it relates to IT governance and a high-level view of what is involved in demonstrating conformance. This standard does not, however, provide more detailed guidance regarding how to demonstrate conformance. COBIT 5 provides more detailed guidance on accomplishing the three main governance tasks (evaluate, direct and monitor) shown in ISO/IEC 38500:2008.

COBIT 5 often refers to *enablers* to describe initiatives for IT governance. In fact, having an enabler-based approach is one of the core principles of COBIT 5's IT governance guidance. Enablers are enterprise resources and other factors that influence whether IT governance will be successful. COBIT 5 identifies seven enablers. They are depicted in Figure 6.5 and are further explained in the list below.

- Organisational structures – the organisational structure should support good activities and decisions regarding IT governance and management.
- Culture, ethics and behaviour – there should be good practices in place for "creating, encouraging and maintaining desired behaviour throughout the enterprise."
- Principles, policies and frameworks – There should be a limited number of principles in simple language used by organisations. All stakeholders should also have easy access to effective, efficient and non-intrusive policies. Comprehensive, flexible and current IT governance and management frameworks should also be used and available to all stakeholders.
- Information – Information should be properly defined and otherwise governed and managed to ensure its quality, security and accessibility.
- Services, infrastructure and applications – resources, such as infrastructure and applications, should be used so that IT-related services are delivered effectively and to the proper service level.
- People skills and communication – People should have appropriate education, skills, knowledge and experience to successfully perform assigned roles and responsibilities.
- Processes - processes are broadly defined in COBIT 5 as "a collection of practices influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (e.g. products, services)" (ISACA, 2010b). COBIT 5 defines a number of management and governance processes and provides good practice guidance and activities for each.

Figure 6.6 depicts the governance and management processes outlined in COBIT 5. According to COBIT 5, "Incorporating an operational model and a common language for all parts of the enterprise involved in IT activities is one of the most important and critical steps towards good governance. It also provides a framework for measuring and monitoring IT performance, communicating with service providers, and integrating best management practices" (ISACA, 2010b). COBIT 5, therefore, provides a process reference model that describes a set of governance and management processes that most organisations use. A process capability level is also provided to assess the extent to which a process is measuring up to the requirements for it.

This section has highlighted some of the key components involved in conformance as part of IT governance. The areas in which conformance need to be demonstrated have been

highlighted as conformance with 1) legal and regulatory obligations: regulatory, legislation, common law and contractual obligations and 2) internal requirements as set forth in: internal policies, standards, professional guidelines and systems for IT governance. Three core tasks necessary for demonstrating IT conformance (evaluate, direct and monitor) have been identified and explained. Additionally, the role of enablers in accomplishing conformance activities has been highlighted. To ensure conformance as part of IT governance, therefore, an understanding of the requirements for conformance (as outlined in various ***conformance requirement documents***) should influence the implementation of the tasks of ***evaluate, direct and monitor*** with the aid of ***enablers***.

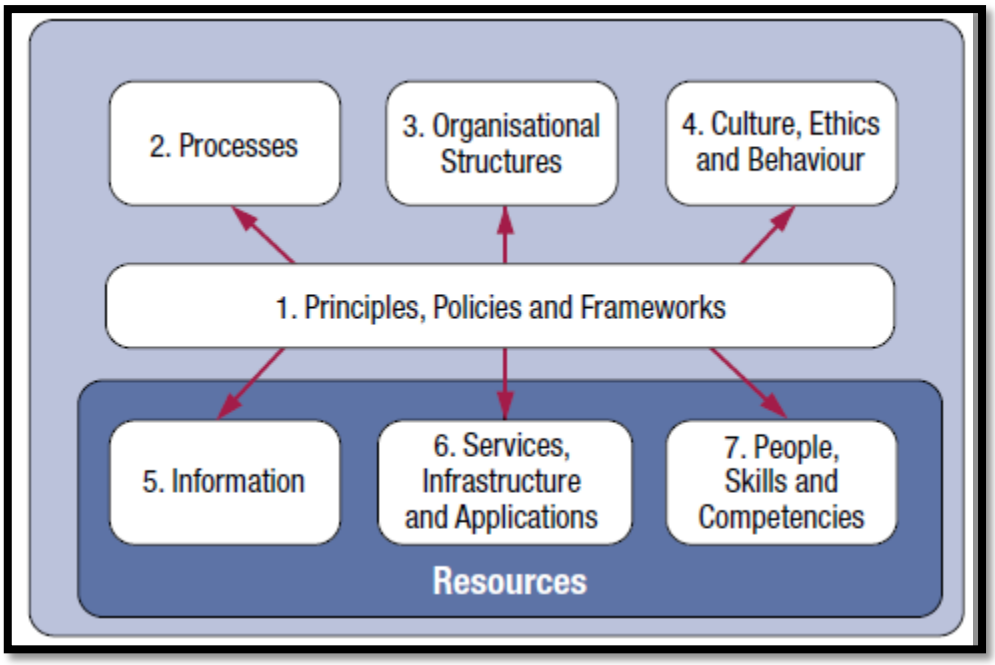


Figure 6.5 Seven enablers defined in COBIT 5 (ISACA, 2010b)

The components identified in both this and the preceding subsection form part of the FACCE. Figure 6.7 diagrammatically depicts the FACCE. From the discussion in this section it should be possible to identify and motivate the core components of the FACCE, shown as yellow rectangles in the figure.

To **assure** cloud-based email conformance, the FACCE uses the components and relationships as described in the internationally accepted framework for assurance: the IFAE. To be able to assure cloud-based email *criteria* for cloud-based email, conformance must be established. The criteria should then be assessed for suitability by a *practitioner* and be communicated to the *responsible party* and intended user and used as a basis for collecting

and analysing *evidence* that cloud-based email is being implemented, governed and managed in a compliant manner. The results of the assurance engagement should be summarised in an *assurance report* communicated to the *intended user*.

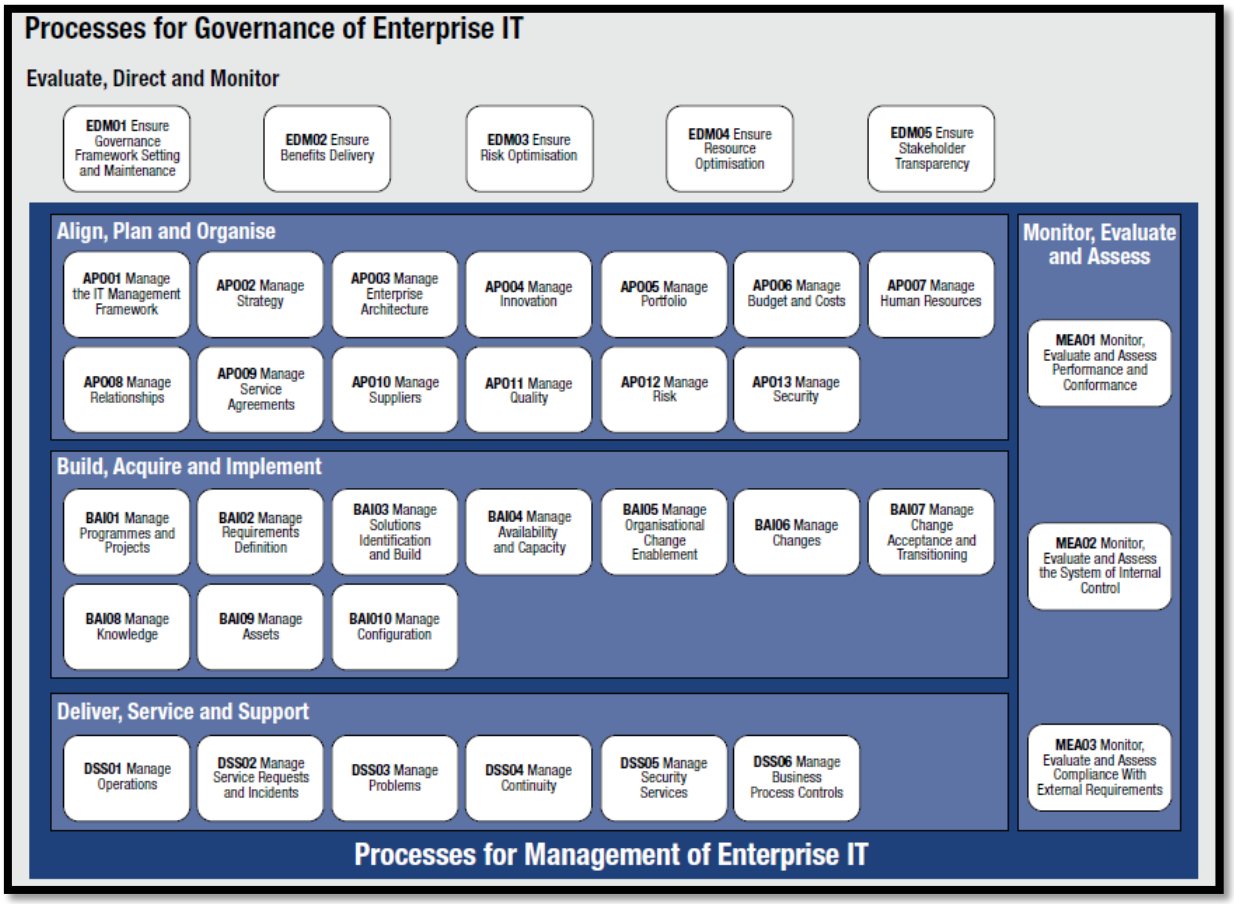


Figure 6.6 The governance and management processes that form part of COBIT 5 (ISACA, 2010b)

To address the **conformance** of cloud-based email, the FACCE describes how components and relationships necessary for IT conformance as part of IT governance can be used with the components and relationships for assurance. The FACCE describes how this is achieved in terms of a *methodology* and *guiding information* that informs how cloud-based email conformance should be achieved.

The *guiding information* consists of a set of documents that contain requirements for cloud-based email conformance or *conformance requirement documents*. As stated earlier, ISO/IEC 38500:2008 specifies that conformance involves complying with 1) legal and regulatory obligations: regulatory, legislation, common law and contractual obligations and 2) internal requirements as set forth in: internal policies, standards, professional guidelines and systems for IT governance (ISO, 2008, p. 22). Guiding information for cloud-based

email conformance, therefore, contains various *laws and regulations* that relate to cloud-based email at higher education institutions. They also relate to documents outlining the *IT governance structure* used by the institution, *standards and professional guidelines* and *internal policies*.

The guiding information is used in the *methodology* for assuring the conformance of cloud-based email with FACCE. The methodology describes how conformance of cloud-based email can be governed and managed to assist organisations in assuring conformance. The macro methodology for assuring cloud-based email conformance as described in the FACCE is based on the governance tasks of *evaluate, direct* and *monitor* as described in the IT governance model in ISO/IEC 38500:2008. The detailed description of the methodology is discussed in the next stage of description.

This first stage description of the FACCE aimed to:

- Make it clear that the FACCE is a framework for assuring conformance that is based on accepted frameworks, standards and best practice guidelines for assurance and conformance as part of IT governance.
- Help identify and explain the core components and relationships of the FACCE as shown in yellow in Figure 6.7. It should now be possible to look at this figure and both 'pick out' and understand the role of each of the core components for the FACCE.

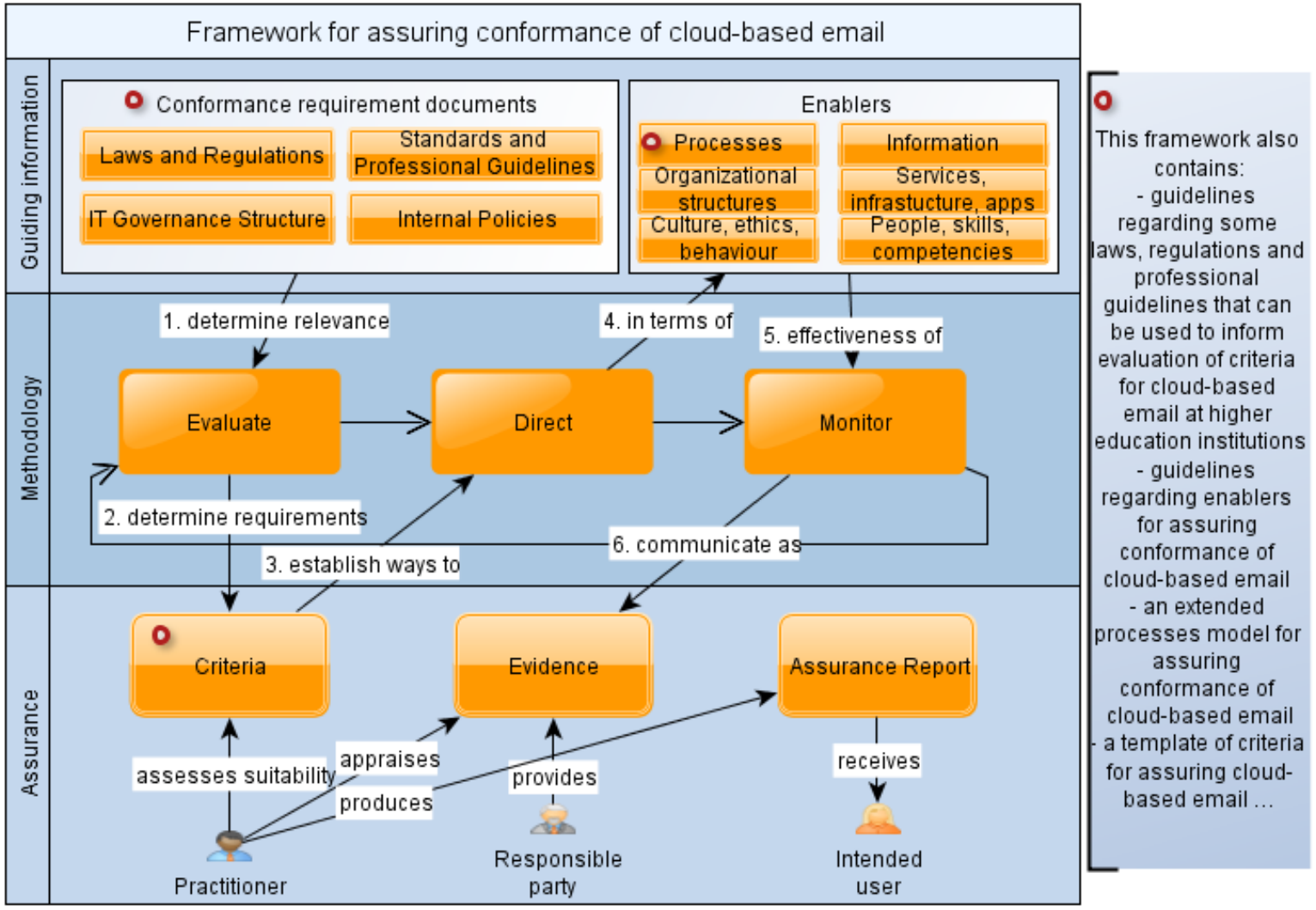
Exactly how this framework can be used for assuring the conformance of cloud-based email has not yet been fully addressed. The next section provides further detail.

6.3.2 Stage 2: Describing a methodology for assuring conformance

The previous section has highlighted key components and relationships that are part of a framework for assuring the conformance of cloud-based email (FACCE). The manner in which these components interact together to assure cloud-based email conformance is described in this subsection. This interaction between components is described mainly in terms of the methodology that binds these components together.

As stated previously, the macro methodology for assuring cloud-based email conformance as described in the FACCE is based on the tasks that ISO/IEC 38500:2008 describes as necessary for ensuring conformance from an IT governance perspective. These tasks are: *evaluate, direct* and *monitor* conformance initiatives. The core role of these tasks becomes clear in the description of the micro methodology of the FACCE that follows.

Figure 6.7 **A Framework for Assuring the Conformance of Cloud-based Email (FACCE)**



The micro methodology for assuring cloud-based email conformance at higher education institutions in South Africa includes the six steps shown as numbered arrows in Figure 6.7 and described below. The related core task for governing conformance is shown in bold in the description of each step in the methodology. The other core components are highlighted using italics for each step.

1. As per number one (labeled as '1. determine relevance') in Figure 6.7, the first step is to **evaluate** *conformance requirement documents* to determine the relevance of the contents of these documents with regard to cloud-based email conformance. This is clearly an important step, since it is impossible to assure conformance unless there is a clear picture of what an institution is required to conform to. A full set of relevant conformance requirement documents should, therefore, be identified and evaluated for relevance regarding cloud-based email. Depending on how cloud-based email is used and implemented at various institutions, different conformance requirement documents may apply. To illustrate, the laws and regulations that would apply to institutions regarding document retention may differ depending on who is using the cloud-based email system (for example only students or staff and students). The type of information that is solely managed by the CSP (for example if only students use cloud-based email while staff email is provisioned in-house, any correspondence between staff and students would still be stored on internal email servers, therefore, only email correspondence between students would be solely managed by the CSP) may also influence which requirement documents are relevant.
2. **Evaluate** relevant conformance requirement documents to determine requirements for cloud-based email conformance. The documents identified as relevant in the previous step can now be evaluated to specify what exactly is required from higher education institutions. The requirements identified should be communicated as *criteria* for assuring cloud-based email conformance. Having a clear set of criteria for cloud-based email conformance provides an important basis for assuring cloud-based email conformance. Criteria can be examined from an assurance perspective to establish relevance for an assurance engagement. Once this has been done, all actors (practitioners, responsible parties and intended users) have a clear understanding of what is required for cloud-based email conformance and of how to proceed as described in the next step.

3. Use the established *criteria* for assuring cloud-based email conformance to establish directives. Examining the criteria for cloud-based email conformance assists in determining how to meet these requirements and, therefore, how to **direct** activities accordingly. This is especially true if guidelines for accomplishing criteria are captured where possible when evaluating the requirements.
4. **Direct** initiatives to support cloud-based email conformance in terms of *enablers*. Directives for cloud-based email conformance should be communicated in terms of enablers. There will usually be at least a process in place to ensure that the directives are carried out efficiently.
5. **Monitor** the effectiveness of initiatives involving one or more *enablers* for cloud-based email conformance. The maturity of processes for cloud-based email conformance should be periodically evaluated, and the results should be recorded. Where possible, tools should be used to automatically monitor and record cloud-based email activities and incidents.
6. **Monitor** the effectiveness of activities for assuring cloud-based conformance, and communicate what has been established as *evidence*. Using a simple automated tool to continuously record the results of any monitoring activities described in step five will allow institutions to get an indication of how they are measuring up to criteria at any given stage. This allows institutions to easily recognise where improvement is required and can build trust that cloud-based email is used efficiently within the institution.

This methodology should be used in a continuous and iterative manner. As the legal, IT and other aspects of the environment in which higher education institutions change and progress, relevance of conformance documents and criteria should be periodically reassessed. As feedback is received regarding the effectiveness of initiatives for cloud-based conformance, and as guidelines and the IT capabilities change, directives regarding the use of enablers for cloud-based email should be updated. The environment and effectiveness of initiatives should be continuously monitored, and this information be made available to relevant parties. Reports generated based on this framework can be stored as conformance requirement documents that are later reviewed to determine criteria for cloud-based email conformance.

The components and relationships that make the FACCE a practical ideal type micro-conceptual framework could be useful in improving assurance of cloud-based email conformance should now be evident. For the FACCE to be of use for cloud-based email

specifically, however, it also provides more detailed guidance to assist in accomplishing this, as described in the next subsection.

6.3.3 Stage 3: Cloud-based email guidance

The first two stages of describing the FACCE have provided a high-level understanding of how the FACCE can be used to assure cloud-based email conformance. The FACCE needs to be easy, though, to implement at higher education institutions in South Africa and achieve real value. Accordingly, more detailed guidance regarding cloud-based email at higher education institutions is necessary. The FACCE provides this level of detail, as is illustrated by the red circles and explanatory notes on the side of Figure 6.7. This detail is summarised in this last stage of the FACCE description. More detail regarding this detailed guidance is available in Appendices A1 – A4.

There are several areas in which more guidance is provided to assist in implementing FACCE. These include:

- A recommended reference list of conformance requirement documents to consider for cloud-based email conformance in South African higher education institutions. (Appendix A1)
- Guidelines that can serve as a basis for creating an extended processes model for cloud-based email conformance. Guidelines for cloud-based email specific processes, such as a process for determining legal risk for cloud-based email, are outlined. (Appendix A2)
- A guiding list of criteria to assure cloud-based email conformance. (Appendix A3)
- A prototype tool for capturing and analysing data gathered when applying FACCE. (Appendix A5)

Each of the detailed elements listed above are briefly explained in the following paragraphs.

As stated earlier, it is clear that an important part of assuring conformance is determining what exactly higher education institutions are required to conform to regarding cloud-based email. As shown in Figure 6.7 and discussed before, the FACCE broadly describes the type of documents that should be considered for cloud-based email conformance: documents outlining legal and regulatory obligations, documents describing the IT governance structure used for the institution, various standards and professional guidelines that are relevant to cloud-based email at higher education institutions and internal policies. The FACCE outlines **recommended reference lists** of laws and regulations and standards and professional

guidelines that are likely to contain relevant guidance regarding cloud-based email compliance for higher education institutions in South Africa. These reference lists are not necessarily complete, neither are all documents referred to in them necessarily relevant to all higher education institutions in South Africa. It remains each institution's responsibility to determine a complete list of relevant conformance requirement documents. The reading lists do assist with this task, though. They provide an overview of what could be considered for cloud-based email conformance.

Understanding which laws and regulations are relevant and how they are to be interpreted is not a trivial matter. Furthermore, as established in previous chapters, understanding which laws and regulations apply to cloud computing solutions is generally an even more challenging process, given that cloud computing solutions may be run across multiple jurisdictional borders. This is true of cloud-based email in South Africa. Higher education institutions using this solution should not only consider the impact of South African laws and regulations regarding cloud-based email but also the relevant laws that govern the country under which the CSP is bound. This is true whether or not the email is accessed from a proxy server in South Africa. Since this is the case, the recommended reading list for legal and regulatory obligations includes both South African laws and regulations that may be relevant and American laws and regulations that may be applicable. It is highly recommended that legal advice is sought when institutions scrutinise these and other laws and regulations that institutions consider relevant for cloud-based email conformance. In addition to a list of potentially relevant laws, Appendix A1 also provides a list of potential legal issues that may form a basis for a discussion regarding legal risks with such legal experts.

The vast and possibly confusing array of relatively new guidelines for cloud computing has been discussed in Chapter 4. The recommended reference list for cloud-based email related standards and professional guidelines is, therefore, made up in part by the various standards and guidelines that have been discussed in Chapter 4. Guidelines specifically for cloud-based email provided by CSPs are not included here since they will obviously be relevant.

Recommended reference guidance is not provided for the IT governance structures used at higher education institutions, since it is assumed institutions have already adopted an IT governance structure that guides all IT initiatives within the institutions. There is, however, guidance given regarding how this should be used to determine criteria in Appendix A2.

Since internal policies will differ depending on the institution being considered, a recommended reference list for internal policies is also not provided.

In addition to the recommended reference lists, the FACCE provides guidance about certain **cloud-based email specific processes** that can be used to form an extended processes model for assuring cloud-based email conformance. Appendix A2 describes processes for tasks such as assuring legal and regulatory compliance (Viljoen, Von Solms, & Lawack-Davids, 2012), for analysing IT governance structures to determine cloud-based email conformance requirements, for assigning roles and responsibilities for cloud-based email conformance to staff and other processes.

Another area of guidance for the implementation of the FACCE is a **sample list of criteria**. The list of criteria can be used as a basis for cloud-based email conformance initiatives at any higher education institution in South Africa. This list addresses many areas of concern that should be considered. In addition, it structures these criteria in a manner that allows for easy reporting based on criteria in line with best practice. The categories of criteria for cloud-based email conformance in the list are based on relevant existing process goals outlined in COBIT 5. The criteria in these categories should be transferable to other ways of categorising that institutions may choose. It is recommended, however, that the categories should be chosen in a manner that can be easily linked to certain categories outlined in the IT governance structure used by the higher education institution. This allows for reports regarding adherence to criteria to be easily generated in a manner that is easily understood and put in context, since it is communicated in terms of the accepted IT governance structure of the institution.

The FACCE also includes a prototype tool for capturing conformance and assurance related information regarding cloud-based email. This tool is not meant to be a fully functional system that can be implemented as-is at higher education institutions to support the FACCE, but it does provide a prototype system that provides the basic mechanisms needed to support FACCE. These mechanisms can be fully enhanced and implemented at a later stage. The prototype tool provides a mechanism for storing criteria and information about the criteria such as the source (for example, a best practice guideline or internal policy) that motivates the criteria. This ensures that the criteria used for assurance of cloud computing services are based on an analysis of best practice guidelines and other relevant internal and external guidelines and standards. In addition, the prototype tool allows one to store reference to any relevant guidelines associated with the criteria that may be found during the evaluation of the

conformance requirement documents. This assists in the processes of using the criteria to create directives that are in line with guidelines for good practice. In addition, the prototype tool provides a mechanism for assisting institutions with capturing and storing information about evidence that criterion is met and that processes and activities are in place.

Capturing all the information described in the previous paragraph in the manner outlined in the prototype tool allows for the generation of reports that reflect what is required in terms of assuring cloud-based email conformance, how these requirements are derived, the extent to which these requirements are being met and where attention should be given to address problems in this regard. The information in such reports can be communicated to various relevant parties.

The description of the FACCE as presented in the three stages discussed in this chapter has explained how the FACCE can be used to assist in aiding the assurance of cloud-based email conformance at higher education institutions in South Africa. The first stage has clarified how the FACCE uses components and relationships recognised as necessary for a best practice based approach to ensure assurance and conformance. The second stage has described a methodology that binds these components together in a manner that can be used for assuring the conformance of cloud-based email. The final stage has provided further guidance that can be used when implementing the FACCE at higher education institutions in South Africa.

6.4 Value of the FACCE

Cloud-based email is a solution that offers higher education institutions the opportunity to take advantage of a necessary service (email) being provisioned and maintained by a service provider for free. There would evidently be great advantage in being able to access such a service. Higher education institutions, therefore, ought to take advantage of opportunities like this. However, they must also ensure that this is done in a manner showing due care that conforms to requirements of good governance, legal and regulatory obligations and good practice. FACCE assists in this regard by providing a means for *assuring the conformance* of cloud-based email for higher education institutions. Some of the characteristics of FACCE that make it a desirable solution are outlined in the following paragraphs.

FACCE is aligned closely with good practice for assurance, conformance and IT governance as outlined in an international framework for assurance engagements, ISO/IEC 38500:2008

and COBIT 5 specifically. Using such a best practice-based approach assists in demonstrating *due diligence*, since it can be argued that, by following such an approach for assuring conformance, reasonable steps have been taken to avoid committing a tort or offence.

In addition, the FACCE is based strongly on standards and guidelines for IT governance, especially in the area of conformance. It can, therefore, be used to demonstrate good *IT governance* in the area of cloud-based email conformance.

Since assurance is strongly related to building confidence and trust, FACCE could also be used to assist in building *trust and confidence* in the compliant use of cloud-based email at higher education institutions.

Clearly, the FACCE could assist higher education institutions in taking advantage of the opportunities related to the use of free cloud-based email in a manner that assures conformance. It also meets the objectives for a solution to the problem: the lack of structured guidelines for assuring the conformance of cloud-based email is putting this service at risk in higher education institutions in South Africa**.** The next chapter will verify the effectiveness of the FACCE in this regard.

6.5 Conclusion

The fact that the lack of structured guidelines for assuring the conformance of cloud-based email is putting this service at risk in higher education institutions in South Africa is a definite problem, and it has been highlighted repeatedly in this work thus far. This chapter has outlined a Framework for Assuring the Conformance of Cloud-based Email (FACCE) that can be used to address this problem. The FACCE uses a best practice based approach to assure conformance. This is accomplished by using components and relationships described as essential for assurance in an internationally accepted framework (IFAE) and components and relationships that are recognised to promote conformance in the context of IT governance by the standard for IT governance (ISO/IEC 38500:2008) and a widely accepted best practice guide for IT governance (COBIT 5). It provides a structured methodology that can be used repeatedly for assuring cloud-based email conformance. It also provides detailed and structured guidelines that can be used to implement this framework at higher education institutions in South Africa.

In addition to designing and developing an artifact, demonstrating and evaluating (as described by Peffers et al., 2008) the artifact should be completed according to the design science research methodology described at the outset of this chapter. How this is done is outlined in the following chapter.

CHAPTER 7

FACCE verification

7.1 Introduction

A framework for assuring the conformance of cloud-based email (FACCE) has been motivated, designed and presented. As shown in Figure 7.1 and explained in detail in Chapter 2, the design science research methodology described by Peffers et al. (2008) has been used to guide and describe the design and development of the FACCE. The problem addressed by the FACCE has been defined, and the importance of the problem has been motivated. The objectives of the FACCE have been identified, explained and motivated. Finally, the design and development of the FACCE as an artifact has been described in the previous chapter. As shown in green in Figure 7.1, the remaining steps of the design science research methodology - demonstrating and evaluating the artifact - are still to be conducted. This is done in this chapter. The evaluation described here also satisfies the design science principle of design evaluation described by Hevner et al (2004). The steps of demonstrating and evaluating the artifact serve as the means of verifying the utility, quality and efficacy of the framework.

The chapter begins by describing how the utility of the FACCE has been demonstrated in a suitable context; a South African higher education institution that has been using cloud-based email for a number of years. The chapter then describes how the FACCE has been evaluated and presents the results of the evaluation.

7.2 FACCE Demonstration

Demonstration is a required activity in the design science research methodology described by Peffers et al. (2008). According to these authors, this requires one to demonstrate "the use of the artefact to solve one or more instances of the problem. This could involve its use in experimentation, simulation, case study, proof, or other appropriate activity" (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2008, p. 55).

The use of the FACCE has been demonstrated at a South African university, which will hereafter be referred to as 'the University'. The University has been using cloud computing to provision email services for students since 2009. The University was one of the pioneers

in the adoption of this cloud computing service in South Africa. In 2007, the University started testing the use of the service. In 2008, the University used a pilot group of students to test the cloud-based email system while still running an in-house email service for all students. Early in 2009, the University started using cloud-based email for all newly enrolled students. Microsoft is the University's CSP for student email. Originally, the service was provisioned as Live@Edu. In August of 2013, Microsoft upgraded this service to Office 365 at the University.

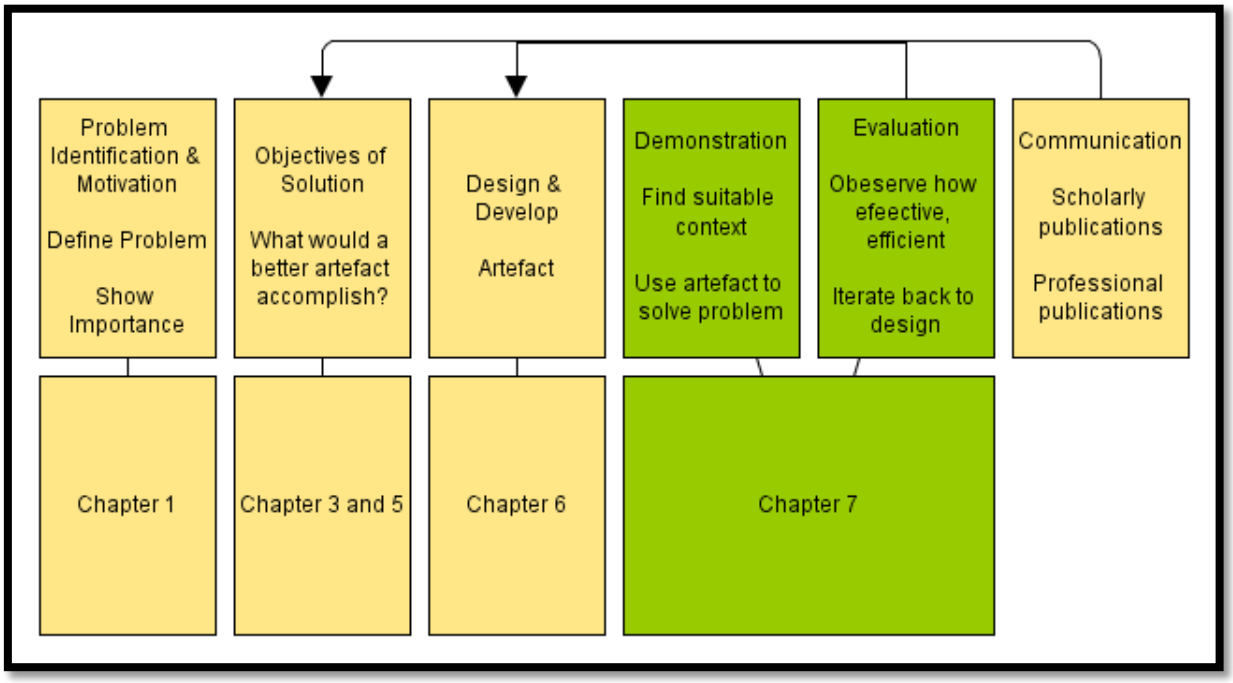


Figure 7.1 Chapter in relation to the activities for the DSRM

This section describes how the FACCE was used at the University and the findings of this demonstration.

7.2.1 Implementation at University

The steps that were taken for the demonstration of FACCE at the University can be categorised and described in a number of phases. These are described below:

Phase 1: Choose conformance areas to be used for demonstration purposes

FACCE includes a guiding list of sample criteria. This list contains some high-level criteria for cloud-based email conformance that should be considered and (where applicable)

expanded into more detailed criteria for conformance by each institution. This high-level criterion is shown in Table 7-1.

For the purposes of the demonstration of FACCE at the University, two of these areas were chosen to apply and demonstrate the utility the methodology outlined in FACCE. The conformance areas chosen were 'manage roles and responsibilities' and 'project management.' Once this was done, the phases described in the following subsections were applied to each of these areas.

Phase 2: Gather and evaluate relevant conformance requirement documents.

As described in the FACCE methodology, it is important to gather a full set of relevant conformance requirement documents that can be used to get an accurate understanding of what is required for conformance. To achieve this during the demonstration of FACCE, staff members were interviewed to determine the requirements for conformance in the areas of managing roles and responsibilities and ensuring project management. Information regarding the following types of documents was analysed:

- The IT governance structure for the institution
- Internal policies related to the conformance areas
- Any relevant requirements in contracts or SLA with the CSP
- Any legal risks identified and sources (laws or regulations) that describe the legal risk
- Any guidance/best practice advice that guides the use of cloud-based email (including any guidance provided by the CSP)

The following conformance requirement documents were identified for the two areas of conformance under investigation:

- The University uses principles outlined in COBIT 5 and ITIL in the governance of IT.
- There are a number of internal policies that were identified as relevant including policies regarding how contracts should be dealt with at the University and policies regarding how significant projects at the University are dealt with.
- It is standard practice within the ICT department of the University that significant changes to any IT system are dealt with as a project.
- Various documents, emails, web sites and other resources provided by the CSP that provide guidance on various aspects of cloud-based email management and practice were identified.

- Best practice guidance described in the recommended reference list (a component of the FACCE) relating to managing roles and responsibilities for cloud computing were identified as relevant.
- It was determined that the University uses principles from various best practice guidelines, such as Prince 2, to guide project management.

Conformance area	Criteria	High-level process	Cloud-based email specific process
Internal Compliance	Cloud-based email initiatives should be aligned with the overall strategy and other high-level directives provided in the institution's IT governance and management framework.	NA	FACCE: P1
Risk Management	Risks related with cloud-based email should be identified, assessed and mitigated in a manner that is in line with the risk appetite and risk management strategy of the institution.	COBIT 5: EDM03 (Ensure Risk Optimization), APO12 (Manage Risks)	FACCE: P2
External Compliance	The institution should ensure and gain assurance that it complies with all requirements related to cloud-based email imposed on it by legal and regulatory bodies.	COBIT 5: MEA03 (Monitor and evaluate compliance with external requirements), APO12 (Ensure risk management)	FACCE: P3, P2
Value Optimization	It should be ensured that optimal value is achieved through the use of cloud-based email by ensuring that anticipated value of cloud-based email is evaluated and communicated and that goals for achieving value are monitored and attained.	COBIT 5: EDM02 (Ensure Value Optimization)	FACCE: P4
Manage relationship with CSP	Relationships with the CSP should be managed, ensuring that the service provided meets business requirements, the CSP is operating in an effective and compliant manner and that contracts and SLAs are managed.	COBIT 5: APO09 (Manage Service Agreements), APO10 (Manage Suppliers)	FACCE: P5
Manage roles and responsibilities	It should be ensured that all parties concerned are aware of and able to carry out their responsibilities related to cloud-based email.	COBIT 5: APO07 (Manage Human Resources), APO08 (Manage relationships)	FACCE: P6
Ensure proper project management	The adoption of cloud-based email should be treated as a project and, as such, all applicable guidelines for project management used by the institutions should be applied.	COBIT 5: BAI01 (Manage programmes and projects)	FACCE: P7
Ensure security	The security of cloud-based email at the institution should be insured.	COBIT 5: DSS07 (Manage security)	

Table 7-1 FACCE guiding list of sample high-level criteria

Information regarding relevant conformance requirement documents identified in this phase of the FACCE demonstration were captured and stored in the database of the prototype tool that is part of FACCE.

Phase 3: Evaluate conformance requirement documents to identify criteria

Once the conformance requirement documents were identified, they were analysed to determine further criteria to support the high-level criteria associated with the conformance areas of managing roles and responsibilities and ensuring project management for cloud-based email. This was done in consultation with members of staff at the University. For clarity, in this chapter only some of the criteria identified in the demonstration of the FACCE are described. These criteria will be used to describe the subsequent phases of the FACCE demonstration as well. They serve to illustrate the use of FACCE at the University. These criteria are described below:

- Based on an internal policy adopted by the University, it was determined that a requirement for internal conformance was: to ensure that the legal department receives and reviews contracts with CSP.
- Based on guidance by bodies such as COSO and ENISA regarding the importance of ensuring that organisations identify legal risks associated with cloud computing, the following criterion was identified for the University: An entity should be responsible for ensuring that the institution's use of cloud-based email and related services comply with applicable laws and regulations, taking into account that the CSP may be under the jurisdiction of another country.
- Based on guidance from COBIT 5 which stresses the importance of monitoring performance and conformance, the following criteria were determined: There should be an annual review of effectiveness and conformance of the cloud-based email service. The contractual compliance review is the responsibility of the Information security officer and the engineer of messaging services. The review of availability and performance management is the responsibility of the engineer of messaging services.

As mentioned previously, the three criteria listed above will be used to illustrate how the following phases of the FACCE demonstration took place at the University. The criteria identified, the sources that motivated the criteria and any guidelines for meeting the criteria were once again captured and stored by the prototype tool for implementing the FACCE.

Phase 4: Monitor effectiveness of processes and activities in place for criteria for cloud-based email conformance

The next steps in the methodology for assuring the conformance of cloud-based email (as explained by the FACCE) is to analyse the criteria to determine directives that describe how various enablers are to be used to meet criteria. The University where FACCE has been demonstrated has been using cloud-based email for a number of years already, and has many directives and processes and activities in place to ensure that the directives are achieved. The next phase of the demonstration of the FACCE, therefore, encompassed the last two steps in the FACCE methodology, monitoring the extent to which enablers are being used to meet the criteria for cloud-based email conformance. Once again this was achieved by means of a structured interview with various members of IT staff at the University. Each member of the staff was asked to:

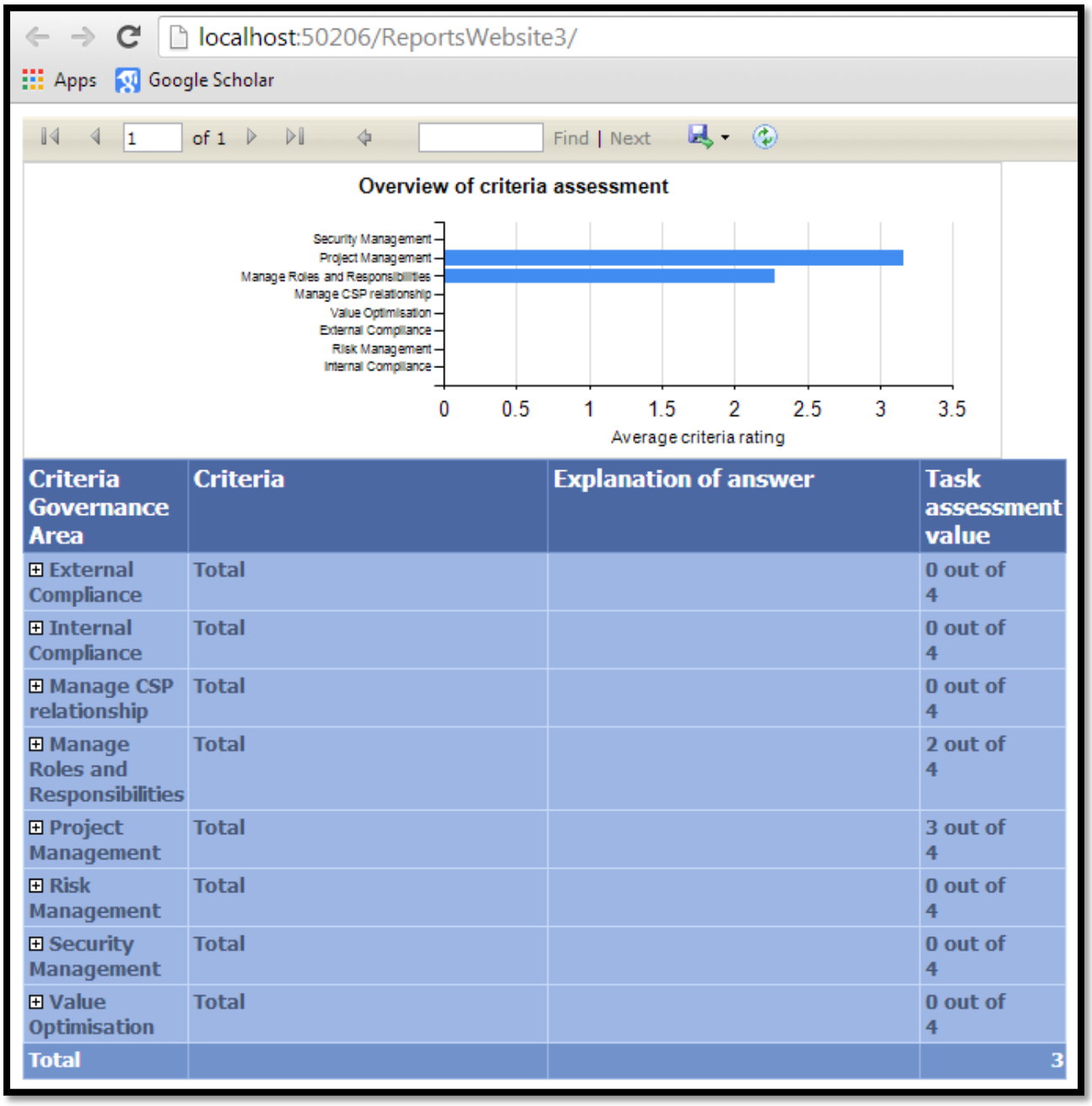
- Rate the extent to which the identified criteria were being met on a scale of zero to four. A rating of zero would indicate that the criteria had not been met at all. A rating of 4 would indicate that the criteria had been fully satisfied.
- Explain their rating. This explanation would include a description of relevant enablers involved to satisfy the criteria where appropriate.
- Provide evidence of their answers. This could include various different types of documents including emails, policies, plans, meeting agendas or a simple written explanation of a process that could be followed to retrieve evidence.

The results of this investigation were captured and stored in the FACCE prototype tool. The results of this investigation are discussed in the next subsection.

Phase 5: Report on the findings

All the information gathered during the preceding phases of the demonstration of the use of FACCE at the University was captured into a database by the FACCE prototype tool. If the FACCE were to be fully implemented, there would have to be mechanisms in place to ensure the validity and accuracy of all information gathered in such a process. The demonstration of the FACCE at the University shows that the FACCE can be used as the basis for carrying out such activities at South African higher education institutions, although it was not a full implementation of the FACCE. Storing the information gathered during this demonstration of the FACCE methodology in a central place, however, allows one to analyse this

information in various ways. By storing information about the criteria, the best practice guidelines and other conformance requirement documents that motivate the criteria, information regarding directives and the results of monitoring activities related to the criteria a number of useful reports can be produced. During the demonstration of the FACCE, the prototype tool merely produced some basic reports that illustrate how this can be done.



Criteria Governance Area	Criteria	Explanation of answer	Task assessment value
⊞ External Compliance	Total		0 out of 4
⊞ Internal Compliance	Total		0 out of 4
⊞ Manage CSP relationship	Total		0 out of 4
⊞ Manage Roles and Responsibilities	Total		2 out of 4
⊞ Project Management	Total		3 out of 4
⊞ Risk Management	Total		0 out of 4
⊞ Security Management	Total		0 out of 4
⊞ Value Optimisation	Total		0 out of 4
Total			3

Figure 7.2 Sample report by FACCE prototype tool

One of the types of overview reports produced by the prototype tool is depicted in Figure 7.2. As can be seen in the figure, only the two areas of conformance (project management

and managing roles and responsibilities) were implemented and reported on during the demonstration of FACCE at the University. The report allows institutions to get an overall view of the level of assurance that is associated with the conformance of cloud-based email. To receive more details about the criteria associated with the particular conformance area, one can drill down into the report to see the related criteria and information regarding the extent to which the criteria have been met.

Figure 7.3 depicts another type of report that can be produced when cloud-based email assurance and conformance related information is gathered and stored as outlined by the FACCE. This report assists with answering questions such as: Why do we approach activities related to cloud-based email as we do?

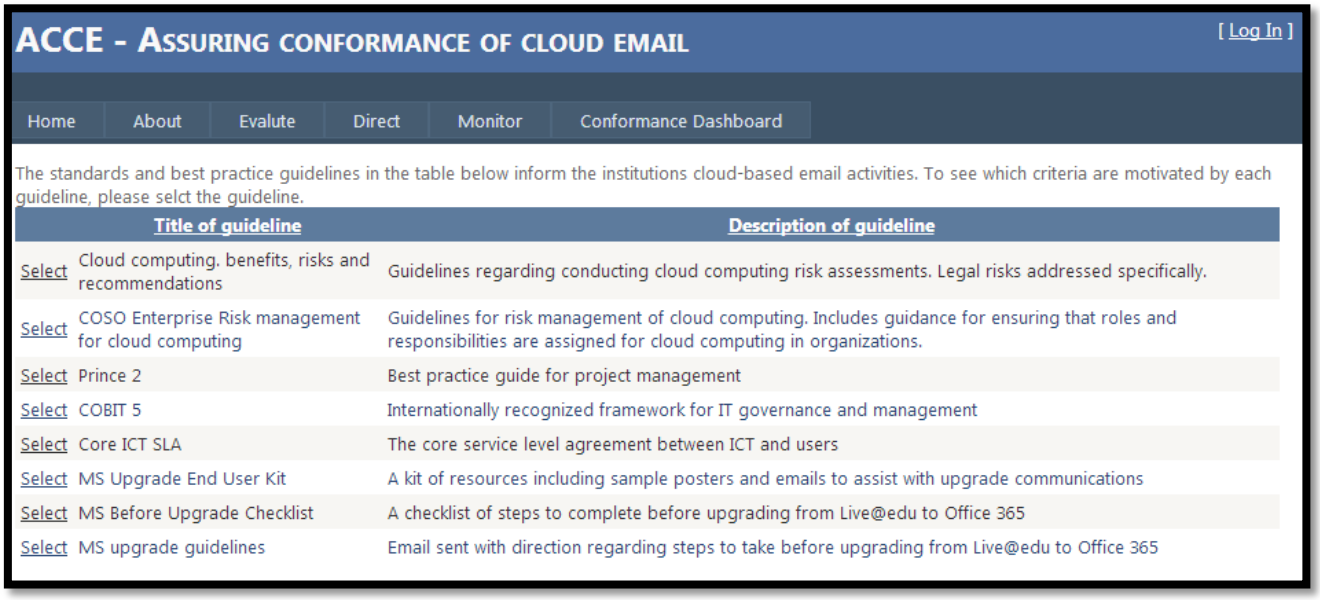


Figure 7.3 Second sample report of guidelines related to cloud-based email activities

The report assists with answering such questions by providing a list of best practice guidelines and other conformance requirement documents that are related to criteria. Once again, one can drill down into a report like this by selecting a guideline and viewing a list of criteria that are motivated by that conformance requirement document.

Phase 6: Establish directives for the conformance of cloud-based email

During the demonstration of the utility of the FACCE at the University, the reports and other findings were discussed with IT managers. Based on this, the managers were able to analyse where new directives had to be given or existing directives adjusted. For example, the results of the demonstration highlighted the fact that a criterion for internal conformance was that

the University's contract with the CSP had to be lodged with the legal department at the University. This criterion was based on an internal policy that came into effect after the implementation of the FACCE at the University. Accordingly, management issued the directive that the correct procedure was to be followed to lodge the contract with the legal department.

Another result of the demonstration was that the University decided to investigate ways in which mechanisms could be put in place to ensure that appropriate legal advice was sought in determining legal risks associated with cloud-based email and any other cloud computing solutions the University would consider employing in the future. This decision was made, to a certain extent, because of the best practice guidance referred to in the FACCE's recommended reference list and guidance in the cloud-based email-specific process for assigning roles and responsibilities.

Other areas that warranted attention include ensuring that internal procedures for maintaining the cloud-based email service were recorded and recognising the legal department as stakeholders in appropriate cloud-based email and other computing projects and managing their engagement. Criteria related to change projects (like the upgrade to Office 365) were generally well met. This was attributed in part to good guidance, communication and support from the CSP.

The six phases described in this section show how the utility of the FACCE has been demonstrated at a South African higher education institution that uses cloud-based email. The next section clarifies how this has accomplished the design science goal of establishing the utility of the framework as the artifact of this work.

7.2.2 Findings of Demonstration

From the preceding description of the demonstration of the FACCE, it should be clear that this framework can be successfully used to improve the assurance of cloud-based email conformance at South African higher education institutions. The phases that are described in the previous section for implementing the FACCE at the University are based firmly on the methodology outlined in the FACCE. All the components of the FACCE (conformance requirement documents, enablers, criteria, evidence and reports regarding assurance) were used and demonstrated at the University. In addition, the more detailed elements of the FACCE (the sample list of high-level criteria, the recommended reference list and the prototype tool for capturing and analyzing conformance and assurance data) have also been

successfully used at the University to support the approach encouraged by FACCE for improving the assurance of cloud-based email.

The utility of the FACCE is also demonstrated in the feedback from the University. Although the University has much experience using cloud-based email and has mature processes and activities in place to ensure conformance of this service, the University was able to follow the methodology and supporting elements of the FACCE to determine where action could be taken to improve the overall cloud-based email conformance. This should be clear from the description of phase six of the demonstration of the FACCE. Staff members at the University also commented that they would use the principles of the FACCE when investigating the adoption of other cloud computing solutions at the institution. They also commented on the benefits of having a holistic view of what activities and initiatives were in place to ensure the conformance of cloud-based email conformance. This holistic view was aided by going through the methodology promoted by the FACCE and capturing and communicating the information with the aid of the prototype tool for the FACCE implementation. This improved communication gives staff more confidence in the conformance of this service. Staff also commented that they would have benefitted from using the approach promoted by the FACCE when they first began using cloud-based email.

Clearly, it has been demonstrated that the FACCE provides a framework that can be useful to higher education institutions in South Africa for assuring the conformance of cloud-based email. The framework is flexible and can be used by institutions that have been using cloud-based email for some time already or by institutions that are starting out with the project of investigating the adoption of cloud-based email. The detailed elements of the FACCE (the sample list of high-level criteria, the recommended reference list and the prototype tool for capturing and analyzing conformance and assurance data) can be used as a basis for the implementation of the FACCE. These elements should, however, be refined and expanded upon in further work.

The process of applying the FACCE at the University has clearly demonstrated the fact that the artifact from this work can be used to solve an instance of the problem of improving the assurance of cloud-based email compliance at higher education institutions in South Africa.

In demonstrating the FACCE at the University it has also been possible to observe and measure how well the artifact supports a solution to this problem. This is the requirement set

out in the fifth activity of the design science research methodology: evaluation. How this requirement has been met in this work is described in more detail in the next section.

7.3 FACCE Evaluation

As mentioned previously, another activity in the design science research methodology is to evaluate the artifact. According to the authors of the methodology, to do this, one must "observe and measure how well the artefact supports a solution to the problem." It also involves "comparing the objectives of a solution to actual observed results from use of the artefact in the demonstration" (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2008, p. 56). This section describes how the FACCE has been evaluated.

7.3.1 Method of evaluation

Pries-Heje, Baskerville and Venable (2008) describe a framework for artifact evaluation in which the evaluation is described in terms of *what*, *how* and *when*. According to this framework, evaluation may occur ex ante (before the system is constructed), ex post (after the system is constructed) or both. These terms are used to describe *when* an evaluation occurs. *What* is evaluated is described either a design process or a design product. When deciding *how* to evaluate an artifact either naturalistic or artificial forms of evaluation can be chosen. Artificial evaluation is conducted in "a contrived and non-realistic way" (Pries-Heje, Baskerville & Venable, 2008, p.4). Examples of methods for artificial evaluation include laboratory experiments, simulations and mathematical proofs. Naturalistic evaluation is done when the utility of an artifact is tested "within its real environment i.e., within the organization" (Pries-Heje, Baskerville & Venable, 2008, p.4). Figure 7.4 summarises how the FACCE has been evaluated in terms of the framework for artifact evaluation described by Pries-Heje et al. The following paragraph describes the FACCE evaluation in more detail.

The strategic framework for applying evaluation in design science research can be applied to the evaluation of the FACCE as follows:

- When has the evaluation been done? Ex Post. The FACCE is evaluated after it has been designed.
- What has been evaluated? A design process. In this context a design process is a set of guidelines that describe activities, methods and tools that can be used to guide the design of a product. A good design process should lead to the design of a good product. The FACCE describes a design process which can be used to guide the

production of a good system for assuring the conformance of cloud-based email at higher education institutions in South Africa.

- How has the FACCE been evaluated? A naturalistic evaluation has been done. A case study like approach has been used. As described in the previous section, the FACCE has been implemented at a South African university with the problem which the FACCE aims to address. In addition, surveys have been used to determine the perceived success of the FACCE in meeting its goals. The remainder of this section describes these two aspects of the evaluation of the FACCE in more detail. Firstly though, the objectives and criteria against which the FACCE is evaluated are described in the next paragraph.

	Ex Ante	**Ex Post**
Naturalistic	Design Process	**FACCE Evaluation:** P: demonstration and survey C: perceived success
	Design Product	
Artificial	Design Process	Design Process
	Design Product	Design Product

Figure 7.4 FACCE evaluation in terms of strategic framework for evaluation in design science (Pries-Heje, Baskerville & Venable, 2008)

To be able to evaluate the utility of an artifact, it is intuitive that one should clearly understand the objectives and criteria that the artifact aims to achieve. The objectives and criteria for the FACCE have been described and summarised in Chapter 5. They are repeated here for easy reference.

The objectives for a framework to assist with assuring the conformance of cloud-based email are listed below:

- Objective: Assist with promoting trust and confidence in the internal and external conformance of cloud-based email
    - Requirement: Assure conformance by using accepted assurance and conformance methods and techniques.

    - Requirement: Ensure that the framework addresses legal and regulatory conformance risks.
    - Requirement: Ensure that the framework addresses internal conformance requirements, including requirements in policies and internal governance structures.
    - Requirement: The framework should assist higher education institutions by promoting confidence that they are governing and managing cloud-based email in a manner that conforms to internal and external requirements.
- Objective: Assist with demonstrating due diligence
    - Requirement: Promote a best practice/standards based approach to assure conformance.
- Objective: Assist with achieving the goals of IT governance (strategic alignment and value optimization) for cloud-based email
    - Requirement: Ensure that the conformance and assurance activities promoted by the framework are strongly guided by best practice guidelines for IT governance.

The structured feedback form that was used in the evaluation of the FACCE can be found in Appendix A4. The feedback form is designed to determine whether the FACCE is perceived to be successful in meeting these criteria. The subsequent description of the evaluation of the FACCE will highlight how the objectives and criteria have been achieved.

The preceding sections have described how the utility and efficacy of the FACCE have been demonstrated at a South African higher education institution that is using cloud-based email. The demonstration has shown that the framework can be effectively used to identify and communicate information regarding the assurance and conformance of cloud-based email in a manner that helps institutions take steps to improve the overall conformance of cloud-based email. In addition, it promotes assurance that requirements for conformance have been met and that activities related to ensuring conformance are well motivated by best practice guidelines.

The FACCE has been further evaluated at the University, by means of collecting and analyzing structured feedback. It can be argued that an evaluation of an artifact by one organisation may not easily prove the utility of such an artifact for other organisations. The utility and value of the FACCE has therefore been further verified through the evaluation of

the FACCE by five other professionals with knowledge in the subject area. The evaluation by this second group of evaluators is described in subsection 7.3.3. The next subsection starts by describing the feedback from two members of staff at the University: the chief information officer (CIO) and the senior engineer of messaging services (hereafter simply referred to as the senior engineer). These individuals were asked to watch and listen to a presentation regarding the framework. This presentation included information about how the FACCE had been used at the University. The presentation is available in Appendix A6. They were then asked to provide their feedback using the report back form shown in Appendix A4. A document that summarises the FACCE was also provided to these staff members to refer to for more information. This document also contained the full-recommended reference list and sample high-level processes for cloud-based email (found in Appendices A1 and A2 respectively). The feedback from these staff members is discussed in the following subsection.

7.3.2 Evaluation results from individuals involved in the FACCEC demonstration.

As will be shown in this section, the feedback from the staff at the University demonstrates their belief that the FACCE meets the objectives set out for this framework. The objectives necessitate that the FACCE assists with improving levels of conformance and assurance related with cloud-based email at higher education institutions. Secondary objectives of the framework include that it promotes trust and due diligence regarding cloud-based email.

When asked, "Do you believe that using the FACCE as a guide for implementing a program for assuring cloud-based email conformance could improve the level of *assurance* associated with cloud-based email at your institution?" both staff members agreed with the statement. The CIO supported his answer by adding that the University currently did not have such a framework and that the FACCE is "detailed and interlinked". The senior engineer of messaging services commented that "The framework will be useful in that it highlights the requirements for assuring conformance of cloud-based email implementations. It will allow IT departments to ensure that a cloud-based email implementation meets internal policy as well as regulatory policy in South Africa. By taking a best practice approach, it will assist IT staff to ensure a holistic project management approach is taken that will include correct governance."

When asked "Do you believe that using the FACCE as a guide for implementing a program for assuring cloud-based email conformance would improve the level of *conformance* associated with cloud-based email at your institution?" the CIO agreed with the statement and the senior engineer strongly agreed. To substantiate his answer the senior engineer explained that conformance is a broad topic that can be difficult to fully grasp when one's job entails focusing primarily on "technical IT work". He then added that "Having a guideline that targets a specific service will make it easy for IT staff to improve conformance levels of that service."

From the above it is clear that the FACCE can be used to meet its primary objectives of improving the level of assurance and conformance at higher education institutions in South Africa. As explained in Chapter 3 trust, auditing and due diligence are three topics which are closely linked with the subjects of assurance and conformance. During the evaluation of the FACCE, staff members were also asked to provide their feedback with regard to the impact that FACCE has on these topics.

Regarding the potential to assist with easing the process of auditing cloud-based email related activities this question was raised: "Do you believe that using the FACCE as a guide for implementing a program for assuring cloud-based email conformance would make it easier to provide information for *auditing* cloud-based email?" Both staff members at the university agreed that it would. The CIO stated that "All the processes followed in the methodology leave an audit trail that any auditor should be satisfied with." The senior engineer said that "Auditors will use the same or similar criteria and guidelines to measure and will require evidence that these criteria and resulting process have been met and completed. By using the FACCE, the proof required will be centrally stored and easily found."

The feedback regarding the FACCE's impact on trust relating to cloud-based email provided an interesting insight into two perspectives on the matter of trust. This question was asked: "Do you believe that using the FACCE as a guide for implementing a program for assuring cloud-based email conformance could improve the level of *trust* associated with cloud-based email at your institution?" The senior engineer indicated that he neither agreed nor disagreed with the question. He explained "The only major "trust" concern with cloud-based email is that the CSP is an American company. With all the media coverage recently on the American government accessing private information, there will be a level of mistrust. I,

however, do not think that this will be negated by any means of assurance." This statement reflects what is stated in Chapter 5 regarding trust when it comes to cloud-based email. Generally, higher education institutions seem to have a relatively high-level of trust in cloud-based email services providers. This was demonstrated during an interview with the senior engineer during the demonstration of the FACCE at the University. There the senior engineer spoke about the University having had a good and long standing relationship with the CSP. He said that this was one of the reasons that they chose to use this CSP's service with cloud-based email instead of the services of a competitor. As described in Chapter 5, the level of trust in cloud computing services is also likely to increase as cloud computing services mature and become more widely used. The real problem was shown in Chapter 5 to be higher education institutions' trust that they are able to use the services provided by CSPs in a manner that complies with requirements imposed on them and not in the ability of the CSP to provide the service in a reliable manner. The CIO of the University reflects that he perceives that the FACCE can be used to improve trust in this regard. He agreed that the FACCE could be used to improve trust in cloud-based email services. In explaining his answer he added that "FACCE is linked to governance structures, policies, law and regulations" and that "FACCE considers monitoring aspects."

Regarding the impact of the FACCE on demonstrating due diligence, staff members were asked "Do you believe that using the FACCE as a guide for implementing a program for assuring cloud-based email conformance could assist in demonstrating *due diligence* with regard to cloud-based email at your institution?" The senior engineer agreed that FACCE could assist in this regard. He elaborated by stating "It [FACCE] will provide a means of proving that the identified criteria for assurance have been met and that good project management has taken place. While the work is often done [at the University], the proof of such is not centrally stored and adequate review therefore does not take place." The CIO strongly agreed that FACCE could assist with promoting due diligence with regard to cloud-based email. He said that "All the loops covered makes a strong case for due-diligence having been followed."

Evaluators of the FACCE at the University clearly have confidence that the FACCE can be used to assure the conformance of cloud-based email at higher education institutions in South Africa. The following subsection highlights how feedback from evaluators of the

FACCE that were not involved in the demonstration of the framework express similar confidence.

7.3.3 Evaluation results from individuals not involved in the FACCE demonstration.

In addition to the staff at the University, the FACCE has also been evaluated by five other professionals. The evaluators are:

- Evaluator A: The CIO of another South African university.
- Evaluator B: The IT Director of a third South African university.
- Evaluator C: The director of the school of IT at a college in the United Kingdom.
- Evaluator D: A manager at a South African branch of a prestigious international company that specialises in assurance. Evaluator D is an expert in IT governance and assurance.
- Evaluator E: An operations specialist at a leading South African communications service provider who has previously conducted research in the field of IT governance.

As can be seen from this list of evaluators, three of the five evaluators work at higher education institutions. Two of these represent South African universities and the third a college in a different country. The two evaluators at the South African universities were asked the same questions as the staff at the University where the FACCE has been demonstrated. The questions related directly to the use of the FACCE at their given institutions. The feedback form used for these evaluators is shown in Appendix A4. The other evaluators were asked slightly modified, more general questions regarding the utility of FACCE to South African higher education institutions in general. The questions posed to these evaluators are shown in Table 7.5.

Table 7.5 summarises the feedback provided by the evaluators regarding the FACCE. As can be seen from this table the majority of the evaluators indicate that the FACCE can be effectively used to achieve its objectives of improving the level of assurance, conformance and trust regarding the use of cloud-based email at South African higher education institutions.

Do you agree that using FACCE as a guide for implementing a program for assuring cloud-based email conformance could improve the level of *assurance* associated with cloud-based email at higher education institutions in South Africa?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
			1	3	1
Do you agree that using FACCE as a guide for implementing a program for assuring cloud-based email conformance could improve the level of *trust* associated with cloud-based email at higher education institutions in South Africa?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
			1	4	
Do you agree that using FACCE as a guide for implementing a program for assuring cloud-based email conformance would improve the level of *conformance* associated with cloud-based email at higher education institutions in South Africa?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
			1	3	4
Do you agree that using FACCE as a guide for implementing a program for assuring cloud-based email conformance could assist in demonstrating *due diligence* with regard to cloud-based email at higher education institutions in South Africa?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
			1	2	2
Do you believe that using FACCE as a guide for implementing a program for assuring cloud-based email conformance would make it easier to provide information for *auditing* cloud-based email?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
			1		
Do you believe that the principles demonstrated in the prototype tool (provided as a simple example of a tool for gathering and analysing cloud-based email assurance and conformance information) could be expanded and modified into a useful tool at higher education institutions in South Africa?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
			1	4	
Do you think FACCE would be practical and easy to implement?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
			1	4	

Table 7-5 Summary of feedback from five other evaluators

The majority of the evaluators are also of the view that the FACCE can assist with demonstrating due diligence regarding the governance of cloud-based email at higher education institutions in South Africa. These evaluators also believe that the FACCE could be easy to implement. There is a single evaluator who does not express the same confidence; Evaluator B. The reason given by this evaluator for his neutral response is that the university which he represents has taken the decision not to use cloud-based email.

Some of the comments provided by the evaluators regarding the framework further highlight the confidence these have towards the utility of the FACCE. Regarding the value of the FACCE in terms of improving *assurance*, Evaluator D (the expert in IT governance and assurance) says, "It provides a very clear and simplistic approach which demonstrates key considerations for obtaining assurance and guiding conformance." Evaluator E says of the FACCE, "Instead of improving the level of assurance, it firstly identifies the level of assurance. One can therefore way up the cost of implementation versus the identified level of assurance and make a business decision around the level of acceptable risk and available budget."

When commenting on the use of the FACCE for improving *trust* in cloud-based email this same evaluator says, "The framework quantifies the security risk and level of compliance with best-practice. The resultant risk therefore creates transparency, which creates trust, as the risk can be proactively managed." Evaluator A highlights the benefit of the best practice based approach of the FACCE by saying that, "Trust is earned by consistency and this is achieved through the use of best practices."

With regard to the ability of the FACCE to improve the level of *conformance* of cloud-based email at higher education institutions in South Africa Evaluator E adds, "Again, the level of conformance is quantified, allowing responsible parties to way up the benefits of a higher level of conformance and the resultant costs that would be incurred."

Evaluator A strongly agrees that the FACCE can be used to assist with improving *due diligence* in governing cloud-based email. In this regard he says, "The methodology to implement assurance is iterative in nature, allowing continuous improvement." Evaluator D adds, "the framework is clear and concise and in my view provides a holistic representation of the key factors at a high level of what organisations need to consider – this therefore demonstrates the application of due diligence in the framework. However, further due diligence would need to be applied by an organisation adopting the framework to determine

for example appropriate organisation specific structures and internal policies etc. But the framework highlights this as something that needs to be addressed."

Evaluator E expresses confidence in the value of the FACCE regarding *auditing* by saying, "The auditing process is simplified tremendously by this framework, as the hard work of creating a compliance tick list is done up front, when all the various requirements must be considered to implement this framework."

Regarding the value of a tool developed based on the prototype tool of the FACCE Evaluator D says, "Yes I agree. This could expedite the audit process. King III chapter 5 'the governance of information technology' states that technology should be used to improve audit coverage and efficiency. This tool could do just that if implemented effectively." Evaluator C adds, "There are likely to be existing platforms that could be adapted to support the framework, not only for gathering data, but also for managing, monitoring and auditing. (For example, I am thinking of https://www.atlassian.com/software/jira)."

Although Evaluator E believes that the FACCE could be easily implemented at higher education institutions in South Africa he adds, "Yes. Buy-in is required on a very high level within an organization or institution, and a dedicated team would have to be created, whose job it would have to be to assure that all requirements are listed and their compliance estimated correctly and diligently captured. The biggest hurdles would therefore be political buy-in and the disciplined execution of the framework." Evaluator D says, "… the framework is clear, concise and well thought it. It provides a simplistic approach to addressing cloud based email conformance and assurance."

Evaluator A summarises the value of the FACCE as follows, "It appears to be a practical and well-structured framework, connecting conformance requirements and enablers into an iterative methodological process which results in defined criteria producing the required assurance!"

Based on the preceding information, it can be argued that the FACCE can be used by higher education institutions in South Africa to meet its goals of assisting with improving the levels of conformance, assurance, trust and due diligence related to cloud-based email. Further feedback from the evaluators showed that the prototype tool could be fully implemented to be useful at the University. The CIO at the University where the FACCE has been demonstrated also commented that the FACCE is "easy to understand and follow" and that it

would be practical and easy to implement at the University. This further verifies the utility and practicality of the FACCE.

7.4 Conclusions

This chapter has made it clear how two of the activities outlined in the design science research methodology, demonstration and evaluation, have been applied to the FACCE, the artifact. The results of these activities have shown that the FACCE can indeed be used to effectively and efficiently help higher education institutions in South Africa improve the level of assurance for the conformance of cloud-based email. This has been further verified by the positive feedback regarding the value of the FACCE by four other evaluators.

The following chapter concludes this work. There it is made clear how this chapter has contributed to the overall rigour of this research study.

CHAPTER 8
Conclusion

8.1 Introduction

According to the Oxford dictionary, the word conclusion can imply two meanings. A conclusion can be something brought to a finish, "the summing-up of an argument or text". Alternatively, a conclusion can be "a judgment or decision reached by reasoning". This chapter concludes in both of these ways. This chapter concludes this work by summing up how the objectives of this work have been addressed. It also highlights certain judgments related to the research conducted by listing contributions made, lessons that have been learnt during the completion of this work and opportunities for further research related to this work.

8.2 Research Objectives

As has been highlighted in this work by means of literature review and surveys, ***the lack of structured guidelines for assurance of cloud-based email conformance is putting this service at risk in higher education institutions in South Africa.*** This problem has been especially emphasised in Chapter 5. The relevance and importance of the problem has also been highlighted in an article that has been prepared (and is currently under review) as a result of this work.

To assist with addressing this problem, the main objective of this work has been to compile a framework to assist South African higher education institutions to assure that cloud-based email solutions are used in a manner that adequately applies the conformance principle of governance. To assist with accomplishing this objective, the following sub-objectives were also identified:

- To identify established and accepted standards, frameworks or theories for conformance and assurance that can be used as a foundation for the development of a framework for assuring the conformance of cloud-based email.
- To devise what conformance and assurance problems currently are encountered with cloud-based email solutions.
- To find out which existing guidelines are currently being used for cloud-based email implementations. To determine the shortcomings associated with existing guidelines.

- To formulate how existing standards, regulations, best practice guidelines, policies and other factors should influence or change to accommodate cloud-based email conformance concerns in higher education institutions in South Africa.

This section highlights how each of these objectives has been met in this research study.

8.2.1 Main objective

To compile a framework to assist South African higher education institutions to assure that cloud-based email solutions are used in a manner that adequately applies the conformance principle of governance

Such a framework has been developed. A framework for assuring the conformance of cloud-based email (FACCE) is described in Chapter 6. This framework has been developed using the design science methodology described by Peffers et al. (2008). The list below highlights how the activities in this methodology have been applied in this work.

- **Activity 1: Problem identification and motivation.**
  Requirement: Define the specific research problem and justify the value of a solution.
  The specific research problem has been clearly defined, delineated and stated in this work. The problem addressed: ***the lack of structured guidelines for assurance of cloud-based email conformance is putting this service at risk in higher education institutions in South Africa.*** Chapter 1 has introduced the problem. Chapter 5 has clearly motivated the problem and its relevance. The results of surveys and the literature review are used in this chapter to motivate the problem. In addition, a paper that has been prepared for publication has been submitted to a reputable South African journal; it outlines and motivates the problem.
- **Activity 2: Define the objectives for a solution.**
  Requirement: Infer the objectives of a solution from the problem definition and knowledge of what is possible and feasible.
  The objectives of the solution have been clearly stated and motivated in chapters 3 and 5.
- **Activity 3: Design and development.**
  Requirement: Create the artefact.

Chapter 6 has described the framework for assuring cloud-based email conformance (FACCE) that has been created as an artifact as the solution to this work using the design science research methodology.

- **Activity 4: Demonstration.**

  Requirement: Demonstrate the use of the artefact to solve one or more instances of the problem.

  The efficiency and utility of FACCE has been demonstrated at a South African University that uses cloud-based email. This demonstration is described in Chapter 7.

- **Activity 5: Evaluation.**

  Requirement: Observe and measure how well the artefact supports a solution to the problem.

  FACCE has been evaluated by means of demonstration (as described in the previous step) and by means of feedback from experts at the South African University where it was demonstrated and five other evaluators. The evaluation has shown that FACCE can effectively meet the objectives outlined. The evaluation of FACCE is described in Chapter 7.

- **Activity 6. Communication.**

  Requirement: Communicate the problem and its importance, the artefact, its utility and novelty, the rigour of its design, and its effectiveness to researchers and other relevant audiences, such as practicing professionals, when appropriate.

  The specific problem of cloud-based email assurance and its importance has been communicated in a paper in this regard. The paper is under review at a reputable South African journal, the Africa Education Review. A paper describing the artifact of this work (FACCE) has also been accepted for presentation at an international conference (The 8th International Conference for Internet Technology and Secured Transactions) in December. This paper will also appear in the conference's proceedings, which are to be published by IEEE. In addition, components of this research have been published in the South African Journal of Business Management (Von Solms & Viljoen, 2012). There is also currently a paper that describes research done in this study entitled 'Towards cloud computing assurance' under review at this journal. Further aspects of this work have been presented at the South African Networks and Telecommunications Conference (Viljoen, Von Solms, & Lawack-Davids, 2012). All papers related to this work are found in Appendix B. A presentation has also been used to communicate and explain the FACCE and the motivation of the framework to the chief information

officer (CIO) and the senior engineer of messaging services at the university where the FACCE was demonstrated. This presentation is found in Appendix A6.

Besides adhering to the design science research methodology, as explained in the preceding section, this work has also met the guidelines for design science research by Hevner et al. (2004) in designing FACCE. These seven guidelines are listed and explained in terms of this research below. For each of the items in the list, the guideline is shown in bold and the description of the guideline is shown in italics, followed by a description of how the guideline is applied in this work.

1. **Design as an Artifact -** A framework for assuring the conformance of cloud-based (FACCE) is a viable artifact that has been created, the utility of which has been demonstrated.
2. **Problem relevance** - The problem relevance is described in section 8.2.1, activity 1. As has been highlighted repeatedly, a real and relevant problem is also addressed by this work.
3. **Design evaluation** – The FACCE has been verified for utility, quality and efficacy in a case study at a South African higher education institution that uses cloud-based email. Since the generalisability of the findings of a case study can be questioned, FACCE has been further evaluated by five other professionals with relevant expertise to verify the results of the demonstration and evaluation activities at the University. The description of activities four and five of the design science research methodology (as described in Chapter 7) provides more detail regarding how this guideline has been followed.
4. **Research contributions** – The contribution of this work is described in the next section in this chapter.
5. **Research rigour** - An accepted methodology (the design science research methodology) has been used in the construction of FACCE.
6. **Design as a search process** - As described in the methodology used for constructing the FACCE (the design science research methodology), an iterative approach has been used to design and improve the FACCE until the framework meets the objective of providing a manner that can assist in assuring cloud-based email conformance within higher education institutions in South Africa.
7. **Communication of research** – The FACCE has been communicated to and used by IT staff at a higher education institution in South Africa. In addition, the framework and much of its supporting research has been published and presented (or is currently under

review) in various conferences and journal publications, as described earlier in this chapter.

From the above, it should be clear that the main objective of this work (to compile a framework to assist South African higher education institutions to assure that cloud-based email solutions are used in a manner that adequately applies the conformance principle of governance) has been met satisfactorily. The demonstration and evaluation of FACCE have clearly shown that this framework can be effectively used to assist South African higher education institutions to improve the overall level of assurance that they are using cloud-based email in a manner that complies with internal and external conformance requirements. As such, it can be argued that the FACCE is a valuable artifact that can be used to address a relevant problem.

8.2.2 Sub objective 1

To identify established and accepted standards, frameworks or theories for conformance and assurance that can be used as a foundation for the development of a framework for assuring the conformance of cloud-based email.

Chapter 3 has identified and explained a number of standards and frameworks in the fields of IT governance, assurance and IT conformance that have been used as a basis for the development of FACCE. These have primarily included:

- ISO/IEC 38500:2008, the *international standard for corporate governance of information technology*
- COBIT 5 and
- The international framework for assurance engagements

Chapter 6 describes how the guiding principles in these accepted works have been used to develop FACCE.

8.2.3 Sub objective 2

To devise what conformance and assurance problems are currently encountered with cloud-based email solutions.

As highlighted in Chapter 5, there are general problems regarding the assurance of both internal and external conformance when using cloud-based email. The results of an

investigation into problems related to internal compliance for cloud-based email at higher education institutions are outlined in a paper that has been prepared and presented at a reputable South African conference. This paper can be found in Appendix B3. The results of this investigation have also motivated the cloud-based email-specific process for ensuring external compliance that forms part of the more detailed guidelines for the FACCE, which are detailed in Appendix A2.

Problems regarding assurance of internal conformance have also been repeatedly highlighted in this work. The guidelines for cloud-based email specific processes that form part of FACCE (Appendix A2) assist in addressing this.

8.2.4 Sub objective 3

To find out which existing guidelines are currently being used for the management and governance of cloud-based email implementations. To determine the shortcomings associated with existing guidelines.

As described in Chapter 5, there is a lack of guidelines for the management and governance of cloud-based email. Guidelines from CSPs can be useful to institutions when implementing and maintaining the email service, but they are generally more technical and task specific in nature and do not adequately address the overarching areas of cloud-based email management and governance. In the general area of cloud computing, there has been more work done to produce management and governance guidelines. These are discussed in Chapter 4. This chapter also identifies the shortcomings of these guidelines. As highlighted there, none of these guidelines alone provide adequate guidance regarding the assurance of cloud-based email conformance. As is described in the next subsection, FACCE provides a way of using principles from existing guidelines, such as those identified and summarised in Chapter 4, to assist with the assurance of cloud-based email conformance.

8.2.5 Sub objective 4

To formulate how existing standards, regulations, best practice guidelines, policies and other factors should influence or change to accommodate cloud-based email conformance concerns in higher education institutions in South Africa.

FACCE provides a methodology that encourages institutions to determine criteria for conformance based not only on policies and legal, regulatory and contractual obligations but also on various applicable best practice guidelines. This is in line with the principles for

conformance outlined in ISO/IEC 38500. In addition, the detailed guidelines that form part of FACCE highlight some existing guidelines that are likely to be applicable and describe where these are likely to be applicable to cloud-based email at South African higher education institutions. This can be seen in Appendix A1 and Appendix A2.

From this section, it should be clear that the research objectives of this work have been met. In addition, it should be evident that this has been accomplished in a manner that demonstrates care to follow accepted guidelines for conducting research. The next section briefly specifies the contributions of this work.

8.3 Research Contributions

The main artifact of this work (FACCE) contributes to assurance regarding cloud computing services by addressing this problem: the lack of structured guidelines for assuring the conformance of cloud-based email is putting this service at risk in higher education institutions in South Africa. It has been verified that the FACCE can be used to address this problem effectively. The evaluation and demonstration have shown that FACCE can be used to contribute to the levels of conformance, assurance, trust and due diligence for cloud-based email at higher education institutions in South Africa.

The areas of IT governance, IT conformance and IT assurance are well established areas that have been widely researched. Well recognised models and frameworks have already been developed and established in these areas. These frameworks and models have been used by organisations using a traditional model of provisioning IT services for some time already. This is highlighted in Chapter 3. How established models and framework of IT governance, IT conformance and IT assurance can be applied to the relatively new field of cloud computing has generated much interest and research recently. As described in Chapter 4, much work has been done recently to provide guidance regarding the relatively new field of cloud computing. In Chapter 4 guidelines that touch on aspects of the governance, assurance and conformance of cloud computing are described. The existing work does not (to the knowledge of the researcher) however, specifically focus on the area of assuring conformance of cloud computing from a governance perspective. Guidelines regarding the governance, assurance or conformance of cloud computing also tend to be conceptual and high-level in nature. As such they often lack detailed, situation specific guidelines. None of the work found by the researcher has specifically addressed the problem of assuring

conformance of cloud-based email at higher education institutions in South Africa. The FACCE makes a significant contribution in this area.

This work contributes to conformance by providing higher education institutions with a way to identify, communicate and monitor the extent to which conformance criteria have been achieved in the institution. This in turn assists with identifying where corrective action can be taken to improve the overall conformance of cloud-based email.

In addition, the FACCE assists with assurance by promoting and providing a means to identify and communicate criteria and related evidence. Both evaluators of the FACCE agreed that it could be used to make it easier to provide auditors with relevant information and that the FACCE would improve the level of trust for cloud-based email conformance. This work can, therefore, be said to contribute to the area of cloud-based email assurance.

Since conformance and assurance are both essential elements of governance, it can also be argued that the FACCE can make a contribution in the field of cloud computing governance. The FACCE is soundly based on an internationally accepted standard for IT governance (ISO/IEC 38500) and detailed guidelines of the FACCE are closely linked with COBIT 5. Both evaluators of the FACCE agree that this framework can be used to assist with demonstrating due diligence with regard to cloud-based email. The CIO strongly agreed that this was the case and said that "all the loops covered makes a strong case for due-diligence having been followed".

Although the FACCE has been designed and tested specifically for use with cloud-based email at higher education institutions in South Africa, it is based soundly on governance and assurance principles that can be applied to other cloud computing solutions. This became obvious during the demonstration of the FACCE at the South African university. The staff members (experts) expressed the intention of using the principles of the FACCE as they investigated and potentially adopted and implemented various other cloud computing solutions at the University. The FACCE, therefore, can be seen to make a contribution to the field of cloud computing assurance and conformance in general by laying the foundation for further work that can be done. Some of the potential for further work in this field is highlighted in the next section.

8.4 Limitations and Further Research

There is further research that can be done based on the work conducted in this study. All the detailed guidelines of the FACCE have been derived purely from a study of the guidelines from the reputable IT governance bodies listed in Chapter 4. Academic work and guidelines from other bodies has not been consulted when developing the FACCE cloud-based email specific processes. The FACCE cloud-based email specific guidelines (aside from the process describing how to ensure management of legal risks) the and the recommended reference list have also not been peer-reviewed and published. Although the value of some of these detailed guidelines was demonstrated to an extent during the demonstration of the framework, not all these guidelines were used for the demonstration. All these detailed guidelines of the FACCE can therefore be enhanced. This includes the recommended reference list, the guidelines for cloud-based email-specific processes and the prototype tool. The University where FACCE was demonstrated expressed that the prototype tool could be developed into a useful tool for the institution. At this stage the prototype tool merely illustrates how the concepts of the FACCE could be implemented. It is far from a fully functional tool. The University said that it would like the tool developed to be used for all cloud computing solutions that could be potentially used at the institution. A suggestion made by staff was that the tool be implemented in such a way that information gathered by various individual institutions could be shared with other institutions, to learn about cloud-based email criteria and concerns collaboratively. To illustrate this, the following example can be used. University X conducts an assessment of legal risks regarding cloud-based email with the aid of legal advisers using the guidelines outlined in the FACCE. This university could then use a fully implemented tool based on the prototype tool that is part of FACCE. Using this tool, University X decides to share the results of this risk assessment with all other universities that are using the tool. This information can then feed into the conformance requirement documents that are used by University Y when following the FACCE methodology.

Another possible area for future work is suggested by one of the evaluators of the FACCE who says, "There are likely to be existing platforms that could be adapted to support the framework, not only for gathering data, but also for managing, monitoring and auditing. (For example, I am thinking of https://www.atlassian.com/software/jira)." How the FACCE could

be implemented using existing tools and platforms could be another interesting area for future research.

The FACCE has also only been demonstrated at one South African university which has already been using cloud-based email for a number of years. The value of the FACCE could be further evaluated by testing it in cases where cloud-based email is being introduced to an institution for the first time.

Only some criterion for assuring the conformance of cloud-based email was used when demonstrating the FACCE. The other criterion could also be used to further evaluate the FACCE.

One of the evaluators of FACCE highlights another limitation of the framework that could be addressed in further research: the means to ensure the quality of the assurance and conformance processes motivated by the FACCE. The evaluator comments, "… the framework indicates that assurance is an important consideration that needs to be factored in (which is good). However, the framework does not ensure that assurance activities are of quality and are effective – it is these two factors that will ultimately ensure that trust is cultivated." Similarly he adds, "The framework merely indicates that conformance is a key consideration. However it is the quality and effectiveness of the conformance processes that will ultimately impact on the level of conformance." As indicated by this evaluator the impact of this limitation is significant and future work in this regard could be valuable.

As highlighted previously, the potential value of the FACCE as a basis for further research into the field of cloud computing in general has also been highlighted. An evaluator of the FACCE makes this clear in this comment: "I do not believe that tertiary institutions would be the main beneficiaries of such a framework. Top of the list are financial institutions, which have extremely tight regulatory and best practice requirements. Other regulated industries also have a variety of acts, standards, and best practice frameworks that they either must conform to, or would give them a competitive marketing advantage, if compliance can be punted by Sales staff. These institutions typically have far greater IT budgets than tertiary institutions, with much bigger risks if non-compliance is overlooked." This evaluator adds, "Large corporate and government organisations have a long list of conformance requirements imposed on them, or ones that they strive to achieve, especially if they are in a security conscious industry such as financial institutions, and if they are listed on a stock

exchange, which typically require governance transparency and corporate governance codes such as King 3 for the Johannesburg Stock Exchange and compliance with the Sarbanes Oxley Act for the New York Stock Exchange. Most of these institutions struggle to keep an overview of their compliance. This framework could help them create a quantitative dashboard, highlighting areas of concern and allowing risk of non-compliance to be managed and financial implications to be weighed up. The framework therefore has the opportunity of tracking corporate compliance on a far wider scope than merely IT governance in a cloud environment." This evaluator strongly suggests that the FACCE be expanded and tested in case studies for other cloud computing solutions besides cloud-based email. Further work into how the FACCE could be adapted and implemented for other institutions and for other cloud computing solutions could therefore be valuable. As highlighted in Chapter 5, cloud-based email is one of the earliest and most widely used forms of cloud computing. The work done and tested in this more established form of cloud computing solutions, therefore, has great potential to contribute to an understanding of other cloud computing solutions. Further research based on this work could be used to make a significant contribution to the problems of trust, assurance and conformance in cloud computing.

8.5 Epilogue

As stated in the introduction to this chapter, conclusions sum up, express judgments and finish off ideas. Here, this work is finished off by stating that this concluding chapter has summed up various arguments and judgments that have been made throughout this research to motivate the work done here. Hopefully this has been done in a manner that demonstrates that the objectives of the work have been met in a way that makes a contribution to the problem of cloud-based email assurance. It is the belief of the researcher that cloud computing could potentially make a real positive impact on cash-strapped education institutions if it can be used in a way that assures institutions that they are doing so in a secure and compliant manner. It is, therefore, hoped that this work can be used to inform and stimulate other works in the important fields of cloud computing, assurance and conformance.

REFERENCES

Abbadi, I. M. (2013). A framework for establishing trust in cloud provenance. *International Journal of Information Security, 12*(2), 111-128.

Abdullah, N. S., Sadiq, S., & Indulska, M. (2010). Emerging challenges in information systems research for regulatory compliance management. In B. Pernici (Ed.), *Advanced Information Systems Engineering. 22nd International Conference, CAiSE 2010, Hammamet, Tunisia, June 7-9, 2010. Proceedings* (pp. 251-265). Tunisia: Springer.

Ali, S. (2006). Effective information technology mechanisms: An Australian study. *Gadjah Mada International Journal of Business*, 69-102.

Amis, J. M., & Silk, M. L. (2008). The philosophy and politics of quality in qualitative organizational research. *Organizational Research Methods, 11*(3), 456-480.

Arora, D., Millman, E., & Neville, S. W. (2013). Enabling richer statistical MANET simulations through cluster computing. *Cluster Computing, 16*(4), 989-1003. doi:10.1007/s10586-013-0247-x

Ashford, W. (2011, April). Security in the cloud: top nine issues in building users' trust. *Computer Weekly*. Retrieved from http://www.computerweekly.com/feature/Security-in-the-cloud-Top-nine-issues-in-building-users-trust

Assurance. (n.d.). *Business Dictionary*. Retrieved from http://www.businessdictionary.com/definition/assurance.html

Aumueller, D. C. (2010). *IT-compliance analysis for cloud computing.* (Doctoral dissertation, University of Applied Sciences Darmstadt). Retrieved from http://germany.emc.com/collateral/about/news/emc-publications/articles/it-compliance-analysis-for-cloud-computing-dirk-aumueller.pdf

Australian Government. (2013, May). *The national cloud computing strategy.* Retrieved from Department of Broadband, Communications and the Digital Economy: http://www.attorneygeneral.gov.au/Mediareleases/Pages/2013/Third%20quarter/5July2013-PolicyforGovernmentuseofcloudcomputingservices.aspx

Bahga, A., & Madisetti, V. K. (2012). Analysing massive machine data in a computing cloud. *IEEE Transactions On Parallel & Distributed Systems, 23*(10), 1831-1843. doi:10.1109/TPDS.2011.306

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

Besnard, P., & Hunter, A. (2008). *Elements of argumentation.* Cambridge, Massachusetts: MIT Press.

Best, P. J., Mohay, G., & Anderson, A. (2004). Machine-independant audit trail analysis - a tool for continous audit assurance. *Intelligent Systems in Accounting, Finance & Management, 12*(2), 85-102.

Bogdan, R. C., & Biklen, S. B. (1998). *Qualitative research in education. An introduction to theory and methods.* Needham Heights: Allyn & Bacon, A Viacom Company.

Borenstein, N. N., & Blake, J. J. (2011). Cloud computing standards: Where's the beef? *IEEE Internet Computing, 15*(3), 74-78.

Brandic, I., Raicu, I., Srirama, S. N., Batrashev, O., Jakovits, P., & Vainikko, E. (2011). Scalability of parallel scientific applications on the cloud. *Scientific Programming, 9*(2/3), 91-105.

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

Britto, M. (2012, January). Cloud computing in higher education. *Library Student Journal*.

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

Brown, W. C. (2006). IT governance, architectural competency, and the Vasa. *Information Management & Computer Security, 14*(2), 140-154. doi:10.1108/09685220610655889

Business Wire. (2011, April 28). *Major study finds rapid adoption of hosted email compliance.* Retrieved May 20, 2012, from Business Wire: http://www.businesswire.com/news/home/20110428006151/en/Major-Study-Finds-Rapid-Adoption-Hosted-Email

Carnevale, D. (2008). Colleges get out of e-mail business. *The Chronicle of Higher Education, 4*(18), A1.

Carter, D. (2011, April 22). *After Balking, Yale switches to Gmail*. Retrieved May 15, 2012, from eCampus News: http://www.ecampusnews.com/top-news/after-balking-yale-switches-to-gmail/

Cattedu, D. (2011, January 17). *Security and Resilience in Governmental Clouds.* Retrieved from ENISA: http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

Celar, S., Seremet, Z., & Turic, M. (2011). Cloud Computing: Definition, characteristics, services and models. *Annals of DAAAM & Proceedings*, 1-2.

Chambers, A. (2009, April). The black hole of assurance. *Internal Auditors, 66*(2), 28-29.

Chris, H. (2010). Standards for a Better Cloud. *Baseline*(106), 28.

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

CIO Council & Chief Acquisition Officers Council. (2012, February). *Creating Effective Cloud Computing Contracts for the Federal Government. Best Practices for Acquiring IT as a Service.* Retrieved from https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

Cisco. (n.d.). *Cloud computing in Higher Education: A Guide to Evaluation and Adoption.* Retrieved from http://www.cisco.com/web/offer/email/43468/5/Cloud_Computing_in_Higher_Education.pdf

Cloud Industry Forum. (2011). *Cloud adoption and trends for 2012.* Retrieved from Cloud UK: http://www.fasthosts.co.uk/downloads/white-papers/4692406_assoc.pdf

Cloud Industry Forum. (2012). *UK Cloud adoption and trends for 2013.* Retrieved from http://cloudindustryforum.org/downloads/whitepapers/cif-white-paper-8-2012-uk-cloud-adoption-and-2013-trends.pdf

Cloud Security Alliance. (2009a). *Cloud Security Alliance.* Retrieved January 25, 2010 from http://www.cloudsecurityalliance.org/

Cloud Security Alliance. (2009b, December). *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.* Retrieved January 25, 2010

Cloud Security Alliance. (2010, March). *Top Threats to Cloud Computing V1.0.* Retrieved March 8, 2010, from CSA: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cloud Security Alliance. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Retrieved March 8, 2012, from CSA: https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

Computer Weekly. (2009, Novemeber 27). *Putting e-mail in the cloud.* Retrieved 10 10, 2010, from http://www.computerweekly.com/Articles/2009/11/30/239454/Putting-e-mail-in-the-cloud.htm

Conry-Murray, A. (2010, April 26). SaaS E-Mail's moment. *Information Week*, pp. 19-26.

Corbyn, Z. (2009, August 20). *Second Life out as techies embrace cloud email.* Retrieved March 02, 2010, from Times Higher Education: http://www.timeshighereducation.co.uk/story.asp?storycode=407839

COSO. (n.d.). *Welcome to COSO*. Retrieved January 21, 2013, from COSO: http://www.coso.org/

Creswell, J. W. (2003). *Research design: qualitative, quantitative, and mixed methods approaches.* Thousand Oaks, California, USA: Sage Publications.

Creswell, J. W., & Plano-Clark, V. L. (2007). *Designing and conducting mixed methods research.* Thousand Oaks, California, USA: Sage Publications.

CSA. (2011, July). Trusted Cloud reference architecture. *Trusted Cloud reference architecture*. Retrieved from https://cloudsecurityalliance.org/research/tci/

CSA. (2012, September 20). *Cloud Control Matrix.* Retrieved from Cloud Controls Matrix: https://cloudsecurityalliance.org/research/ccm/

Dameri, R. P. (2009). Improving the benefits of IT compliance using enterprise management information systems. *Electronic Journal Information Systems Evaluation, 12*(1), 27-38.

Department of Basic Education. (n.d.). *List of South African universities*. Retrieved February 25, 2014, from Department of Basic Education: http://www.education.gov.za/FurtherStudies/Universities/tabid/393/Default.aspx

Department of Education. (2009). Strategic plan 2009-2013. South Africa.

Diligence. (2013). *Oxford Dictionaries.* Oxford University Press. Retrieved from http://oxforddictionaries.com/definition/english/due%2Bdiligence

Ding, Z., Xu, J., & Yang, Q. (2013). SeaCloudDM: a dtabase cluster framework for managing and querying massive heterogeneous sensor sampling data. *Journal of Supercomputing, 66*(3), 1260-1284. doi:10.1007/s11227-012-0762-1

Dodds, T. (2007). Information Technology: a contributor to innovation in higher education. *New Diretions for Higher Education, 137*, 85-97.

Du, B. H., & Cong, Y. (2010, October). Cloud computing, accounting, auditing and beyond. *CPA Journal*, 66-71.

Dutta, A., Peng, G. C., & Choudharya, A. (2013). Risk in enterprise cloud computing: The perspective of IT experts. *Journal of Computer Information Systems, 53*(4), 39-48.

ENISA. (2009a, November 20). *Cloud computing benefits, risks and recommendations for information security.* (D. Catteddu, & G. Hogben, Eds.) Retrieved from http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

ENISA. (2009b, November). *Cloud Computing Information Assurance Framework.* Retrieved February 22, 2010, from http://www.enisa.europa.eu/

ENISA. (2010). *ENISA Cloud Computing Risk Assessment*. Retrieved June 5, 2010, from ENISA: http://www.enisa.europa.eu/act/res/other-areas/cloud-computing

ENISA. (2011, December). *Procure Secure. A guide to monitoring of security service levels in cloud contracts.* Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

European Commission. (2012, December). (L. Schubert, K. Jeffery, & B. Neidecker-Lutz, Eds.) Retrieved January 3, 2013, from A roadmap for advanced cloud technologies

under H2020: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-expert-group/roadmap-dec2012-vfinal.pdf

Evani, U. S., Challis, D., Jin, Y., Jackson, A. R., Paithankar, S., Bainbridge, M. N., . . . Yu, F. (2012). Atlas2 Cloud: a framework for personal genome analysis in the cloud. *BMC Genomics*, 1-9. doi:10.1186/1471-2164-13-S6-S19

Farah, S. (2010). Cloud computing or software as a service - which makes most sense for HR? *Employment Relations Today, 36*(4), 31-37.

Farber, R. (2009, November/December). Cloud computing: Pie in the sky? *Scientific Computing*, 18, 20.

Fingar, P. (2009). *Dot.Cloud: the 21st Century Business Platform Built on cloud Computing.* Tampa, Florida, USA: Meghan-Kiffer Press.

Fleishman, G. (2012, August). A brief history of email. *Macworld, 29*(8).

Focus Market Research. (2011, August). *Focus Research study: The state of cloud in 2011.* Retrieved from http://b2b.ziffdavis.com/research/focus-survey-results-state-cloud-computing-2011/

Fox, R. (2009). Library in the clouds. *OCLC Systems & Services: International digital library perspectives*, *25*(3), 156-161.

Fujioka, E., Berghe, E. V., Donnelly, B., Castillo, J., Cleary, J., Holmes, C., . . . Halpin, P. (2012). Advancing global marine biogeography research with open-source GIS software and cloud computing. *Transactions in GIS, 16*(2), 143-160. doi:10.1111/j.1467-9671.2012.01310.x

Gash, D., Ariyachandra, T., & Frolick, M. (2011). Looking to the clouds for business intelligence. *Journal of Internet Commerce, 10*(4), 261-269.

Gatewood, B. (2009, July/August). Clouds on the Information Horizon: How to avoid the storm. *Information Management*, pp. 32-36.

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.

Geer, D. (2011, October). Cloud email: The good, the bad, the uptime. *University Business, 14*(9), pp. 31-36.

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

Gerring, J. (2007). *Case study research.* Cambridge: Cambridge university Press.

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/

Gillham, B. (2000). *Case study research methods.* London: Continuum International Publishing Group.

Goldsborough, R. (2012, February). The latest in Web Email. *Tech Directions, 71*(7), p. 12.

Google. (2009). *More than 7 million students use Google Apps*. Retrieved April 3, 2010, from Google Apps: http://www.google.com/a/help/intl/en/edu/index.html

Google. (2011). Retrieved May 15, 2012, from Google Apps for Education: http://www.google.com/apps/intl/en/edu/index.html

Goulart, K. (2012, November 13). University migrates to Office 365 for cloud-based email. *Computer Weekly*, 23-25.

Gumbel, P. (2004, November 21). *How it all went so sour*. Retrieved August 7, 2010, from Time.com: http://www.time.com/time/magazine/article/0,9171,901041129-785318,00.html

Hancock, D. (2002, June 26). *World-class scandal at WorldCom*. Retrieved August 7, 2010, from CBS News.com: http://www.cbsnews.com/stories/2002/06/26/national/main513473.shtml

Healy, P. M., & Krishna, G. P. (2003). The Fall of Enron. *Journal of Economic Perspectives, 17*(2), 3-26.

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

Hofstee, E. (2006). *Constructing a good dissertation.* (A. Denniston, Ed.) Sandton, Johannesburg, South Africa: EPE.

Horwath, C., Chan, W., Leung, E., & Pili, H. (2012, June). *Eneterprise Risk Manage for Cloud Computing.* COSO.

IBM. (2009, July). The Benefits of Cloud Computing. Somers, NY, USA.

InfoWorld. (2009). *Cloud computing deep dive.* USA: InfoWorld.com.

International Auditing and Assurance Standards Board. (2004). *International framework for assurance engagements.* Retrieved from IFAC: http://www.ifac.org/sites/default/files/downloads/b003-2010-iaasb-handbook-framework.pdf

IoDSA. (2009). *The King report on corporate governance for South Africa (The Institute of Directors in Southern Africa) September 2009.* South Africa: Institute of Directors in Southern Africa. Retrieved from http://www.iod.wowinteractive3.co.za/Portals/0/IoDSA_King_Report_Flip_Book/IoDSA_King_Report_Flip_Book.html

Ion, I., Traian, S., & Cristian, A. (2008). The IT audit - A major requirement for the management quality and success in the European business context. *Annals of The University of Oradea, Economic Science Series, 17*(4), 1397-1401.

ISACA. (2008a, May 1). *IS Auditing Guideline: G2 Audit Evidence Requirement.* Retrieved from ISACA: http://www.isaca.org/Knowledge-Center/Standards/Pages/IS-Auditing-Guideline-G2-Audit-Evidence-Requirement1.aspx

ISACA. (2008b). *ITAF: A professional practices framework for IT assurance.* Rolling Meadows, IL, USA: ISACA. Retrieved from ISACA: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ITAF-A-Professional-Practices-Framework-for-IT-Assurance.aspx

ISACA. (2008c, May 2008). *New research highlights the business benefits of continuously improving IT GRC Practices.* Retrieved March 16, 2010, from ISACA: http://www.isaca.org/Content/ContentGroups/News_Releases1/20082/New_Research_Highlights_Benefits_of_Improving_IT_GRC_Practices.htm

ISACA. (2009). *Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives.* Rolling Meadows, IL, USA: ISACA. Retrieved June 10, 2010, from http://www.isaca.org/Knowledge-Center/Research/Documents/Cloud-Computing-28Oct09-Research.pdf

ISACA. (2010a). *Cloud Computing*. Retrieved July 5, 2010, from ISACA.org: http://www.isaca.org/Groups/Professional-English/cloud-computing/Pages/Overview.aspx

ISACA. (2010b). *COBIT 5. A Business framework for the governance and management of enterprise IT.* Rolling Meadows, IL, USA: ISACA.

ISACA. (2011). *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud.* 3701 Algonquin Road,Suite 1010Rolling Meadows,IL 60008 USA: ISACA. Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Cloud-Computing-Controls-and-Assurance-in-the-Cloud.aspx

ISACA. (2012a, July). *Calculating Cloud ROI: From the Customer Perspective.* Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Calculating-Cloud-ROI-From-the-Customer-Perspective.aspx

ISACA. (2012b, February). Guiding Principles for Cloud Computing Adoption and use. *Guiding Principles for Cloud Computing Adoption and use*. Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Guiding-Principles-for-Cloud-Computing-Adoption-and-Use.aspx

ISACA. (2012c). Security Considerations for Cloud Computing. 3701 Algonquin Road,Suite 1010Rolling Meadows,IL 60008 USA. Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Security-Considerations-for-Cloud-Computing.aspx

ISACA. (2013). COBIT 5 for assurance. Rolling Meadows, IL, USA: ISACA. Retrieved from http://www.isaca.org/COBIT/Pages/Assurance-product-page.aspx

ISACA. (n.d.). *What we offer & whom we serve*. Retrieved January 21, 2013, from ISACA: http://www.isaca.org/About-ISACA/What-We-Offer-Whom-We-Serve/Pages/default.aspx

ISACA & CSA. (2012). *2012 Cloud Computing Market Maturity Study Results.* Retrieved January 2013, 2013, from ISACA: http://www.isaca.org/Knowledge-

Center/Research/ResearchDeliverables/Pages/2012-Cloud-Computing-Market-Maturity-Study-Results.aspx

ISO. (2008, June 1). ISO/IEC 38500:2008 Corporate governance of information technology. *International Standard*. Pretoria, Pretoria: SABS Standards Division.

ISO. (2012, December 19). *ISO/IEC WD 27018.* Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498

ISO. (2012, December 21). *ISO/IEC WD TS 27017.* Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757

ISO. (n.d.). *About ISO*. Retrieved January 21, 2013, from ISO: http://www.iso.org/iso/home/about.htm

IT Governance Institute. (2007). *COBIT 4.1*. Retrieved 10 23, 2010, from ISACA: http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx

ITGI. (2003). *Board Briefing on IT Governance* (Second Edition ed.). Rolling Meadows, IL, USA: IT Governance Institute.

Iyer, B., & Henderson, J. C. (2010, June). Preparing for the future: Understanding the seven capabilities of cloud computing. *MIS Quaterly Executive, 9*(2), 117 - 131. Retrieved from http://drhesterwebspace.net/wiki/images/c/cf/IH2010.pdf

Jackson, G. A. (2011, July/August). Leading an IT organization out of control. *EDUCAUSE Review*, 32-42.

Jericho Forum. (2009, April). *Cloud Cube Model: Selecting Cloud formations for secure collaboration.* Retrieved February 22, 2010, from www.jerichoforum.org

Johnson, L., Adams, S., & Cummins, M. (2012). *The MMC Horizon Report: 2012 Higher Education Edition.* Austin, Texas: The New Media Consortium.

Kahn, K. M., & Malluhi, Q. (2010). Establishing trust in cloud computing. *IT Professional*, 20-27. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5593036&isnumber=5593026

Kalyvas, J. R., Overly, M. R., & Karylyn, M. A. (2013a). Cloud computing: A practical framework for managing cloud computing risk. Part 1. *Intellectual Property & Technology Law Journal, 25*(3), 7-8.

Kalyvas, J. R., Overly, M. R., & Karylyn, M. A. (2013b). Cloud computing: A practical framework for managing cloud computing risk. Part 2. *Intellectual Property & Technology Law Journal, 25*(4), 19-27.

Katz, R. N. (2008). The gathering cloud: Is this the end of the middle? In R. N. Katz, *The tower and the cloud. Higher Education in the age of cloud computing* (pp. 2-41). USA: EDUCAUSE.

Katz, R., Goldstein, P., & Yanosky, R. C. (2009, January 22). *Cloud computing in higher education*. Retrieved February 25, 2014, from http://net.educause.edu/section_params/conf/ccw10/highered.pdf

Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011). TrustCloud: A framework for accountability and trust in cloud computing. *2011 IEEE World Congress on Services* (pp. 584-588). Washington, DC: IEEE Computer Soceity. doi:10.1109/SERVICES.2011.91

Kobielus, J. G. (2009, January 20). *Cloud Computing Viewpoint. Cloud services need strong governance.* Retrieved August 26, 2010, from Cloud Computing Journal: http://cloudcomputing.sys-con.com/node/813522

Kumar, G. S., & Weinberg, Z. A. (2011, 19 July). *Havard College to switch Email Provider to Gmail*. Retrieved May 15, 2012, from The Harvard Crimsom: http://www.thecrimson.com/article/2011/7/19/email-gmail-harvard-students/

Kundra, V. (2011). *Federal cloud computing strategy.* White House,[Chief Information Officers Council.

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.

Lethbridge, T. C., & Laganiere, R. (2005). *Object-Oriented Software Engineering: Practical Software Development using UML and Java* (Second ed.). McGraw-Hill.

Linkous, J. (2008, December). Put the 'i' in IT compliance. *Communications News*, pp. 26-28.

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

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011, September 8). NIST Cloud Computing Reference Architecture. *NIST Special Publication 500-292*. Retrieved January 3, 2013, from http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505

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

Lockheed Martin, LM Cyber Security Alliance & Market Connections, Inc. (2010, April). *Awareness, Trust and Security to shape government Cloud Adoption.* Retrieved June 2, 2010, from http://www.lockheedmartin.com/data/assets/isgs/documents/CloudComputingWhitePaper.pdf

March, S. T., & Storey, V. C. (2008). Design sceince in the information systems discipline: an introduction to the special edition on design science research. *MIS Quaterly, 32*(4), 725-730.

Martens, B., & Teuteberg, F. (2011). Risk and compliance management for cloud computing services: designing a reference model. *AMCIS*.

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

McCollum, T. (2011). Regulations top IT Audit concerns. *Internal Auditor, 68*(3), 14-15.

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/

Mell, P., & Grance, T. (2011, January). The NIST definition of cloud computing (draft). *NIST special publication 800-145*. Retrieved January 3, 2013, from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Merriam, S. B. (1998). *Qualitative research and case study applications in education.* San Francisco: Jossey-Bass Publishers.

Meyrick, J. (2006). What is good qualitative research? A first step towards a comprehensive approach to judging rigour/qulaity. *Journal of Health Psychology, 11*(5), 799-808.

Microsoft. (2009). *Free Student Email Accounts and More*. Retrieved April 3, 2010, from Microsoft Live@edu: http://www.microsoft.com/liveatedu/free-email-accounts.aspx?locale=en-US&country=US

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis.* Sage Publications, Thousand Oaks.

Mircea, M., & Andreescu, A. I. (2011). Using cloud computing in education: a strategy to improve agility in the current financial crisis. *Communications of the IBIMA, 2011*, 15. Retrieved from http://www.ibimapublishing.com/journals/CIBIMA/cibima.html

Modi, T. (2009, November 23). *Avoiding the storms: Why we need cloud governance.* Retrieved January 29, 2010, from ebizQ: http://www.ebizq.net/topics/cloud_computing/features/11934.html?pp=1

National education information policy. (2004, August 13). *Government gazette, 471, 26766*. South Africa.

Nawrocki, T. (2011). Data security in a Tech-Crazed world. *Journal of financial planning, 24*(7), 20-25.

Nelson, L., & McCollum, T. (2004). Stepping into continuous audit. *Internal Auditor, 61*(2), 27-29.

Nelson, M. R. (2009, Summer). The Cloud, the Crowd, and Public Policy. *Issues in Science and Technology*, pp. 71-76.

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/

NIST. (2011a). *Guidelines on Security and Privacy in Public Cloud Computing (Draft Special Publication 800-144).* Gaithersburg, MD: US Department of Commerce.

NIST. (2011b, October 31). *NIST US Government Cloud Computing Technology Roadmap Volume iii.* Retrieved from Technical considerations for USG computing deployment decisions. First working draft:

http://www.nist.gov/itl/cloud/upload/NIST_cloud_roadmap_VIII_draft_110111-v3_rbb.pdf

NIST. (2012, May 31). *NIST General Information*. Retrieved January 21, 2013, from NIST: http://www.nist.gov/public_affairs/general_information.cfm

NIST. (n.d.). Inventory of Standards Relevant to cloud computing. *Inventory of Standards Relevant to cloud computing*. Retrieved from http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory

Noirid, S., & Srisa-ard, B. (2007). E-learning Models: A review of literature. *The 1st Interantional Conference of Educational Reform 2007*, (pp. 94-105). Thailand.

Nolan, R., & McFarlan, W. F. (2005). Information technology and the board of directors. *Harvard Business Review, 83*(10), 96.

Northbridge. (2012, June 20). *2012 Future of cloud computing survey results.* Retrieved from http://www.northbridge.com/2012-cloud-computing-survey

OECD. (2004). *OECD Principles of Corporate Governance 2004.* France: OECD Publishing.

Online social networks: Everywhere and nowhere. (2008, March 22). Retrieved June 10, 2010, from The Economist: http://www.economist.com/node/10880936

Osterman Research. (2011, April). *Why the cloud is not killing off the on-premises email market.* Retrieved February 21, 2013, from An Osterman Research White Paper: http://www.altn.com/Literature/WhitePapers/US-Cloud_Vs_Email-WhitePaper.pdf

Ovum. (2010, June 18). *Cloud Computing Governance 'Must Improve'.* Retrieved August 26, 2010, from Data Storage Connection: http://www.datastorageconnection.com/article.mvc/Cloud-Computing-Governance-Must-Improve-0001?atc~c=771+s=773+r=001+l=a

Oxford Dictionaries. (2010, April). Oxford Dictionaries. Retrieved August 2010, 6, from Oxford University Press: http://oxforddictionaries.com/view/entry/m_en_gb0256470

Pacella, R. (2011). Hacking the cloud. *Popular Science, 278*(4), 68-71.

Pearl, M. (2012, June 4). *Cloud for all seasons - A strategic journey for maximum business value.* Retrieved from https://h30613.www3.hp.com/media/files/downloads/Non-FilmedSessions/BB3253_PwC_SRC.pdf

Pearson, S. (2013). *Privacy, security and trust in cloud computing.* Retrieved from http://www.hpl.hp.com/techreports/2012/HPL-2012-80R1.pdf

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008, Winter). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45-77.

Peterson, R. (2004). Crafting information technology governance. *Information Systems Management, 21*(4), 7-22.

Phillips, C. (2009, November). Clearing Away Infrasrtucture Muck. *Baseline,* 11.

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

Posthumus, S., Von Solms, R., & King, M. (2010). The board and IT governance: The what, who and how. *South African Journal of Business Management, 41*(3), 23-32.

PR Newswire. (2012, October 15). Sendmail Research: Organization slowly but surely embracing cloud-based email. *PR Newswire US.*

Prensky, M. (2001, October). Digital Natives, Digital Immigrants. *On the Horizon, 9*(5), 6. Retrieved April 1, 2013, from http://www.marcprensky.com/writing/prensky%20-%20digital%20natives,%20digital%20immigrants%20-%20part1.pdf

Pricewaterhouse Coopers. (2012, January). *The future of IT outsourcing and cloud computing.* Retrieved January 3, 2013, from Events & Trends: http://www.pwc.tw/en_TW/tw/publications/events-and-trends/assets/e255.pdf

Pries-Heje, J., Baskerville, R., & Venable, J. R. (2008). *Strategies for design science research evaluation.* Retrieved January 21, 2014, from http://is2.lse.ac.uk/asp/aspecis/20080023.pdf

Racz, N., Weippl, E., & Seufert, A. (2010). A process model for integrating IT governance, risk, and compliance management. *Proceedings of the Ninth Baltic Conference on Databases and Information Systems,* (pp. 155-170).

Raghuphati, W. (2007). Corporate Governance of IT: A Framework for Development. *Communications of the ACM*, 94-99.

Rana, M., & Fakrudeen, M. (2011). Cloud computing framework and service model for the visually impaired. *International Journal of Technology, Knowledge & Soceity, 7*(2).

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

Rashidi, A., & Movahhedinia, N. (2012). A model for user trust in cloud computing. *International Journal on Cloud Computing: Services and Architecture, 2*(2).

Redmond, T. (2008, October). Looking at Email as a Service. *Windows IT Pro*, pp. 40-45.

Reilly, S. (2011). New assurance standard is required to give cloud users more confidence. *Computer Weekly*(7), 20.

Research. (n.d.). *Oxford Dictionary*. Retrieved from http://oxforddictionaries.com/definition/english/research

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

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

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research methods for business students.* London: Prentice Hall.

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

Schadler, T. (2009b, August 13). *Tier your workforce to save money with cloud-based corporate email.* Retrieved May 20, 2012, from Forrester: http://www.forrester.com/Tier+Your+Workforce+To+Save+Money+With+CloudBased+Corporate+Email/fulltext/-/E-RES54544

Schlarman, S. (2007). The IT Compliance Understanding the Elements. *Information Systems Security, 16*, 224-232.

Schmelzer, R. (2009, July 17). *Cloud Governance Awakes.* Retrieved January 29, 2010, from http://cloudcomputing.sys.com/node/1039534/print

Shea, R., Liu, J., Ngai, E., & Cui, Y. (2013). Cloud gaming: architecture and performance. *IEEE Network, 27*(4). doi:10.1109/MNET.2013.6574660

Shields, P. M., & Tajalli, H. (2006). Intermediate theoory: The missing link in sucessful student scholarship. *Journal of Public Affairs Education, 12*(3), 313-334.

Shivakumar, B. L., & Raju, T. T. (2010). Emerging role of cloud computing in redefining business operations. *Global Management Review*, 48-52.

Srinivasan, M. (2011). Cloud-based email architecture for higher education institutions. *Issues in Information Systems, XII*(1), 339-345.

Suess, J., & Morooney, K. (2009, September/October). Identity management & trust services: Foundations for cloud computing. *EDUCAUSE Review*, 25-42.

Sun Microsystems. (2009, June). Introduction to Cloud Computing Architecture. (1). Santa Carla, CA, USA.

The Economist. (2008, March 19). *Online social networks: Everywhere and nowhere.* Retrieved June 10, 2010, from The Economist: http://www.economist.com/node/10880936

The Radicati Group, Inc. (2012, August). *Corporate IT and business user survey, 2012-2013.* (S. Radicati, Ed.) Retrieved from http://www.radicati.com/wp/wp-content/uploads/2012/08/Corporate-IT-and-Business-User-Survey-2012-2013-Executive-Summary2.pdf

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

Tout, S., Sverdlik, W., & Lawver, G. (2009). Cloud computing and its security in higher education. *The Proceedings of the Information Systems Education Conference 2009. 26*, p. 5. Washington DC: EDSIG.

Van den Bergh, J., & Deschoolmeester, D. (2010). Ethical decision making in ICT: Discussing the impact of an ethical code of conduct. *Communications of the IBIMA*, 1-10. doi:10.5171/2010.127497

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, porcesses and relational mechanisms for IT governance. *Strategies for information technology governance*, 1-36.

van Hoboken, J. V., Arnbak, A. M., van Eijk, N. A., & Kruisjen, N. P. (2012, November). *Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act.* Retrieved April 1, 2013, from Institute for Information Law: http://www.ivir.nl

Viljoen, M., Von Solms, R., & Lawack-Davids, V. (2012). Regulatory Compliance in Cloud Computing: An IT perspective. *SATNAC 2012.* George.

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.

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

Wang, C. (2009, July 1). *Forrster: A close look at cloud computing security issues.* Retrieved January 29, 2010, from CSO: http://www.csoonline.com/article/print/496388

Ward, B. T., & Sipior, J. C. (2010). The internet jurisdiction of cloud computing. *Information Systems Management, 27*(4), 334-339.

Wei, D. (2010). The impact of emerging technologies on small and medium enterprise (SMEs). *Journal of Business Systems, Governance & Ethics, 4*(4), 53-60.

Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results.* Harvard Business Press.

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

Wright, C. S. (2008). *The IT regulatory ans standards compliance handbook.* Syngress.

Yanosky, R. (2010, November/December). From users to choosers: Central IT and the challenge of consumer choice. *EDUCAUSE review*, 46-56.

Yeh, C. (2012). Cloud computing and human resources in the knowledge era. *Human Systems Management, 31*(3/4), 165-175.

Yin, R. K. (2009). *Case study research: design and methods* (Fourth ed., Vol. 5). Thousand Oaks, Calinfornia, USA: Sage.

Zhou, R., & Xie, B. (2010). The educational technology centre: A window to view the progress of Chinese ICT-based higher education. *British Journal of Educational Technology, 41*(4), 642-659.

Appendix A: FACCE detailed guidelines and demonstration information

This appendix includes:

- Appendix A1: FACCE recommended reference list
- Appendix A2: FACCE cloud-based email-specific process guidelines
- Appendix A3: FACCE guiding list of sample high-level criteria
- Appendix A4: FACCE feedback form for evaluators
- Appendix A5: FACCE prototype tool (on accompanying CD)
- Appendix A6: FACCE presentation used during demonstration at the University (on accompanying CD)

Appendix A1

FACCE Recommended reference List

Identifying a set of documents that contain requirements for cloud-based email conformance (hereafter referred to as conformance requirement documents) is an important step in assuring cloud-based email conformance. ISO38500 lists areas in which conformance is necessary. These include conformance with: 1) legal, regulatory and contractual obligations; 2) the IT governance structure used for the institution; 3) various standards and professional guidelines that are relevant and 4) internal policies.

To assist in identifying a set of conformance requirement documents, a set of recommended reference documents are outlined here. These include lists of 1) laws and regulations and 2) standards and professional guidelines that are likely to contain relevant guidance regarding cloud-based email compliance for higher education institutions in South Africa. These lists are not complete, neither are all documents referred to in them necessarily relevant to all higher education institutions in South Africa. It remains each institution's responsibility to determine a complete list of relevant conformance requirement documents. The recommended reference lists do assist with this task, though. They provide an overview of what should be considered a minimum for cloud-based email conformance.

Recommended reading guidance is not provided regarding the IT governance structures used at higher education institutions, since it is assumed that the decisions have already taken place and that there is an established IT governance structure in place that guides all IT initiatives within the institutions. Since internal policies will be different depending on the institution being considered, these are also not considered here.

RECOMMENDED LEGAL & REGULATORY REFERENCES

Understanding which laws and regulations are relevant and how they are to be interpreted is not a trivial matter. Furthermore, understanding which laws and regulations apply to cloud computing solutions is generally an even more challenging process, given the fact that cloud computing solutions may be run across multiple jurisdictional borders. This is true of cloud-based email used in South Africa. Higher education institutions using this solution should not only consider the impact of South African laws and regulations regarding cloud-based email but also the relevant laws that govern the country under which the CSP is bound. This is true whether or not the email is accessed from a proxy server in South Africa. As this is the case,

the recommended reference list for legal and regulatory obligations includes both South African laws and potentially relevant regulations and American laws and potentially applicable regulations. It is ***highly recommended that legal advice be sought when institutions scrutinize these and other laws and regulations that institutions consider as potentially relevant for cloud-based email conformance.***

POTENTIALLY RELEVANT SOUTH AFRICAN LAWS AND REGULATIONS

Michalson is a reputable South African law firm that specializes in IT law. Its website contains legal advice and guidance about various aspects of IT Law, including guidelines about the potential legal implication of using email. An article that provides guidance about which South African laws affect email and how is found at: http://www.michalsons.co.za/email-compliance-email-law-in-south-africa. The laws that are referred to are listed in the table below. South African laws and regulations can be found at the web site www.info.gov.za.

Title	**Where to find**
Electronic Communications and Transactions act, 2002 (ECT)	http://www.info.gov.za/view/DownloadFileAction?id=68060
Regulation of Interception of Communications and Provision of Communication-related information Act, 2002 (RICA)	http://www.info.gov.za/gazette/acts/2002/a70-02.pdf
Companies Act, 2008	http://www.info.gov.za/view/DownloadFileAction?id=98894
Promotion of Access to Information Act, No. 2 of 2000	http://www.info.gov.za/view/DownloadFileAction?id=68186

Table A.1 List of potentially applicable South African laws and regulations

Some of the areas related to email addressed in these laws, as described by Michalsons, are summarized in Table A.2.

Question	Offence	Source
When is it illegal to **intercept emails**?	**ECT 86.** (1 i Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1993). a person who intentionally accesses or intercepts any data without authority or permission to do so. is guilty of an offence. But **RICA** says you may intercept if communication system provided wholly or partly for business use.	ECT, RICA
In setting up accounts with a CSP for cloud-based email in your organisation do you make any **personal information** of any users available to the CSP?	**ECT section 51 (6).** A data controller may not disclose any of the personal information held by it to a third party. Unless required or permitted by law or specifically authorized to do so in writing by the data subject. **PPI**. **''personal information''** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— *(a)* information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; *(b)* ***information relating to the education*** or the medical, financial, criminal or employment history of the person; *(c)* any identifying number, symbol, ***e-mail address***, physical address, telephone number or other particular assignment to the person; *(h)* the ***name of the person*** if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;	ECT, PPI
Do you have a stored record of the **personal information** shared and who it is shared with?	The data controller must for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.	ECT section 51 (7)
May your organisation need to use **emails as evidence**? Can you prove that the message was reliably generated and stored?	Information in the form of a data message must be given due evidential weight. (3) In assessing the evidential weight of a data message, regard must be had to (a) the reliability of the manner in which the data message was generated, stored (b) the reliability of the manner in which the integrity of the data message was (c) the manner in which its originator was identified; and (d) any other relevant factor.	ECT section 15

Email retention	Must keep copies of various records including meeting minutes, accounting info etc. for 7 years. Records must be kept at company and if not somewhere else in SA. When not kept at company must notify where saved. Person has right to request such info and it is an offence if the company doesn't make this info available in a reasonable amount of time.	Companies Act section 24 and 25

Table A.2 Summary of potential legal issues

INTERNATIONAL

It is important to be cognizant of that fact that the laws and regulations of other countries may have to be considered when determining legal risks associated with cloud-based email. This is true even when the higher education institution data is held in a different country. If the CSP conducts systematic business in America, for example, certain American jurisdiction may apply (van Hoboken, Arnbak, van Eijk, & Kruisjen, 2012). Consult with legal advisers to determine the potential legal risks associated with this fact. A paper by van Hoboken et al. outlines some noteworthy legal concerns for higher education institutions using cloud computing. It also provides a summary of how certain American laws and regulations can be applied in this regard. The paper can be accessed at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534. Some of the American laws described in this paper are listed below.

- Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act),
- FISA (Foreign Intelligence Surveillance Act),
- FAA (FISA Amendments Act of 2008) and
- ECPA (Electronic Communications Privacy Act).

The 'Third party doctrine' is also highlighted. The doctrine claims that one's reasonable expectation of privacy is diminished when personal information is handed over to a third party. This may be a potential legal risk that is worth discussing with legal advisers.

CLOUD COMPUTING GUIDANCE

There is currently a vast and possibly confusing array of relatively new guidelines for cloud computing. Table 2 below highlights some of these guidelines by a number of reputable IT governance bodies. A brief summary of what the document contains is also given. The

following table, Table A.3, then highlights some of the guidance provided by other bodies that supply reputable cloud computing guidance. The spreadsheet provided as part of this feedback kit (*FACCE criteria and evidence.xls*) references many of these documents as guidelines for achieving criteria for cloud-based email conformance.

IT Governance Body	**Document Name**	**Summary of contents**
ISACA www.isaca.org/cloud	Cloud Computing: Business benefits with security, governance and assurance perspective	A brief document that highlights some risks associated with cloud computing and suggests some strategies to meet these risks. Suggestions include using SLAs effectively, making cloud computing considerations part of the organisation's overall governance program and considering assurance issues related to transparency, privacy and compliance.
	Guiding principles for cloud computing adoption and use	Explains and give recommendations regarding how the principles of trust, capability, accountability, enterprise risk, cost benefit and enablement can be applied when using cloud computing.
	Calculating cloud ROI: From a customer perspective	Explains the importance of calculating the ROI for cloud computing, the challenges of doing so and guidance on how to do it.
	Security considerations for cloud computing	Describes various risks associated with cloud computing and ways to mitigate such risks with mapping to guidance from COBIT 5. A four-step process is described, which organisations can use to choose a viable cloud computing solution. Decision trees for selecting a cloud service model and selecting a cloud deployment model are given. Factors that organisations have to consider after the adoption of cloud services are also given.
	IT control objectives for cloud computing	Describes how COBIT, Risk IT, Val ITTM and the Business Model for Information SecurityTM (BMISTM) can help organisations adopt and use cloud computing in a way that follows the principles of good governance, is secure and provides a level of assurance. The document describes how the tools listed above can be used together for governance of the cloud. It also describes various assurance frameworks for the cloud and the advantages and disadvantages of each of these. In addition, it maps control objectives from COBIT 4.1 with cloud computing.

	COBIT Process Assessment Model (PAM): Using COBIT 4.1	This has a section for cloud computing.
COSO http://www.coso.org/default.htm	Enterprise Risk Management for cloud Computing	COSO provides a framework that elaborates on the framework for enterprise risk management. In addition, they provide guidance regarding the roles and responsibilities that various managers at different levels of management in the organisation should fulfil regarding cloud computing. They also suggest ways that various cloud computing risks should be dealt with.
ISO http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757	ISO/IEC WD TS 27017	Information technology -- Security techniques -- Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002.
NIST http://www.nist.gov/itl/cloud/	NIST Cloud Computing Standards Roadmap SP 500-291	Provides information about cloud computing architecture and use cases before discussing the need for cloud computing standards. Focuses on standards for interoperability, security and portability. Does a gap analysis to determine what cloud-specific standards are needed. Mainly technical standards are identified as missing. The work does, however, identify the need for standardization of policies and processes to ensure compliance with audit, security and legal requirements. The need for standards to help organisation in the assessment of cloud services before implementation is also highlighted. Cloud-based email is referred to several times in the document to illustrate the need for standardization.
	NIST Cloud computing Reference Architecture NIST SP 500-292	As the title indicates, this document provides a reference architecture that details the various actors, their roles, and the architectural elements that are used for cloud computing. The document also provides a cloud computing taxonomy with various cloud computing terms and definitions.
	NIST SP 500-293. US government cloud computing technology roadmap volume 1:	Volume 1 This document defines and discusses ten high-level requirements for further adoption of cloud computing.

	High-Priority Requirements to Further USG Agency Cloud Computing Adoption	
	NIST SP 500-293. US government cloud computing technology roadmap volume 2: Useful information for cloud adopters	Volume 2 Summarizes the work covered in the NIST documents listed previously in this document. It also lists several high-level concerns related to cloud computing adoption and suggestions to mitigate each of the listed risks. References to work done to assisting in mitigating risks are given after each risk is discussed.
	US government cloud computing technology roadmap volume 2 (First Working Draft) Technical considerations for USG cloud computing deployment decisions	Volume 3 Although this document is still a working draft, it provides guidance that IT decision makers can use when making decisions about adopting and implementing cloud computing. It discusses a "Decision Framework for Cloud Adoption" and provides a set of use cases where the decision framework is applied. The use cases have not yet been completed.
	Guidelines on Security and Privacy in Public cloud computing NIST SP 800-144	This document highlights a number of issues, risks and concerns related to the adoption of public cloud services. It also provides a set of recommendations that organisations considering the use of the public cloud can use.
	The NIST Definition of cloud computing NIST SP 800-145	This provides a widely referenced definition for cloud computing.
	Draft Cloud computing synopsis and recommendations NIST SP 800-146	This provides general recommendations for organisations considering use of the cloud. Recommendations are also given for the different cloud environments (SaaS, IaaS and PaaS) and specific recommendations regarding general terms of use for the cloud are given.
CIO Council https://cio.gov/building-a-21st-century-government/cloud/	Federal Cloud Computing Strategy	The American government's decision to adopt a "Cloud first policy" is explained and justified by highlighting the benefits associated with cloud computing. Risks of cloud computing are listed in the document. A "Decision Framework for Cloud Migration" is also given.
	Creating effective cloud	This briefly discusses the need for and issues related to

	computing contracts for the Federal Government: Best Practice for acquiring IT as a Service	terms of service agreements, non-disclosure agreements and service level agreements. The document also lists and explains prescriptive cloud computing standards and guidelines from NIST.
	State of public sector cloud computing	Describes the work NIST is doing with regard to cloud computing. It provides numerous case studies about the state adoption of cloud computing.

Table A.3: Summary of guidance from IT Governance bodies

Body	**Document Title**	**Summary**
CSA https://cloudsecurityalliance.org/	Security guidance for critical areas of focus in cloud computing version 3.	A method for evaluating tolerance before moving assets to the cloud. Describes a conceptual framework to explain cloud computing. The document also gives recommendations and guidelines in 13 critical areas of focus in cloud computing. These areas involve issues of governance and operation in the cloud.
	Cloud consumer advocacy questionnaire and information survey	The results of a survey of leading CSPs. The survey was conducted to determine the data governance and data security capabilities that these CSPs provide. Areas of maturity and concern are concluded from these findings.
	Trusted Cloud Reference Architecture Quick guide to the reference architecture	The documents present and explain a reference architecture that provides a "methodology and a set of tools that enable security architects, enterprise architects, and risk management professionals to leverage a common set of solutions."
	Top threats to cloud computing survey results update 2012	This is a two-page document illustrating the top threats to cloud computing, as discovered through a survey.
Commission of the European Communities, Expert Group on Cloud Computing	Quantitive Estimates of the demand for cloud computing in Europe and the likely barriers to uptake	This provides a set of recommendations based on the findings of a survey of European organisations about the barriers, concerns and benefits of cloud computing. Recommendations include removing regulatory barriers to adoption, building trust and promoting standardization and interoperability.
	Communication from the Commission to the European Parliament, the	This document outlines plans and recommendations that the Commission makes in order to support and encourage the adoption of cloud computing in Europe.

	Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the potential of cloud computing in Europe.	The main areas that require attention deal with the different legal frameworks that affect cloud computing, problems with contracts and problems related to the proliferation of standards. The work refers extensively to the Digital Agenda for Europe.
ENISA http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing	Cloud Computing: Benefits, risks and recommendations for information security	A list of risks is given. These are rated and explained according to severity. A list of vulnerabilities is also given. In addition, a list of questions is provided which will help organisations ensure that they have adequate information protection when using cloud computing. Furthermore, the document provides a set of legal recommendation for the use of cloud computing.
	Cloud Computing Information Assurance Framework	This "provides a set of questions that an organisation can ask a cloud provider to assure themselves that they are sufficiently protecting the information entrusted to them." The same questions are provided in the document described above.
	Procure Secure. A guide to monitoring of security service levels in cloud contracts.	A subset of the guidelines provided in the assurance framework is presented. The guidelines assist in ensuring security when using cloud services. Once again, a checklist is provided, pertaining to such issues as service availability, log management and incident management.
	Security & resilience in governmental clouds.	Presents a decision-making model that can assist in comparing cloud services and making a decision about cloud services that will meet organisational needs for resilience and security. The report provides a good description and methodology to help analyse legal requirements.

Table A.4: Summary of guidance for cloud computing by other bodies

In Appendix A2, these guidelines are referenced for specific cloud-based email processes. It is, therefore, possible to see the areas of conformance for which each of these guidelines give direction.

Appendix A2

FACCE guidelines regarding cloud-based email specific processes

A process is defined as "a collection of practices influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (e.g., products, services)" (ISACA, 2010b, p. 69).

It is important to have a clearly defined set of processes in place for governing and managing various IT services, including cloud-based email. According to COBIT 5, "Incorporating an operational model and a common language for all parts of the enterprise involved in IT activities is one of the most important and critical steps towards good governance. It also provides a framework for measuring and monitoring IT performance, communicating with service providers, and integrating best management practices".

Determining processes for assuring cloud-based email compliance should not involve reinventing the wheel. Processes that are used for cloud-based email should be based on sound guidance from reputable sources. In addition, they should align with other processes and structures that already make up part of the IT governance and management framework of an institution.

The processes described here for assuring cloud-based email conformance are, therefore, heavily based on the process reference model described by a widely accepted framework for IT governance and management (COBIT 5). They are also solidly based on guidance provided by various reputable bodies regarding cloud-computing practices. Where applicable, each process described here refers to both the cloud computing guidelines and the guiding high-level processes from an accepted IT governance and management framework. The guiding high-level processes should always be consulted in conjunction with the cloud-based email-specific process to determine guidance regarding how the process is "defined, created, operated, monitored, and adjusted/updated or retired" (ISACA, 2011).

Each process description will also include a process goal, which will describe the desired result of the process. Activities associated with each process will also be listed where necessary.

A complete set of processes for assuring cloud-based email conformance is not provided here. Details of the processes described may also not be applicable to all institutions. Each

institution should undertake to determine a set of processes for assuring cloud-based email conformance. The processes listed and described here may merely assist in performing this task.

P1. Ensure internal compliance and alignment of strategy

Process goal: *Cloud-based email initiatives should be aligned with the overall strategies and other high-level directives provided in the institution's IT governance and management framework.*

Process description: It is assumed that every well-governed institution has a defined framework for IT governance and management in place and that it communicates its principles and strategies clearly. As such, there should already be a number of guiding principles, architectures and mechanisms in place that govern all IT projects. Cloud-based email initiatives should align with these.

Activities:

- Ensure that decisions regarding the use and implementation of cloud-based email should align with the culture, ethics and behaviour that are promoted within the institutions. Where necessary, state how the institution's culture, ethics and behaviour should impact cloud-based email initiatives as criteria. This could include matters such as behaviour towards risk taking and following policies.
- Examine the institution's stated strategy, vision, mission, goals and objectives and ensure that the use of cloud-based email aligns with these and that criteria for cloud-based email conformance is determined from these.
- Ensure that existing principles, policies and frameworks within the institution are periodically reviewed to ensure that the requirements they contain relate to cloud-based email (for example, matters such SLAs and document retention) and are recognized as criteria for conformance.
    - Internal policies should always accurately reflect the relevant requirements. To ensure this, with regard to cloud-based email, as the institution's use of cloud-based email changes, policies should be reviewed for relevance and adjusted where necessary.

- Adjusted policies should be accessible to all relevant stakeholders. Obsolete information should be appropriately archived or disposed of.

- Examine the governance framework of the institution to identify components or enablers (such as structures, principles, processes, architectures and practices to achieve the institution's mission, goals and objectives). Decisions regarding cloud-based email should always align and ensure that this takes place. These identified components are likely to include guidelines regarding matters such as policy development, risk management, managing contracts and the organisational structure that should influence cloud-based email activities.
- Establish a set of cloud-based email-specific processes for addressing criteria for cloud-based email conformance.

  There should be one or more processes in place for addressing each criterion identified for assuring cloud-based email conformance. All initiatives for the governance and management of cloud-based email (including a framework for managing policies) should align with the guidance provided by IT governance and management frameworks adopted by the institution. These processes should also be aligned with other relevant accepted standards and good practices. To assist with this, the following activities may help:
  - The processes described by the IT governance and management framework (possibly in the form of a processes reference model) adopted by the organisation should be consulted to determine high-level processes that address the various requirements outlined in the criterion for assuring cloud-based email conformance.
  - Cloud-based email-specific processes should be identified or defined to complement the high-level processes identified in the previous step.
  - Where necessary, more detailed guidelines for using and implementing processes from reputable bodies, such as CSA or the institution's chosen CSP for cloud-based email, should be sought.
  - Practices defined in the guidance found in the preceding steps should be adapted or expanded where required to assure cloud-based email conformance.
  - Directives regarding how processes will be implemented should be communicated.
  - The capability levels of the processes for cloud-based email conformance should be periodically reviewed and communicated.

Related high-level processes: This involves many high-level processes, including COBIT 5: EDM01 (Set and maintain governance framework), APO 1 – APO 3 (Define the management framework for IT, define strategy and manage enterprise architecture).

P2. Risk management

Process goal: *Ensure that risks related with cloud-based email are identified, assessed and responded to in a manner that is in line with the risk appetite and risk management strategy of the institution.*

There are various concerns regarding risks related to cloud computing. Risk management is, therefore, an important aspect of assuring cloud-based email. There are several guidelines to assist with addressing various types of risks related to cloud-based email. This process describes broadly what is to be done at a high-level. The guidelines referred to provides more detailed information.

Although this process relates to identifying all types of risks, including legal risks, the next process addresses the area of legal and regulatory risk in more detail.

Activities:	**Guidelines:**
Identify various types of risks, including: legal and regulatory risks, business and operational risks, security risks and IT services risks.	Horwath, C., Chan, W., Leung, E., & Pili, H. (2012, June). *Eneterprise Risk Manage for Cloud Computing.* Retrieved January 13, 2013, from COSO: http://www.coso.org/-erm.htm ISACA. (2012). *Security Considerations for Cloud Computing.* Rolling Meadows, IL, USA: ISACA. NIST. (2011, November). *US Government Cloud Computing Technology Roadmap Volume II Release 1.0 (NIST Special Publication 500-293).* Retrieved January 13, 2012, from Useful information for cloud adopters: http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeII.pdf CSA, 2011. *Security guidance for critical areas of mobile computing version 3.* [Online] Available at: https://cloudsecurityalliance.org/research/security-guidance/#_overview [Accessed 13 January 2013].
Assess risks. This may	ENISA. (2009, November). *Cloud computing: benefits, risks and*

involve assessing the likelihood and impact of risks.	*recommendations for information security.* (D. Catteddu, & G. Hogben, Eds.) Retrieved June 10, 2010, from http://www.ifap.ru/library/book451.pdf
Develop and document risk response.	Horwath, C., Chan, W., Leung, E., & Pili, H. (2012, June). *Eneterprise Risk Manage for Cloud Computing.* Retrieved January 13, 2013, from COSO: http://www.coso.org/-erm.htm CSA, 2012. *Cloud Control Matrix.* [Online] Available at: https://cloudsecurityalliance.org/research/ccm/

Related high-level processes: COBIT 5: EDM03 (Ensure Risk Optimization), APO12 (Manage Risks)

P3. Ensure legal and regulatory compliance

Process goal: *Ensure the institution complies with all requirements related to cloud-based email imposed on it by legal and regulatory bodies.*

Activities: The process described here should aid in ensuring compliance with laws and regulations related to cloud-based email. Although the steps outlined are intuitive and simple, it is advisable to consult with legal experts during this process. IT experts and other staff members who have not been trained in legal matters may be ill-equipped to draw up legally binding contracts and 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.

- ***Identify legal risks and requirements*** - To identify legal risks, organisations may firstly need to identify and investigate the pertinent regulations 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.
    - ***Identify the legal and regulatory environment*** - There are several South African laws that have a bearing on email management in South Africa. These include some of the laws and regulations listed in Appendix B. Once an organisation is aware of the specific legal requirements that are applicable to the service under consideration, it 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.

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

A comparison between legal requirements and the answers to questions about service provisioning by the CSP would help organisations identify legal risks. Organisations then have the task of attempting to mitigate these risks.

- ***Adhere to criteria for legal conformance and mitigate legal risks*** by using one or more of the methods described below:
  - Contract - Once an organisation has determined which legal risks would need to be addressed, before outsourcing a service to a CSP, the organisation may be able to mitigate some of these risks by negotiating a contract with the CSP. Organisations should carefully assess their contracts to ensure that legal liability is minimized. The contract may be able to demonstrate how the organisation and CSP could agree to a way of provisioning the service in a manner that would allow the organisation to demonstrate compliance. CSPs may not be willing to negotiate contracts with individual organisations, though. Legal risks may, in such cases, still be mitigated by adjusting the organisation's policies, procedures and technical controls.
  - Policies and procedures - Organisations 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. Adjusting internal policies and procedures before adopting a cloud-based service may be essential to ensuring that the company shows internal compliance.
  - Reject service- If organisations are not able to mitigate legal risks to an acceptable level, they must find another way of getting the service they want. The solution may be to improve IT services within the organisation. Using a hybrid cloud-

deployment model could also enable organisations to receive some of the benefits associated with cloud computing, while avoiding certain legal risks.

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

Guidelines: The following document contains a methodology for legal and regulatory compliance in Annex 1: Cattedu, D., 2011. *Security and Resilience in Governmental Clouds.* [Online]
Available at: http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

Related high-level processes: COBIT 5: MEA03 (Monitor and evaluate compliance with external requirements), APO12 (Ensure risk management)

P4. Ensure value

Process goal: *Ensure that optimal value is achieved through the use of cloud-based email by ensuring that anticipated value of cloud-based email is evaluated and communicated and that goals for achieving value are monitored and attained.*

Process description: One of the main goals of IT governance is to *add value to the organisation* (Van Grembergen, De Haes, & Guldentops, 2004, p. 7). The process for determining value is largely dependent on identifying risks and rewards. Information gained during risk management should, therefore, serve as input into this process. For value to be achieved, goals and benefits should also align with the business strategy. Information gained during the process of ensuring alignment with strategy should also feed into this process for ensuring value.

Once risks have been identified and alignment with strategy has been evaluated, value optimization largely depends on evaluating, monitoring and communicating this information, along with information regarding anticipated benefits.

- During the evaluation of cloud-based email, the anticipated benefits that are expected to be derived from the use of this service should be identified and recorded. Where necessary, how the achievement of these benefits is to be measured should also be identified. Actual

achievement of such benefits should then be monitored and reported on. Many of the benefits of cloud-based email are obvious, but they should still be clearly stated.

- Risks vs. benefits should be analysed.

To have a complete view of value, the following questions ought to be addressed and recorded.

- Are we doing the right thing? Does the use of cloud-based email align with the institution's vision, principles and strategy?
- Are we doing this in the right way? Does cloud-based email fit with the existing enterprise? Does it adhere to the architectural principles of our institution? Is it in line with other initiatives?
- Are we doing this well? Is cloud-based email implemented effectively? Are there effective processes, policies and reporting metrics in place to ensure cloud-based email is used effectively?
- Are we getting the benefits? Is the institution getting the benefits expected? (ISACA, 2011).

Related guidelines:

ISACA, 2011. *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud.* Rolling Meadows(IL): ISACA.

ISACA, 2012a. *Calculating Cloud ROI: From the Customer Perspective.* [Online] Available at: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Calculating-Cloud-ROI-From-the-Customer-Perspective.aspx

Related high-level processes: COBIT 5: EDM02 (Ensure Value Optimization)

P5. Manage relationship with CSP

Process goal: *Relationships with the CSP should be managed to ensure that the service provided meets business requirements, the CSP is operating in an effective and compliant manner and that contracts and service level agreements are managed properly.*

Process description: Agreements form an important part of the relationship between the institution and the CSP. Depending on the nature of the relationship between the institution and the CSP, these agreements may or may not be modifiable.

- These agreements should be evaluated to determine:

    - Parameters that inform the interaction between the institution and the CSP.
    - Responsibilities and potential risks that may be imposed on the institutions through these. It is recommended that legal advice is sought in this regard.
- Direction should then be given regarding how contracts and agreements should be managed.
- There should be a system in place to monitor and report on the extent to which SLAs are being achieved. Metrics and parameters should be monitored and reported on to determine the extent to which agreed upon service levels are being met.
- Decisions regarding the need for services or applications that assist with the management or governance of cloud-based email (for example, broker-like services that keep a record of metrics such as availability, incidents over time, etc.) should also be examined and implemented where necessary.
- Contracts and information regarding the monitoring of SLAs should be audited periodically.
- SLAs regarding email services between the institution and users should also be modified and communicated where necessary, as the institution's use of cloud-based email changes.
- The CSPs performance regarding effectiveness and compliance should be monitored, and adjustments should be made to the relationship where it becomes necessary.

Related guidelines:

ENISA. (2011, December). *Procure Secure. A guide to monitoring of security service levels in cloud contracts.* Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

CIO Council, Chief Acquisition Officers Council. (2012, February). *Creating Effective Cloud Computing Contracts for the Federal Government. Best Practices for Acquiring IT as a Service.* Retrieved from https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

Related high-level processes: COBIT 5: APO09 (Manage Service Agreements), APO10 (Manage Suppliers)

P6. Assign roles and responsibilities

Process goal: *Ensure that all parties concerned are aware of and are able to carry out their responsibilities related to cloud-based email.*

Process description: A key principle of good IT governance entails ensuring that staff members at various levels of management throughout an organisation are aware of their IT-related responsibilities. With the relatively new field of cloud computing, it is important that this is done as well. Various managers, from the executive level down, carry responsibilities for cloud computing (Horwath, Chan, Leung, & Pili, 2012, p. 21). This principle should be applied to the use of cloud-based email at higher education institutions as well. Executive management (including the board of directors and the chief executive officer) should be aware of the extent to which cloud-based email, services and other cloud computing solutions are affecting higher education, both globally and in South Africa. Executive management personnel should be aware of their responsibility to *ensure that opportunities presented by developments in IT (such as those presented by cloud-based email) are recognized and exploited in a manner that adds value to an organisation and is secure and compliant with regulations, policies, standards and best practice guidelines* (von Solms & Viljoen, 2012). These managers should also be aware of the risks and opportunities associated with these cloud-based services and how their institution is managing them. It is also important that managers from other departments, such as the legal and financial department, are assigned responsibilities to ensure that cloud-based email is properly managed at the institutions. With the concerns about the legal risks involved with cloud computing and the fact that the institution may be entering a contracted relationship with a CSP, it is especially important to make sure that legal advice is sought in the use of cloud-based email. Table A.5 provides some possible responsibilities for various managers at higher education institutions based on the guidelines set forth by Horwath.

Position	Responsibility
Board of directors	• Be aware of the impact and effect of cloud-based email and related services on higher education • Understand how the risks and benefits of cloud-based email are being managed

	• Leverage internal audit resources for assurance that cloud-based email initiatives are in alignment with the organisation's risk appetite and controls philosophy
Chief Executive Officer	• Be aware of the impact and effect of cloud-based email and related services on higher education • Be aware of how the institution is implementing cloud-based email (what deployment model, for which users)
Chief Financial Officer	• Monitor the financial health of the CSP for cloud-based email
Chief Legal Officer	• Ensure that the institution's use of cloud-based email and related services complies with applicable laws and regulations, taking into account that the CSP may be under the jurisdiction of another country • Monitor new laws and regulations that impact the use of cloud-based email and related services and establish a plan for compliance • Review contacts with CSP providing cloud-based email • Provide input on data classification policies and processes for institution email
Chief Information Officer	• Understand and monitor the potential of cloud-based email to support business needs as this service matures • Assist with incorporating cloud-based email governance into the institution's ERM program • Implement a data classification scheme for email • Establish an incident management program for cloud-based email incidents • Monitor and enforce CSP SLAs
Chief Audit Executive or	• Audit the design and effectiveness of controls and processes for cloud-based email and related services periodically

Internal Auditor	• Audit data on the cloud to verify compliance with data classification policies periodically • Audit contractual compliance with CSP

Table A.5: Possible roles and responsibilities for cloud-based email

This process should be implemented in relation to processes defined by the institution's IT governance and management framework for human resource management. Guidance here will likely include information regarding maintaining adequate staffing, job performance evaluation and maintaining skills and competencies

Related guidance: Horwath, C., Chan, W., Leung, E., & Pili, H. (2012, June). *Eneterprise Risk Manage for Cloud Computing.* Retrieved January 13, 2013, from COSO: http://www.coso.org/-erm.htm

Related high-level processes: COBIT 5: APO07 (Manage Human Resources), APO08 (Manage relationships)

P7. Ensure Project management

Process goal: *The adoption of cloud-based email should be treated as a project. As such, all applicable guidelines for project management used by the institutions should be applied.*

The institution likely already adheres to certain guidelines for project management that guide how plans should be initiated, implemented and closed; how stakeholder engagement should be managed and how factors like risk and quality should be managed. These guidelines should inform the adoption and use of cloud-based email as well.

Related high-level process: COBIT 5: BAI01 (Manage programmes and projects)

Appendix A3

FACCE guiding list of sample high-level criteria

Compliance area	Criteria	High-level process	Cloud-based email specific process
Internal Compliance	Cloud-based email initiatives should be aligned with the overall strategy and other high-level directives provided in the institution's IT governance and management framework.	NA	FACCE: P1
Risk Management	Risks related with cloud-based email should be identified, assessed and mitigated in a manner that is in-line with the risk appetite and risk management strategy of the institution.	COBIT 5: EDM03 (Ensure Risk Optimization), APO12 (Manage Risks)	FACCE: P2
External Compliance	The institution should ensure and gain assurance that it complies with all requirements related to cloud-based email imposed on it by legal and regulatory bodies.	COBIT 5: MEA03 (Monitor and evaluate compliance with external requirements), APO12 (Ensure risk management)	FACCE: P3, P2
Value Optimization	Optimal value should be achieved through the use of cloud-based email by ensuring that anticipated value of cloud-based email is evaluated and communicated and that goals for achieving value are monitored and attained.	COBIT 5: EDM02 (Ensure Value Optimization)	FACCE: P4
Manage relationship with CSP	Relationships with the CSP should be managed, ensuring that the service provided meets business requirements, the CSP is operating in an effective and compliant manner and that contracts and SLAs are managed.	COBIT 5: APO09 (Manage Service Agreements), APO10 (Manage Suppliers)	FACCE: P5

Manage roles and responsibilities	All parties concerned should be aware of and able to carry out their responsibilities related to cloud-based email.	COBIT 5: APO07 (Manage Human Resources), APO08 (Manage relationships)	FACCE: P6
Ensure proper project management	The adoption of cloud-based email should be treated as a project, and, as such, all applicable guidelines for project management used by the institutions should be applied.	COBIT 5: BAI01 (Manage programmes and projects)	FACCE: P7
Ensure security	The security of cloud-based email should be ensured at the institution.	COBIT 5: DSS07 (Manage security)	

Appendix A4

Thesis

Melanie. Viljoen

Dear respondent,

Thank you very much for agreeing to provide feedback regarding a Framework for Assuring the Conformance of Cloud-based Email (FACCE).

To assist with this process, please take a few minutes to listen to the presentation (*FACCE brief description*) provided with this feedback form for a description of FACCE.

Please send your feedback either to Melanie Willett at Melanie.Viljoen@nmmu.ac.za or Prof Rossouw Von Solms at Rossouw.VonSolms@nmmu.ac.za/ 0415043604.

Once again, thank you for your assistance.

Kind regards,

FACCE designers

Using your feedback

FACCE has been developed as part of a PHD studying regarding the use of cloud-based email at higher education institutions in South Africa. FACCE is meant to provide a high-level, conceptual framework that can be expanded and adapted by higher education institutions in South Africa to assist with assuring cloud-based email conformance with internal and external requirements. Therefore although, FACCE provides more detailed guidelines regarding the implementation of the framework, your feedback will be used primarily to verify whether FACCE meets its primary goal of providing a means of assisting higher education institutions in South Africa with assuring the conformance of cloud-based email at a higher conceptual level.

1	Do you believe that using FACCE as a guide for implementing a program for assuring cloud-based email conformance could improve the level of *assurance* associated with cloud-based email at your institution? Why do you say so?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Comments						
2	Do you believe that using FACCE as a guide for implementing a program for assuring cloud-based email conformance could improve the level of *trust* associated with cloud-based email at your institution? Why do you say so?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Comments						
3	Do you believe that using FACCE as a guide for implementing a program for assuring cloud-based email conformance would improve the level of *conformance* associated with cloud-based email	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

	at your institution? Why do you say so?					
Comments						
4	Do you believe that using FACCE as a guide for implementing a program for assuring cloud-based email conformance could assist in demonstrating *due diligence* with regard to cloud-based email at your institution? Why do you say so?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Comments						
5	Do you believe that using FACCE as a guide for implementing a program for assuring cloud-based email conformance would make it easier to provide information for *auditing* cloud-based email? Why do you say so?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Comments						
6	Do you believe that the principles demonstrated in the prototype tool (provided as a simple example of a tool for gathering and analysing cloud-based email assurance and conformance information) could be expanded and modified into a useful tool at your institution? If so to what extent? Please explain your answer.	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Comments						
7	Do you believe that the recommended reference list and/or the cloud-based email specific processes could be modified and expanded to be useful to your institution? To what extent? Why do you say so?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Comments	
8	What do you think the most useful features of FACCE are?
Comments	
9	What features of FACCE do you think are most unlikely to be useful or practical for assuring cloud-based email conformance?
Comments	

10	Do you think FACCE would be practical and easy to implement?	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Comments						
11	Do you have any other opinions or suggestions regarding FACCE?					
Comments						

Thank you!

Appendix A5

FACCE prototype tool (on accompanying CD)

Appendix A6

FACCE presentation (on accompanying CD)

Appendix B: Publications

This appendix includes:

Appendix Number	***Publication reference***	***Status of publication***
Appendix B1	Von Solms, R., & Viljoen, M. (2012). Cloud computing service value: A message to the board. *South African Journal of Business Management, 43*, 73-81.	Published
Appendix B2	Viljoen, M., & Von Solms, R., & Lawack-Davids , V. (2012). Regulatory Compliance in Cloud Computing: An IT perspective. *SATNAC 2012.* George.	Presented and published in proceedings
Appendix B3	Viljoen, M., & Von Solms, R. Cloud-based email adoption at Higher Education Institutions in South Africa. *Africa Education Review.*	Under review at journal
Appendix B4	Von Solms, R., & Viljoen, M. Towards cloud computing assurance. *South African Journal of Business Management*.	Under review at journal
Appendix B5	Willett, M., & Von Solms, R. (2013). A framework for assuring the conformance of cloud-based email. Paper presented at *The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, London	Presented and to be published in proceedings

Appendix B1

Cloud computing service value: A message to the board

R. von Solms* and M Viljoen

School of ICT, Nelson Mandela Metropolitan University,

PO Box 77000, Port Elizabeth 6031, Republic of South Africa

Rossouw.VonSolms@nmmu.ac.za

Received September 2011

This paper aims to alert the board to their duty of adding value to the organizations they represent by recognizing opportunities presented by new developments in information technology. Cloud computing is one such development, which is associated with opportunities and benefits. The service value that can be achieved by using this computing model will be influential in the adoption of cloud computing services. Service value is determined by the warranty and utility associated with that service. Thus, if an organization can associate itself with the utility and warranty on offer via cloud computing, it should consider the adoption of these services. Cloud computing is discussed in terms of service value. This promotes an understanding of factors to be considered when making decisions about the adoption of cloud computing.

This material is based upon work supported financially by the National Research Foundation.

*To whom all correspondence should be addressed.

Introduction

Information Technology (IT) plays an integral part in the operation of many businesses today. In view of the critical role of IT, the board of an organization has the responsibility of ensuring that it is governed in a sound manner. In line with governance principles, the board is responsible for ensuring that new opportunities related to innovative IT developments are recognized and acted on, so that *value* is added to the organization they represent. A relatively new development in IT is cloud computing. There are significant benefits and opportunities associated with this computing model. In order for the board to make a responsible decision with regard to the adoption of cloud computing, the value that can be achieved with this development in IT will need to be analyzed. The IT Infrastructure Library (ITIL) describes how *service value* can be realized in terms of *utility* and *warranty*. This paper discusses the board's responsibility with regard to IT governance. In particular, it describes cloud computing in relation to ITIL's description of service value, in order to promote a clearer understanding of factors to be considered when decisions are to be made

regarding the adoption of cloud computing. In this day and age, when IT governance is part of the mandate of the board of every organization, it is imperative that proper guidelines be provided to assist the board with these critical decisions.

Executives' IT related responsibilities

IT is no longer merely a technical concern which merely involves IT staff. It has become an integral part of all business. The board of an organization, not the IT staff, is ultimately and jointly responsible for ensuring that IT is used in a manner that supports business objectives; and that it is well governed, secure and compliant. Business executives and directors should be aware of the opportunities presented by new IT developments; and they should act accordingly. The following paragraph provides more information on this matter.

The board of an organization has the responsibility of ensuring that sound corporate governance is practiced in the organization. According to the *OECD Principles of corporate governance* (2004), a key fiduciary requirement of the board is the duty of care. This requires that the board should always "act on a fully informed basis, in good faith, with due care and diligence." Since information and IT have become vital to the functioning of most organizations, IT governance is an essential part of all corporate governance. The board is, therefore, required to practice the duty of care with regard to IT. The fact that members of the board may fail to understand the importance and impact of IT on the business has, however, been identified as a problem in the exercising of effective IT governance (Nolan & McFarlan, 2005; Posthumus, von Solms, & King, 2010). Specific responsibilities that the board has with regard to IT governance are highlighted by: *The King Report on Corporate Governance for South Africa 2009* (IoDSA, 2009), hereafter referred to as King III, the *Board Briefing on IT Governance* (ITGI, 2003) and the ISO38500:2008 standard for *Corporate governance of information technology*. Some of these responsibilities are summarized in the list below.

The board of directors should:

- Give strategic direction that is in the best interests of the organization. Part of this mandate includes the assessment of business opportunities (OECD, 2004; IoDSA, 2009).

- Ensure that opportunities associated with new IT developments are recognized and acted on (ISO, 2008; ITGI, 2003; IoDSA, 2009).

- Ensure value delivery from IT (IoDSA, 2009; ITGI, 2003) (IoDSA, 2009; ITGI, 2003).
- Ensure that IT risks are adequately addressed (IoDSA, 2009; ITGI, 2003).
- Ensure compliance with applicable IT laws, rules, codes, standard, guidelines and leading practice (ISO, 2008; IoDSA, 2009).
- Remain accountable for enforcing and monitoring effective IT governance, even when the responsibility for the provisioning of IT services has been delegated to another party (IoDSA, 2009).

From the above, it is clear that *the board is responsible for ensuring that opportunities presented by developments in IT are recognized and exploited in a manner that adds value to an organization and is secure and compliant with regulations, policies, standards and best practice guidelines.* In carrying out their responsibility in this regard, the board will delegate duties to other staff. Managers at all levels throughout the organization should, therefore, work together to ensure that IT governance is effectively accomplished. Opportunities related to new developments in IT should, therefore, be of interest to business executives, and not just to IT staff. The board has the responsibility of exploiting new business opportunities, including IT opportunities that can possibly add value to the organization. One such opportunity is cloud computing.

Cloud computing

Simply explained, cloud computing is a computing model which allows one to access an IT service over a network, as or when it is needed, without worrying about the technical details of how the service is provided. It can be likened to using a shared form of transport instead of one's own car, when needed. There are times when one's needs are best met by using one's own car; but using shared transport may, on occasions, better suit one's needs. To illustrate this point, it may be more convenient for one to ride to work in one's own car; however, if one is planning a trip from Johannesburg to Cape Town one may, in fact, decide to use a means of public transport, such as an aeroplane. In the same way, at times it is best for one to have one's own computer with programs installed on it. There are, however, cases when one would derive substantial benefit from accessing IT resources, such as certain programs or services, over a shared network (using cloud computing). This analogy for cloud

computing explains cloud computing in a very simplified manner. A more comprehensive definition of cloud computing is, in fact, provided by the National Institute of Standards and Technology (NIST). NIST (Mell & Grance, 2009) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." This model is characterized by five essential **characteristics,** three **service models**, and four **deployment models**. These are depicted in Figure 1. NIST describes each of these characteristics, service models and deployment models in more detail. For the purpose of this article, though, only the different deployment models are of interest; and these are described in more detail in the paragraph below.

Cloud computing can be deployed by using private, community, public or hybrid models. The deployment models used for the implementation of cloud computing will affect the level of direct control that organizations have over cloud computing services.

- A **public** cloud describes when IT resources, which are owned and managed by a third-party vendor, are accessed by the general public or by a large industry group over the internet. Public clouds provide the lowest level of direct control by user organizations. The reduction of start-up costs and benefits of freeing up the organization's own IT staff to focus on IT solutions for business problems may, however, be more easily achieved with this model. To use the transport analogy again, a company may at times find it cheaper and easier to use the public transport system to move employees to certain destinations and back, rather than purchasing and using vehicles for the organization for this purpose. For example, if a number of employees from a company in Johannesburg at times have to go for meetings in Cape Town, it would probably be more economical and easier for the company to use the national airlines for this purpose, rather than having a company plane. The company does not, however, have control over the airline, and therefore, has no way of controlling matters, such as the number of delays or the flight schedules.

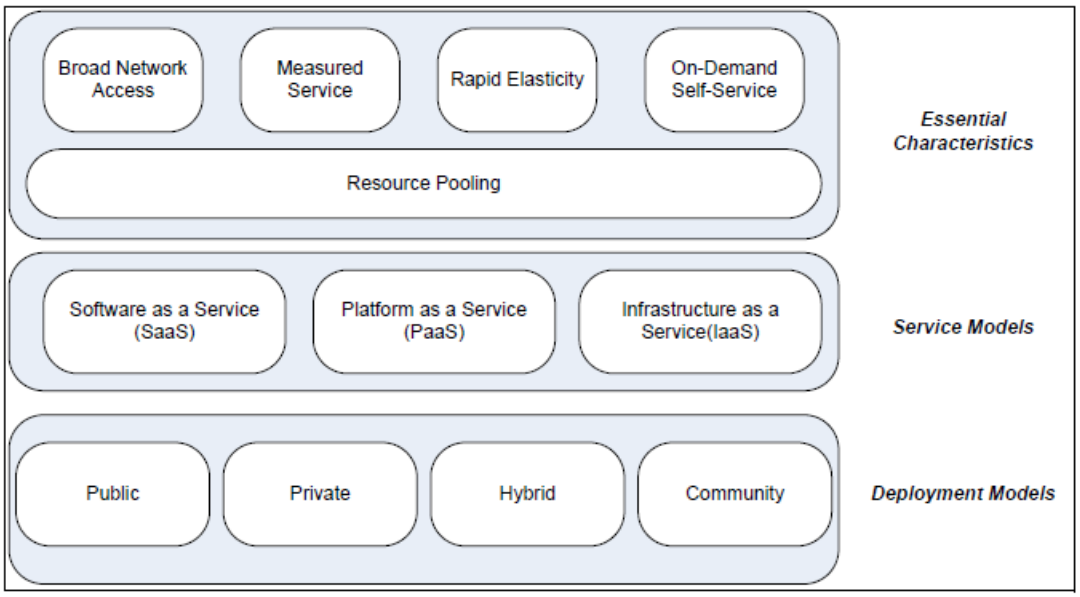


Figure 1: Cloud computing defined. Adapted from (CSA, 2009)

- A **private** cloud is formed when IT resources are virtualized, so that they are available as a pool of resources that can automatically be provisioned on demand within a single organization. A private cloud belongs to only one organization, and is managed either by the user organization or by a third party. The cloud can exist either on or off the premises of the associated organization. The organization implements and manages the cloud directly. The organization, therefore, has a high level of control and transparency; and it is, therefore, more easily able to effectively govern such a private cloud. The use of a private cloud can be likened to a company providing a shuttle service for transporting employees to and from work. This may initially cost the organization more than if all the employees were to get to work using the public transport system, but the organization is in complete control of the system. They can, consequently, arrange the times and routes for the shuttle. When there is a failure in the public transport system, such as when a strike in the bus or taxi sector occurs, the organization's shuttle service can still operate without any problems. A **community** cloud supports a community of users, and can be managed, either by the organizations or by a third party of their choice. This could be compared with a number of companies that get together and hire a bus company to transport employees from a certain outlying area to and from work.

- Organizations may also opt for **hybrid** clouds. With this model, two or more clouds are linked in a way that allows data or application portability. For example, an organization

may decide to run certain components of applications in a public cloud, but keep others that use more sensitive information or are more central to the operation of the organization, in a private cloud (Mather, Kumaraswamy, & Latif, 2009, p. 25). To use the transport analogy, this may be likened to the probable scenario where organizations make use of both public transport and their own shuttle system. Organizations may, for example, shuttle employees to certain predefined areas, after which employees must use public transport, such as a bus or taxi to get home.

When making decisions about using cloud computing, organizations would have to decide on a deployment model that would meet their specific needs.

This section has thus far provided an explanation of what cloud computing is. The following subsection highlights two factors that might motivate business managers to consider cloud computing implementation. Some challenges with cloud computing can then be enumerated.

Cloud computing opportunities and challenges

The following two paragraphs highlight two factors that might motivate business managers to consider cloud computing implementation: 1) Cloud computing is expected to change the way organizations operate; and 2) This is a computing model, which is associated with obvious business benefits. Some challenges associated with cloud computing are here mentioned.

1. Cloud computing is having an impact on organizations.

Indications are that cloud computing is a computing model that should not be overlooked, as a mere new hyped technology. According to the results of a survey by KPMG (Chung & Hermans, 2010) "…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." This survey has found that a significant percentage (58 percent) of the participating organizations are already using some cloud computing services; or, they are expecting to adopt cloud computing within the next 12 months. Various other predictions and surveys support these findings (The Open Group, 2011; Bitcurrent, 2011; Focus Market Research, 2011; Gartner, 2011). Companies, such as Amazon, Google, Microsoft, Sun,

and others, have made an effort to enter the cloud market as cloud-service providers (Mather, Kumaraswamy, & Latif, 2009, p. 214). Cloud computing is obviously not a computing paradigm, which is going to single-handedly transform organizations. Using cloud computing services may not even be a viable option for some organizations. The chances are, however, good that at least some of your competitors will use cloud computing even if you personally do not. Cloud computing is, therefore, a new IT development which is worthy of consideration.

2. Cloud computing is associated with obvious business benefits.

The business opportunities associated with the benefits that can be achieved with cloud computing comprise another factor which drives interest in cloud computing. These benefits include: Cost savings, improved flexibility, improved scalability and greener computing (Du & Cong, 2010; Nawrocki, 2011; Shivakumar & Raju, 2010; ISACA, 2009, p. 6; Nelson, 2009; Fingar, 2009, p. 27; Porta, Karimi, Plakskon, & Sharma, 2009, p. 3; Mather, Kumaraswamy, & Latif, 2009, p. 26; Chung & Hermans, 2010, p. 25). These are significant benefits which may provide opportunities to improve the way an organization operates. Clearly, the potential benefits associated with cloud computing will not always be achieved by organizations. Keeping in mind the responsibilities of executives with regard to IT, executives should, however, recognise and investigate opportunities that arise from developments such as cloud computing.

There are, however, various challenges associated with cloud computing. KPMG's survey (Chung & Hermans, 2010, p. 28) found that issues of primary concern in the use of cloud computing include security, legal, privacy and compliance-oriented issues. The Cloud Security Alliance (CSA) is an organization which aims to promote the use of best practice by providing security assurance within cloud computing. It has identified 13 areas of concern for cloud computing (CSA, 2009b, p. 26). These include issues relating to governance and risk management, legal and electronic discovery, compliance, audit, portability and interoperability. These issues are of material concern to the board which is ultimately responsible for, amongst other things, risk management and compliance.

Thus, although cloud computing offers a number of opportunities and benefits, one needs to consider the associated concerns carefully when considering the use of such cloud-based services.

In the previous section it was highlighted that: The board is responsible for ensuring that opportunities presented by developments in IT are exploited in a manner that adds value to an organization and is secure and compliant with regulations, policies, standards and best practice guidelines. It is vital to bear in mind that IT services, regardless of the manner in which they are provided, remain crucial organizational assets. They remain the responsibility of the board, from a governance point of view.

Cloud computing may result in opportunities for organizations to experience benefits, such as cost savings and improved scalability. For this reason, it is imperative that the board should *recognize* these *opportunities*. But, they will only act on these opportunities if this can be done *in a secure and compliant manner*. The opportunities associated with cloud computing should also only be exploited if they will *add value* to an organization. Thus, it is the duty of the board to continuously seek ways and means to add value to the organization. Cloud computing can potentially add much value on how IT services can be afforded. The IT Infrastructure Library (ITIL) particularly highlights a number of aspects related to *value*. These will be discussed in the next section.

Service value

ITIL is the most widely accepted framework of best-practice guidance for IT service management in the world. According to ITIL (Office of Government Commerce, 2007, p. 17), *value* is the combination of *utility* and *warranty*. Utility is referred to as "fitness of purpose." It is communicated in terms of: 1) Outcomes supported; and 2) Ownership costs and risks avoided. Warranty is related to "fitness for use." Whereas utility involves what the customer gets, warranty involves how the service is delivered. ITIL explains that warranty "ensures the utility of the service is available as needed with sufficient capacity, continuity and security" (Office of Government Commerce, 2007). To illustrate these principles in a simple manner, an analogy can be used. If one considers purchasing a software program one would consider not only whether the program would allow one to accomplish an intended task in an easy-to-use, efficient manner (utility), but also whether one would be able to use this program with assurance. It should not be

"full of bugs." This would prevent one getting the support one needs; and the program would not negatively affect the performance of one's computer (warranty). To acquire good value

from a service, both utility and warranty are necessary (Cartlidge, Hanna, Rudd, Macfarlane, Windebank, & Rance, 2007). ITIL represents this relationship graphically in Figure 2. As seen in this figure, to achieve balanced value from services, there must be good levels of both utility and warranty. IT services which either have high utility and low warranty, or *vice versa*, would have unbalanced value, according to ITIL.

Value is "highly dependent on the customer's perceptions" (Office of Government Commerce, 2007, p. 31). According to ITIL, an organization's perception of value is influenced by the attributes of a service that indicate value, experiences with such attributes, relative endowment of other organizations and the image or actual position in the market of the organization (IoDSA, 2009; IT Governance Institute, 2007).

Well-governed organizations are directed in such a manner that IT is used to meet business objectives and to add value (IoDSA, 2009; IT Governance Institute, 2007). It is, therefore, not surprising that the determination of service value is an important consideration when making decisions. Well-governed organizations plan to create value. Value is communicated in terms of utility and warranty. Both are necessary to achieve good value. These issues will be discussed in more depth in the following two subsections.

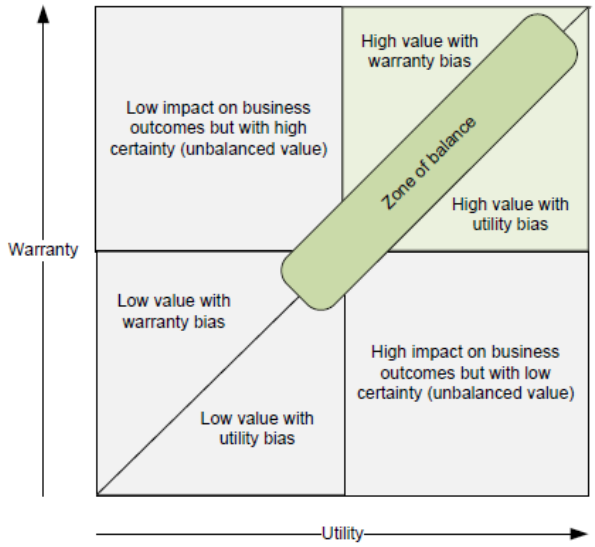


Figure 2 Value communicated in terms of utility and warranty. Adapted from (Cartlidge, Hanna, Rudd, Macfarlane, Windebank, & Rance, 2007)

Utility in the cloud

As mentioned earlier, utility consists of outcomes supported and constraints removed. This section discusses how cloud computing generally influences these two areas that are related to utility.

It is likely that organizations that choose to make use of cloud computing services would do so because of an associated constraint reduction. They are, therefore, expecting utility in terms of limitations removed by using cloud computing services. Constraint reductions can be realized in various ways. Similarly, organizations may consider cloud computing on the basis of expectations that certain outcomes would be supported. Outcomes supported and constraints removed are obviously closely linked. Often a benefit can be described in terms of both constraint reduction and outcomes supported. Therefore, although this section discusses perceptions of constraints removed and outcomes supported separately, it is acknowledged that these areas may overlap significantly.

Surveys by KPMG (Chung & Hermans, 2010), F5 Networks (2009) and Sanhill (Pemmaraju & Rangaswami, 2010) highlight some of the primary benefits in terms of limitations reduced that most organizations expect when using cloud computing services. These include **constraint reductions** in terms of:

- Reduction of costs;
- Improved flexibility or agility; and
- Better scalability.

The extent to which benefits, in terms of constraints removed, are realised in practice will influence the perceived value of cloud computing services. Factors, such as the size of an organization, the organization's in-house IT expertise, the cloud-deployment model and the choice of cloud-service provider (CSP), may all impact on these benefits.

Performance or **outcomes supported** by cloud computing services also affect the utility of these services. Whereas constraint reduction relates to utility in terms of decrease of loss, outcomes supported relates to utility in terms of increased gain by an organization. According to the KPMG survey, cloud computing does not fare as well in this area as it does in supporting constraint reduction. The survey shows that only a small percentage of organizations using cloud computing are experiencing

- Better functionality,
- Improved security, or
- Advanced technology.

In addition, over half of the respondents in the KPMG survey noted that integration with existing IT systems and security needs improvement (Office of Government Commerce, 2007, p. 33).

It is noteworthy that participants in the surveys represented relatively large organizations. It can be argued that small, privately owned businesses without a large IT budget or much IT expertise may acquire more utility in terms of outcomes supported from cloud computing than would larger organizations.

Warranty in the cloud

Factors that contribute to the warranty of a service have already been mentioned, and include the levels of availability, security, capacity, continuity and internal and regulatory compliance that can be guaranteed in the provision of the service. The manner in which warranty is achieved may vary greatly, depending on the environment in which an organization plans to operate. Furthermore, warranty is not necessarily always negatively affected by the adoption of cloud computing. For example: In a small organization with a low IT budget, little in-house IT expertise and an insecure environment, the use of cloud computing may definitely improve service warranty by using services provided by CSPs who have more experience and expertise in providing such a service.

In an organization with a controlled environment, the perception is, however, generally that the less direct control the organization has over the service, the lower the level of warranty. For example, consider an organization that is well governed, implementing various structures, policies, procedures and guidelines to ensure compliance and high levels of service availability, security and continuity. Such an organization has various controls in place to ensure that IT services can be provided with a high level of warranty. They have a high level of control over each service together with an exact knowledge of how security, availability, compliance, and continuity of these services can be implemented, monitored and reported. When using a public deployment model for cloud computing, however, the organization may no longer be able to ensure **availability**. Internet outages, network

problems and problems with the CSP may affect the availability of such a service. In addition, unless the organization has a contractually enforceable service level agreement (SLA) with a CSP, they may have little way of ensuring service **continuity**. Compliance, capacity and security issues may, similarly, affect the warranty by reducing the level of direct control the organization has over the services.

The KPMG survey found that 76% of the respondents indicated that their main concern associated with the use of cloud computing was **security**. Likewise, a survey by CA found that security was one of the primary drawbacks of cloud computing. Interestingly, the KPMG survey found that respondents were more concerned about the lack of transparency than the lack of security measures.

The KPMG survey also indicated that the public sector and financial services (organizations which typically have strong control environments) are less likely to adopt cloud computing (Chung & Hermans, 2010, p. 23). In public organizations legal issues (**regulatory compliance**) can inhibit the adoption of cloud computing. Financial service organizations are likewise slow to use cloud computing – probably because of perceived issues with regard to security and compliance.

Cloud computing service value

Based on the aforementioned, the following issues become apparent:

1. *Users will have to experience real benefits associated with cloud computing for this computing model to be widely adopted.* As stated earlier, ITIL highlights the fact that service value is highly dependent on perception. Surveys, referred to previously, have shown that organizations generally perceive a high likelihood of constraints (such as cost and rigidity) being reduced by the use of cloud computing. If organizations do not achieve any of the real benefits, which they are anticipating while truly implementing cloud computing solutions, this would negatively impact on the general perceptions of utility in the cloud. This would negatively impact cloud adoption in general.
2. *Users would have to be confident of high levels of warranty with cloud computing solutions, if these are to be widely adopted.* Another important factor in the adoption of cloud computing is the perception of warranty associated with the cloud. Services with low levels of warranty have either low or unbalanced value; and they are, therefore, not

likely to be widely used. Some of the warranty-related concerns that users have with cloud computing have already been discussed previously. Figure 3 shows statistics of some of these concerns graphically. These concerns would have to be addressed, in order to improve perceptions of warranty in the cloud; and thereby, positively impact cloud adoption.

3. *Cloud-deployment models that have a higher perceived level of warranty are currently – and will continue to be – the most widely adopted solutions*. The type of cloud-deployment model used affects the level of control an organization has over cloud services. The level of control that organizations in a controlled environment have over IT services is likely to affect the organization's perception of warranty. The cloud deployment models with the highest level of control by organizations, and therefore, the highest perceived level of warranty, are likely to be the most widely adopted cloud models. Figure 4 shows the findings of a survey on the type of cloud-deployment models being considered for use in government agencies (Lockheed Martin; LM Cyber Security Alliance; Market

   Connections, Inc., 2010). As can be seen in the figure, private and hybrid clouds are generally more likely to be adopted than public clouds. Community and hybrid clouds offer organizations more direct control over resources than do public clouds. Private clouds are completely internally controlled and governed; thereby, making it possible to ensure warranty more readily. These are currently the most popular deployment models for government agencies and other organizations (Lockheed Martin; LM Cyber Security Alliance; Market Connections, Inc., 2010; Pemmaraju & Rangaswami, 2010). Public clouds, on the other hand, offer organizations very little direct control of services. They are currently the least popular deployment model for government agencies.

4. *Improved perceptions of warranty with public clouds would positively impact the adoption of this deployment model.* Organizations are still wary of public clouds, but as perceptions of warranty improve, the cloud adoption of this deployment model is likely to improve. A survey of government agencies indicates that trust in the cloud improves with use (Lockheed Martin; LM Cyber Security Alliance; Market Connections, Inc., 2010). It is, therefore, also likely that the perception of warranty of cloud computing will improve with use. It can therefore be concluded that:
5. *The adoption of public clouds will accelerate in time, on condition that perceptions of utility and warranty can be maintained by CSPs.*

The deductions mentioned in this section allow for a high-level understanding of general trends and concerns likely to affect cloud computing adoption. These insights, in turn, can assist board members in making decisions on the adoption of cloud computing services in their organizations. When considering the adoption of a cloud computing service, board members can ask the following general questions:

- What real utility can be achieved by the use of this cloud computing service? Benefits of cloud computing are sometimes hyped. By using this service, can we expect reductions in costs, more business flexibility, and more scalability? Have other companies been using this service? Have they experienced real business benefits?
- How is my business going to be assured of adequate levels of warranty with this cloud computing service? Will there be a contractually enforceable SLA with the CSP? If I use the cloud to provide this service, will we still be able to demonstrate due care and due diligence with regard to the security of the organization's information? Will we still be legally compliant, if this service is provided using cloud computing?
- Considering the information we have gathered regarding the utility and warranty of this cloud computing service, is the use of this service likely to add value to the organization? Which cloud deployment model (public, private, hybrid or community) is going to provide us with the best balance of utility and warranty?
- Adoption of cloud computing is likely to accelerate if CSPs demonstrate the ability to provide utility and warranty. Therefore, if adoption of a specific cloud computing service does not seem feasible at the moment, what is our plan to ensure that we will benefit fully from developments in cloud computing in the future?

The deductions and questions in this section give board members a foundation from which they can make informed decisions regarding the adoption of cloud computing services. Bodies such as the National Institute of Standards and Technology (NIST, 2011b), the European Network and Information Security Agency (ENISA, 2009) and the Cloud Security Alliance (CSA, 2009a) provide more detailed guidelines that may need to be considered in more detail if the decision is made to implement cloud computing services.

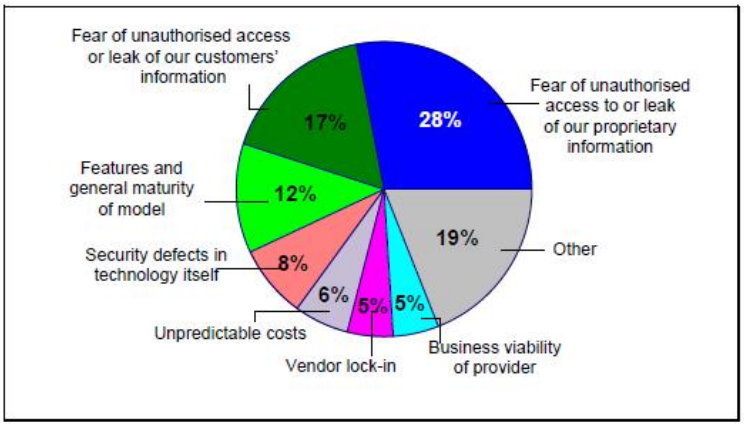


Figure 3 Cloud Computing Concerns. Adapted from (Davis, 2010)

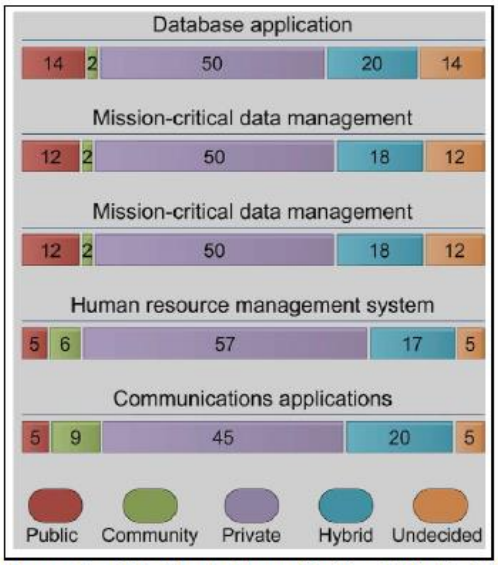


Figure 4 Adoption of services by deployment model. Adapted from (Lockheed Martin; LM Cyber Security Alliance; Market Connections, Inc., 2010)

Conclusion

Cloud computing is a computing model with tremendous potential for benefitting organizations around the world. The board has the responsibility to recognize and act on opportunities presented by such new IT developments – in a manner that will add value to the organization. To determine whether a development in IT, such as cloud computing, would add value to an organization, it is necessary to understand what *service value* is and how it can be achieved. Considering the relatively new concept of cloud computing in terms of how service value is determined, according to ITIL, has allowed us to arrive at some interesting conclusions on the factors that are likely to impact the adoption of cloud computing services. For cloud computing to become a lasting computing model with real value, CSPs are going to have to demonstrate that organizations can derive real utility from

cloud solutions, and that they will have the ability to provide users with guaranteed levels of necessary warranty. Boards which carefully weigh these factors to determine the value that can be achieved by cloud computing in their organizations, will demonstrate that they are aware of the importance of their responsibility in ensuring that opportunities presented by developments in IT are recognized and exploited in a manner that will add value to an organization, and is secure and compliant with all the regulations, policies, standards and best-practice guidelines.

References

Breeding, M. 2009. 'The advance of computing from the ground to the cloud', *Computers in Libraries'*, 29(10), 22 - 25.

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J., & Rance, S. 2007. *An Introductory Overview of ITIL V3.* UK: itSMF.

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

CSA. 2009a. 'Cloud security alliance'. [online] http://www.cloudsecurityalliance.org/ Retrieved January 25, 2010

CSA. 2009b. 'Security guidance for critical areas of focus in cloud computing V2.1'. https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf Retrieved January 25, 2010

Davis, M. A. 2010. 'Global threat, local pain: 2010 strategic security survey'. *InformationWeek.* [online] http://www.informationweek.com/news/galleries/security/vu lnerabilities/226700232 Retrieved 12 February, 2011

ENISA. 2009. *Cloud Computing Information Assurance Framework.* [online] http://www.enisa.europa.eu/ Retrieved

18 January, 2010

F5 Networks. 2009. *Cloud Computing Survey Results June - July 2009.* F5 Networks.

Fingar, P. 2009. *Dot.Cloud: the 21st Century Business Platform Built on cloud Computing.* Tampa, Florida, USA:

Meghan-Kiffer Press.

Fox, R. 2009. Library in the clouds. *OCLC Systems & Services: International digital library perspectives, 25*(3), 156-161.

Harada, Y. 2011. *Study on Cloud Security in Japan.*[online] http://www.isaca.org/Knowledge-

Center/Research/Documents/Cloud_Sec_ITGIJapan_23Feb

2011.pdf

IoDSA. 2009. *The King report on corporate governance for South Africa* September 2009. South Africa: Institute of Directors in Southern Africa.

ISACA. 2009. *Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives.* Rolling Meadows, IL, USA.

ISO. 2008. ISO/IEC 38500:2008 *Corporate Governance of Information Technology*. *International Standard*. Pretoria: SABS Standards Division.

IT Governance Institute. 2007. *COBIT 4.1.*[online]

http://www.isaca.org/KnowledgeCenter/cobit/Pages/Downloads.aspx

ITGI. 2003. *Board Briefing on IT Governance, 2nd Edition.*

USA: IT Governance Institute.

ITGI; PricewaterhouseCoopers LLP.2009. *An Executive*

View of IT Governance.[online] http://www.isaca.org/Knowledge-

Center/Research/Documents/An-Executive-View-of-IT-

Gov-Research.pdf

Jericho Forum. 2009. *Cloud Cube Model: Selecting Cloud formations for secure collaboration.* Retrieved February 22, 2010, from www.jerichoforum.org

Kobielus, J. G. 2009. *Cloud Computing Viewpoint. Cloud services need strong governance.*[online]

http://cloudcomputing.sys-con.com/node/813522

Lockheed Martin; LM Cyber Security Alliance; Market Connections, Inc. 2010. *Awareness, Trust and Security to shape government Cloud Adoption.* [online] http://www.lockheedmartin.com/data/assets/isgs/documents/ CloudComputingWhitePaper.pdf Retrieved 12 February, 2011

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

Mell, P., & Grance, T. 2009. *The NIST Definition of Cloud Computing.* [online] from http://csrc.nist.gov/groups/SNS/cloud-computing/

Nelson, M. R. 2009. 'The Cloud, the Crowd, and Public Policy',*Issues in Science and Technology*, pp. 71-76.

NIST.2009. *Cloud Computing*. [online]Computer Security Resource Centre: http://csrc.nist.gov/groups/SNS/cloudcomputing/

NIST. 2011. *Guidelines on Security and Privacy in Public Cloud Computing (Draft Special Publication 800-144).*

Gaithersburg, MD: US Department of Commerce.

OECD. 2004. *OECD Principles of Corporate Governance 2004.* France: OECD Publishing.

Office of Government Commerce.2007. *ITIL Service Strategy.* UK: The Stationery Office.

Ovum. 2010. *Cloud Computing Governance 'Must Improve'*.

[online]

http://www.datastorageconnection.com/article.mvc/CloudComputing-Governance-Must-Improve-

0001?atc~c=771+s=773+r=001+l=a Retrieved 12 February, 2011

Pemmaraju, K., & Rangaswami, M. R. 2010. *Leaders in the Cloud.* Sandhill Group.

Phillips, C. 2009. 'Clearing Away Infrasrtucture Muck', *Baseline*, 11.

Porta, M., Karimi, A., Plakskon, J., & Sharma, D. 2009. *Capturing the Potential of Cloud*. New York, USA: IBM Corporation.

Appendix B2

Regulatory Compliance in Cloud Computing: An IT perspective

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.

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

Index Terms—Cloud Computing, Cloud computing compliance

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 (ISO/IEC 38500:2008) 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.

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 (2004), 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.

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 (Collins English dictionary and Thesaurus essential edition, 2007). 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 (Giles, 2009).

Ensuring compliance is also an integral part of good governance (ISO/IEC 38500:2008). Good governance in organizations is desirable. Research highlights the benefits of demonstrating good governance (ISO/IEC 38500:2008). 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 (South Africa, 2002), the Electronic Communications Act (UK, 2000) and the USA PATRIOT Act (2001) 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.

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 Security Alliance, 2009, p. 13; Mather, Kumaraswamy, & Latif, 2009, p. 11; Mell & Grance, 2009). Cloud computing can be simply explained by using a utility analogy (ISACA, 2009, p. 4; Breeding, 2009). 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 (Porta, Karimi, Plakskon, & Sharma, 2009, p. 3; Breeding, 2009). 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 (2010) 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.

- "Compliance with regulatory policies on data remains a key hurdle to cloud computing" (Li, Singhal, Swaminathan, & Karp, 2010).
- "Continental also determined that compliance is the greatest barrier to moving IT services to the cloud" (Loebbecke, Thomas, & Ullrich, 2012).
- "Courts will need to determine how existing laws may or may not protect electronic communications and content in this new computing model" (Robison, 2010, p. 1204).
- "Despite the growing popularity of cloud computing services, there appears to be little opportunity for judicial or legislative relief in the near future" (Robison, 2010, p. 1239).
- "Whatever regulatory environment is targeted, cloud-based compliance is nearly always a nontrivial task" (Wood, 2009).
- "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 (Brodkin, 2008).
- "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. (Lanois, 2010, p. 49).

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.

Research has been done concerning applying certain American regulations, such as the Stored Communications Act (SCA) and the Electronic Communications Privacy Act (ECPA) (1986) 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" (Robison, 2010, p. 1239).

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" (Lanois, 2010, p. 49). Lanois (2010, p. 45) 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 (Lanois, 2010, p. 48). 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 (NIST, 2009). 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.

THE IMPORTANCE OF EMAIL COMPLIANCE

Email is a necessary part of many organizations. As stated by Schadler (2009, p. 6), "email is an entitlement, as ubiquitous and expected as an office chair." This is clearly shown in a report by Radicati (2009), 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 (Schadler, 2009, p. 17; Bauer, 2010; Economist, 2008; Ranger, 2008). 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 (Lisa Thornton Inc, 2005).

There is much work and considerable cost involved in maintaining an in-house email solution (Schadler, 2009, pp. 2, 4). A Forrester report has revealed that firms commonly underestimate the full cost of email (Schadler, 2009, p. 4). It is not surprising then, that many companies contemplate cloud-based email solutions with their associated potential advantage of lower costs (LiveOffice, 2009).

The idea of email as a service is not new (Sanborn & Kujubu, 1999; Georgia, 2000). Email-as-a-Service or cloud-based email is one of the cloud services that some foresee will have a marked impact on organizations (Bauer, 2010; Geer, 2008). 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 (Voce, Schadler, Echols, & Burnes, 2009, p. 2).

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" (Voce, Schadler, Echols, & Burnes, 2009, p. 7). According to Schadler (2009, p. 11), 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 (Schadler, 2009, p. 6).

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 (Mather, Kumaraswamy, & Latif, 2009).

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.

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 you 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 emails, 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.

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.

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.

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 (Giles, 2009).

Giles (2009) and Lisa Thornton Inc. (2005) 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. An 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.

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.

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.

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.

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.

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.

REFERENCES

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

Collins English dictionary and Thesaurus essential edition. (2007). UK: HarperCollins Publisher.

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

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/

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

ISO/IEC 38500:2008. (n.d.). Corporate governance of information technology. ISO/IEC.

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.

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.

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

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

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/

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

South Africa. (2002). Electronic Communications and Transactions Act.

UK. (2000). Electronic Communications Act.

USA. (1986). Electronic Communications Privacy Act.

USA. (2001). USA PATRIOT Act.

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.

Appendix B3

Cloud-based email adoption at Higher Education Institutions in South Africa

Authors:

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).

Contact

Institute for ICT Advancement

Nelson Mandela Metropolitan University,

P. O. Box 7700,

Port Elizabeth 6031

Tel: +27 41 5043604, Fax: +27 41 9604

email: Melanie.Viljoen@nmmu.ac.za & Rossouw.VonSolms@nmmu.co.za

Cloud-based email adoption at Higher Education Institutions in South Africa

Abstract

Cloud computing in general is having an impact on organizations today. Cloud-based email in particular is being adopted by educational institutions around the world on a large scale. This paper reports on the state of cloud-based email adoption at higher education institutions in South Africa by describing the findings of a survey of IT managers at sixteen of these institutions. It will show that South Africa follows the global trend of large uptake of cloud-based email for higher education institutions. The fact that although organizations are satisfied with the service they receive from cloud-based email service providers they have several noteworthy concerns regarding the adoption of this service is shown. The fact that IT managers at such South African higher education institutions feel that they will benefit from guidelines for the compliant adoption of cloud-based email is also highlighted.

Keywords: Cloud computing , cloud-based email, cloud computing guidelines, email as a service, cloud computing concerns, cloud computing compliance, higher education, South Africa

Introduction

Cloud computing is a computing paradigm that is causing much interest around the world. It has the potential to allow organizations to utilize computer resources and access IT services for cheaper and with less hassle than ever before (Farah 2010, Mather,

Kumaraswamy and Latif 2009, Shivakumar and Raju 2010). It is however, not a computing paradigm that can always be adopted without hesitation. As with all other IT related matters, managers are obliged to demonstrate due diligence when it comes to making decisions about the adoption of cloud computing. To be able to do this, managers should be fully aware of both the risks and benefits associated with cloud computing. Organizations which adopt new technologies, such as cloud-based solutions, without fully investigating the risks and benefits, can put themselves at risk.

Cloud-based email is a cloud computing service which is rapidly being adopted by organizations internationally. Educational institutions are among the foremost adopters of this cloud computing service (Corbyn, 2009). This paper examines the state of cloud-based email adoption at South African higher education institutions. Firstly the popularity of cloud-based email at educational institutions internationally is highlighted. The state of cloud-based email adoptions in South African universities specifically is then explained by means of an analysis of the results of surveys conducted with IT staff of several South African universities. The findings of the survey include information about what cloud-based email service providers are most popular at South African higher education institutions, how satisfied managers are with the service they receive fom such providers and what concerns such managers have about the service. To begin with though, the term cloud computing is briefly explained below.

Cloud Computing

Cloud computing is a term that has generated much discussion during the last number of years. A search on Google for the term "cloud computing" on 15 July 2010 resulted in about 49,100,000 results. The same search on 14 May 2012 resulted in about 101,000,000 results. Well respected bodies such as NIST (NIST 2009), ISACA (ISACA 2010) and

ENISA (ENISA 2010) have created groups that focus on cloud computing. Bodies devoted to the effective deployment of cloud computing, such as the Cloud Security Alliance (CSA 2009) and the Global Inter-Cloud Technology Forum (GICTF, 2010), have also been formed. Companies such as Microsoft, Google, Novell, Dell, Cisco, Intel, McAffe, Symantec and many others have subsequently become CSA members (CSA 2009). All of these companies, therefore, at least indicate interest in cloud computing. There are also several companies that are acting as cloud service providers (CSPs). Mather, Kumaraswamy and Latif (2009, 214) list some CSPs including Amazon, Google, Microsoft, Salesforce.com and Sun. The investment that companies like these are willing to make to enter the cloud market suggests that they believe that cloud computing will have an impact on the way organizations do business. What is cloud computing though?

Fundamentally cloud computing has to do with the provisioning of services, platforms and fundamental computing resources (infrastructure) as services over the Internet (Cloud Security Alliance 2009b, 13, Mather, Kumaraswamy and Latif 2009, 11, Mell and Grance 2009). Cloud computing can be simply explicated using a utility analogy (ISACA 2009, 4, Breeding 2009). 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 just an abstract idea of where the resources are and how they work. NIST defines it more comprehensively (Mell and Grance 2009) as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

There are a number of concerns that have been raised about organizations using cloud computing services. Some concerns associated with cloud computing found in literature include concerns regarding ensuring security, compliance to both pertinent laws and regulations and internal policies, vendor lock-in and a lack of standards and guidelines about the effective use of cloud computing in organizations.

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 (Porta, et al. 2009, 3, Breeding 2009). Cost reduction is another potential benefit that causes many organizations to be interested in the cloud. According to a recent KPMG survey (KPMG International Cooperative 2011) most organizations are making use of or are planning to make use of various cloud-based solutions. One cloud solution that is being widely adopted in institutions of higher education around the world is that of cloud-based email. The following subsection provides more information about this service.

Cloud-based Email

Email is an important service in most modern organizations. As stated by Schadler (2009, p. 6), "email is an entitlement, as ubiquitous and expected as an office chair." This is clearly shown in a report by the Radicati Group (2009) which projects 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 play an ever increasing role in both personal and professional lives of employees (Bauer, 2010; Ranger, 2008; Schadler, Should your Email live in the cloud? A comparative cost analysis, 2009; Online social networks: Everywhere and nowhere, 2008). As email loads increase, organizations become more dependent on this means of communication.

Traditionally organizations have provided staff with email solutions that have been implemented, maintained, managed and administered by either internal IT staff or by an outsourced IT company. Cloud-based email has emerged as an alternative email solution for organizations. With cloud-based email, organizations receive email services from a service provider, such as Microsoft or Google.

There is much work and costs involved in maintaining an in-house email solution (Schadler, 2009, pp. 2, 4). A Forrester report has revealed that firms commonly underestimate the full cost of email (Schadler, 2009, p. 4). It is not surprising then, that many companies contemplate cloud-based email solutions with their associated potential advantage of lower-cost (LiveOffice 2009).

The idea of email as a service is not new (Schadler 2009, 2, 4). Email-as-a-Service or cloud-based email is one of the cloud services that some foresee will have a marked impact on organizations (Bauer 2010, Geer 2008). 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 (Voce, et al. 2009). 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" (Voce, Schadler, Echols, & Burnes, 2009, p. 7). According to Schadler (2009, p. 11), for mid-size companies' cloud-based email is often cheaper than an in-house email solution. Google and Microsoft make cloud-based email available to schools and universities at no cost. 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 (Schadler, 2009, p. 6). Education institutions that use cloud-based email may also benefit from enhanced services. For example, users of Live@edu not only have access to 10GB mail inboxes that they can access anywhere for life, but are also provided with instant messaging capabilities and 25 GB of free online storage (Microsoft 2010).

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 conformance is demonstrated. Cloud-based email solutions may decrease the level of control organizations have over their email, it does not, however, decrease the responsibility (Mather, Kumaraswamy, & Latif, 2009). It is, therefore, imperative that cloud based email solutions are properly governed to ensure compliance and security as both are core to good governance.

South African Higher Education

Information and education are tightly related. To educate has been defined as providing someone with "training in or information on a particular subject" (Oxford Dictionaries 2010). The introduction of the South African national education information policy (2004) states in part that; "the effective gathering, dissemination and analysis of information in the education system of any country is vital for sound education planning, monitoring and delivery."

It is, therefore, not surprising that ICT plays an important role in higher education. Much research has been done regarding the use of ICT in Higher education (Dodds 2007, Noirid and Srisa-ard 2007, Zhou and Xie 2010). One of the strategic objectives in the strategic plan 2009 – 2013 by the South African department of education (2009) is to support curriculum implementation through the use of ICT. One of the associated targets is to monitor and report on the access to the Internet, electronic communication and the use of ICT for administration and management of education institutions. From the above, the importance of email as a form of electronic communication, specifically in the higher education sector, has been highlighted.

An interesting trend is the rapid adoption of cloud-based email by higher education institutions. The next section discusses this trend.

Cloud-based email and Higher Education

Cloud-based email has had a great uptake among higher education institutions around the world. A report by Zoe Corbyn remarks on work published by Gartner about the hype cycle for education (2009). According to the report cloud-based email has seen a "tremendous uptake" in higher education and is a technology that is "firmly ensconced in the sector." This is evident when the web sites for two of the most popular providers of cloud-based services for education are examined. Microsoft (Live@edu) and Google (Google Apps for Education) both provide education institutions with free access to email and collaboration tools. Google (2011) claims to have "more than fourteen million students and teachers" using Google Apps. Microsoft (2012) states that, "Thousands of educational institutions in more than 100 countries around the world use Live@edu services, accounting for tens of millions of users." Some of the reputable institutions using services provided by Google include Yale University (Carter 2011) and Harvard College (Kumar and Weinberg 2011).

Cloud-based email is a solution which seems to be readily adopted by higher education institutions globally. Is this true in South Africa? Which percentage of South African universities are using cloud-based email and are universities which adopt cloud-based email satisfied with the service they receive from the cloud-based email provider? What are some of the issues which concern university staff about cloud-based email? The following section answers these questions by means of the results of a survey of IT managers of 16 higher education institutions in South Africa.

Cloud-based email in South African Universities

In 2009, and again in 2012, surveys were conducted at a conference of IT managers of South African higher education institutions. In 2009 eight South African institutions responded. This year (2012) sixteen South African institutions responded. This sections outlines the results of the surveys and findings of this study.

1. ***There is major uptake of cloud-based email at South African higher education instituions***

   South Africa is likely to follow the global trend of major uptake of cloud-based email by higher education institutions. In 2009 when asked about plans for using cloud-based email in the future, all respondents who were not already using cloud-based email indicated an intention of implementing it within either one or two years. Figure 1 shows these results.

Figure 1: Cloud-based email adoption in South African higher education institutions in 2009

   Similarly in 2012, by far the majority of the institutions had already started using or intended to use cloud-based email at their institutions in the future. Only one institution indicated that they were not currently planning on using cloud-based email. As can be seen in Figure 2, it is noteworthy that half of respondents had already started using or were currently implementing cloud-based email. Three out of the seven institutors which were planning on using cloud-based email were aiming on doing so within this year. It is expected therefore, that soon most South African higher education institutions will be using cloud-based email in some form.

Figure 2: Cloud-based email adoption in South African higher education institutions in 2012

2. ***Cloud-based email is currently used for students and alumni at South African higher education institutions, not staff.***

All of the respondents that were already using cloud-based email or were in the process of implementing it were using it for students. None of them were outsourcing staff email. When asked whether they are planning on using cloud-based email for staff within the next two years, however, a fair percentage (four from fourteen) of respondents indicated that they would consider doing so. The responses shown in Figure 3 indicated that there is still uncertainty as to whether outsourcing staff email at higher education institutions would be an acceptable solution.

Figure 3: Cloud-based email adoption for staff in South African higher education institutions

Comments from the respondents on this question (shown in Table 1) indicate concerns about being able to provide staff with an adequate level of service and being able to ensure compliance. The comments also indicate that building confidence in cloud-based services is a prerequisite before using such services for staff.

Table 1: Comments regarding cloud-based email for staff

3. ***Live@edu is currently the most popular cloud-based email provider for South African higher education institutions***

As shown in Figure 3, nine out of fifteen (60%) of the institutions who are currently using cloud-based email, or who indicated the intention of using cloud-based email, indicate Microsoft's Live@edu solution as their preferred solution. Interesting five out of the 6 institutions which are already using cloud-based email (83%) are using Live@edu.

Figure 4: Cloud-based email providers preferred by South African Higher education institutions

4. ***South African higher education institutions are satisfied with the service they receive from cloud-based email service providers.***

Most of the institutions surveyed that are currently using cloud-based email are satisfied with the service they receive. This is depicted in Figure 4. In fact 50% of the respondents rate themselves very satisfied with the service they receive. Not a single respondent was dissatisfied.

Figure 5: Satisfaction with cloud-based email in South African higher education institutions

5. ***South African higher education institutions do have noteworthy concerns about the use of cloud-based email.***

Despite the tremendous uptake of cloud-based email, there are concerns regarding the use of this service at higher education institutions in South Africa. Of the sixteen respondents to the 2012 survey, 71% indicated that they do have concerns regarding the use of this service. Figure 6 highlights what some of these concerns are. Regulatory compliance and record management are the issues which most concerned respondents.

Figure 6: Concerns regarding cloud-based email in South African higher education institutions

When given the opportunity to highlight other concerns, IT managers listed amongst other things vendor-lock in and integration issues as concerns. Some comments regarding concerns are shown in Table 2. As Figure 6 shows, there is generally less concern regarding certain issues among institutions who are already using cloud-based email. This seems to indicate that confidence in cloud-based email increases with the adoption of this service.

Table 2: Comments regarding concerns about cloud-based email

The majority of intuitions will use cloud-based email in the future or are currently using it and are satisfied with this service. Still there are many noteworthy concerns regarding the use of this service. This is troubling.

6. ***South Africa higher education institutions feel that they would benefit from a set of guidelines for compliance when using cloud-based email.***

In 2009, seven out of eight respondents either agreed or strongly agreed with the following statement: *I have not been provided with an adequate set of good practice guidelines for the governance, risk and compliance of cloud-based email*. This is shown graphically in Figure 7. Interestingly, the one university which disagreed with the statement did not give an indication of any guidelines they would recommend for cloud-based email implementation when prompted to do so. Further emphasizing the important role of a set of guidelines for compliance using cloud-based email, participants in this year's survey were asked, "Do you think that South African universities would benefit from a set of guidelines for compliance in the adoption of cloud-based email?" Only one out of 17 institutions responded "no". The vast majority of institutions (94%) therefore believe that such guidelines would be beneficial.

Considering the important role of email it is perturbing that IT professionals feel inadequately equipped with regard to the governance, risk and compliance of cloud-based email and are apprehensive about compliance in particular.

Figure 7: Need for cloud-based email guidelines

Conclusion

Cloud-based email has the potential of positively impacting on the delivery of email services at educational institutions. These institutions may derive benefits such as reduced cost, easier email administration, larger inboxes and access to additional services such as instant messaging and online storage for their customers if they utilize cloud-based email. South African higher education institutions are readily adopting cloud-based email. Those using cloud-based email for their students are satisfied with this service. There is, however, concern whether cloud-based email can be used in a way that will be secure, available and compliant. These concerns will have to be addressed for potentially valuable cloud-based

email solutions to be confidently adopted by South African higher education institutions. There is a lack of adequate good practice guidelines regarding ensuring governance, mitigation of risk and compliant use of cloud-based email in higher education institutions in South Africa. Such guidelines may improve confidence when deciding to implement cloud-based email.

References

Bauer, P. 2010. Email as a Service. *CRN.* http://www.channelweb.co.uk/articles/print/2256798 (accessed March 2, 2010).

Breeding, Marshall. 2009. The Advance of Computing From the Ground to the Cloud. *Computers in Libraries'* (Information Today Inc.), November/December 2009: 22 - 25.

Carter, Denny. 2011. *After Balking, Yale switches to Gmail.* http://www.ecampusnews.com/top-news/after-balking-yale-switches-to-gmail/ (accessed May 15, 2012).

Chung, Mike, and John Hermans. 2010. *KPMG's 2010 Cloud Computing Survey.* Netherlands: KPMG.

Computer Security Alliance. 2009. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. http://www.cloudsecurityalliance.org. (accessed January 25, 2010).

Corbyn, Zoe. 2009. Second Life out as techies embrace cloud email. *Times Higher Education.* http://www.timeshighereducation.co.uk/story.asp?storycode=407839 (accessed March 02, 2010).

CSA. 2009. *Cloud Security Alliance.* http://www.cloudsecurityalliance.org/ (accessed Febuary 8, 2010).

Department of Education. 2009. Strategic plan 2009-2013.

Dodds, Ted. 2007. Information Technology: a contributor to innovation in higher education. *New Diretions for Higher Education* (Wiley InterScience) 137: 85-97.

ENISA. 2010. *ENISA Cloud Computing Risk Assessment.* http://www.enisa.europa.eu/act/res/other-areas/cloud-computing (accessed June 5, 2010).

Farah, S. 2010. Cloud computing or software as a service - which makes most sense for HR? *Employment Relations Today* (Wiley Online) 36, no. 4: 31-37.

Geer, David. 2008. Cloud-based Email: Developing technology offers sunny skies to SME IT departments. *Processor.* Vol. 30. no. 36. Sandhills Publishing Company, 23.

GICTF. 2010. *Global Inter-Cloud Technology Forum.* http://www.gictf.jp/index_e.html (accessed May 21, 2012).

Google. 2011. http://www.google.com/apps/intl/en/edu/index.html (accessed May 15, 2012).

ISACA. 2010. *Cloud Computing.* http://www.isaca.org/Groups/Professional-English/cloud-computing/Pages/Overview.aspx (accessed July 5, 2010).

ISACA. 2009. *Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives.* Rolling Meadows, IL.

KPMG International Cooperative. 2011. "Clarity in the Cloud: A Global study of the business adoption of Cloud." *KPMG.com.* http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/cloud-computing/Documents/clarity-in-the-cloud-business-adoption.pdf (accessed May 14, 2012).

Kumar, Gautam S, and Zoe A Y Weinberg. 2011. *Havard College to switch Email Provider to Gmail.* http://www.thecrimson.com/article/2011/7/19/email-gmail-harvard-students/ (accessed May 15, 2012).

LiveOffice. 2009. Cloud Email 101. Cloud Email Buyer's Guide. *Cloud Email 101.* http://www.cloudemail101.org/home (accessed June 10, 2010).

Mather, Tim, Subra Kumaraswamy, and Shahed Latif. 2009. *Cloud Security and Privacy.* First Edition. Edited by Mike Loukides. Sebastopol, CA: O'Reilly Media Inc.

Mell, Peter, and Tim Grance. 2009. The NIST Definition of Cloud Computing. Vers. 15. NIST. http://csrc.nist.gov/groups/SNS/cloud-computing/ (accessed January 29, 2010).

Microsoft. 2010. *Free hosted email, communication and collaboration services.* http://www.microsoft.com/liveatedu/new-student-email.aspx?locale=en-US&country=US (accessed Febuary 15, 2011).

Microsoft. 2012. *Frequently Asked Questions.* http://www.microsoft.com/liveatedu/faq.aspx?locale=en-US&country=US (accessed May 15, 2012).

Microsoft News Centre. 2010. *Universities go back to school with Live@Edu.* http://www.microsoft.com/presspass/press/2010/oct10/10-04msliveedumomentumpr.mspx (accessed Febuary 14, 2011).

Anon. 2004.National education information policy. *Government gazette.* Vol. 471.

NIST. 2009. *Cloud Computing.* http://csrc.nist.gov/groups/SNS/cloud-computing/ (accessed April 13, 2010).

Noirid, Surachet, and Boonchom Srisa-ard. 2007. E-learning Models: A review of literature. *The 1st Interantional Conference of Educational Reform 2007.* Thailand, 94-105.

Anon. 2008. "Online social networks: Everywhere and nowhere." *The Economist.* http://www.economist.com/node/10880936 (accessed June 10, 2010).

Oxford Dictionaries. 2010. *Oxford Dictionaries.* http://oxforddictionaries.com/view/entry/m_en_gb0256470 (accessed August 2010, 6).

Porta, Matt, Anthony Karimi, Joseph Plakskon, and Deepak. Sharma. 2009. Capturing the Potential of Cloud. New York: IBM Corporation.

Ranger, Steve. 2008. Behind the Cloud. *Director*, August: 50-52.

Schadler, Ted. 2009. *Should your Email live in the cloud? A comparative cost analysis.* Forrester, Cambridge: Forrester Research, Inc.

Shivakumar, B. L., and T. T. Raju. 2010. Emerging role of cloud computing in redefining business operations. *Global Management Review*, 48-52.

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

Voce, Christopher, Ted Schadler, Ben Echols, and Sara Burnes. 2009. Should your email live in the cloud? An infrastructure and operations analysis. Cambridge: Forrester.

Zhou, Rong, and Baizhi Xie. 2010. The educational technology centre: A window to view the progress of Chinese ICT-based higher education. *British Journal of Educational Technology* 41, no. 4: 642-659.

Figures

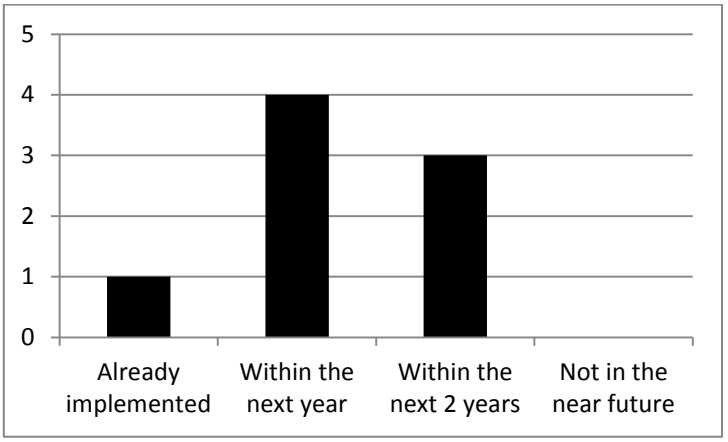


Figure 1: Cloud-based email adoption in South African higher education institutions in 2009

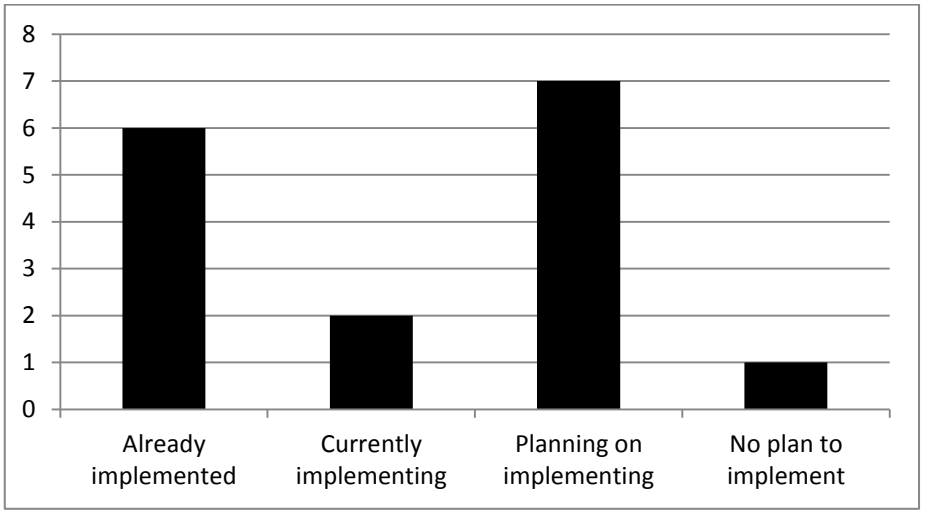


Figure 2: Cloud-based email adoption in South African higher education institutions in 2012

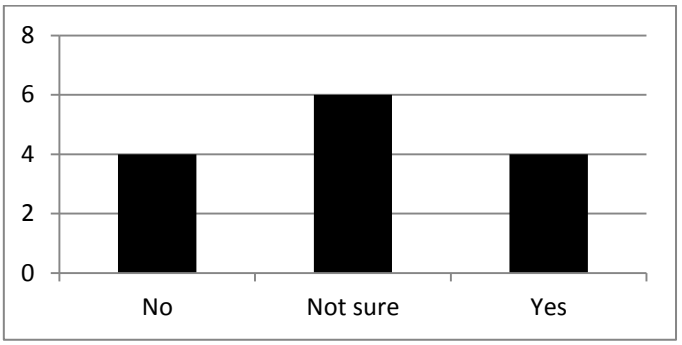


Figure 3: Cloud-based email adoption for staff in South African higher education institutions

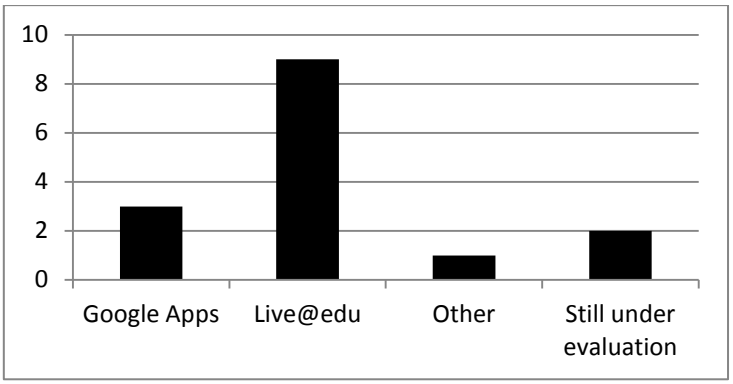


Figure 4: Cloud-based email providers preferred by South African Higher education institutions

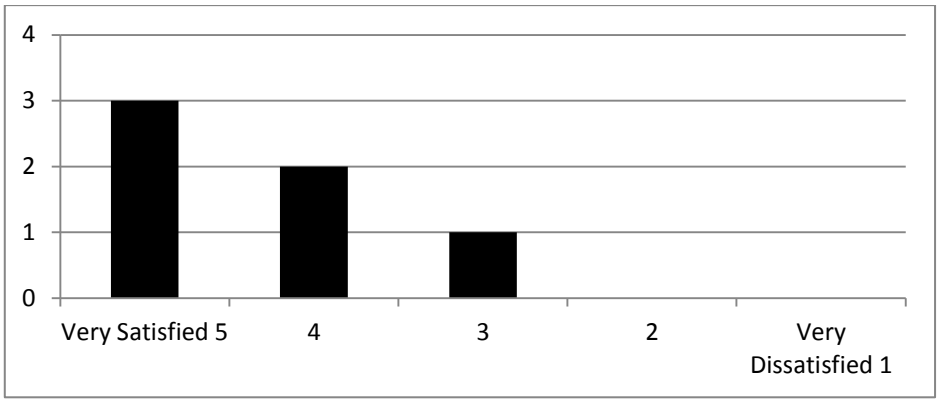


Figure 5: Satisfaction with cloud-based email in South African higher education institutions

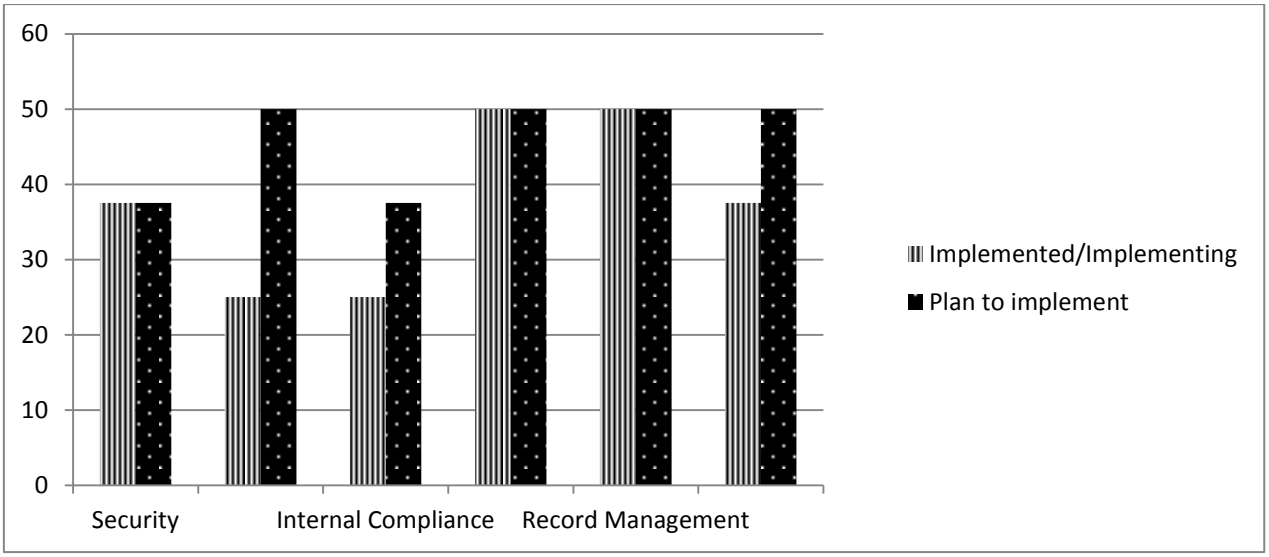


Figure 6: Concerns regarding cloud-based email in South African higher education institutions

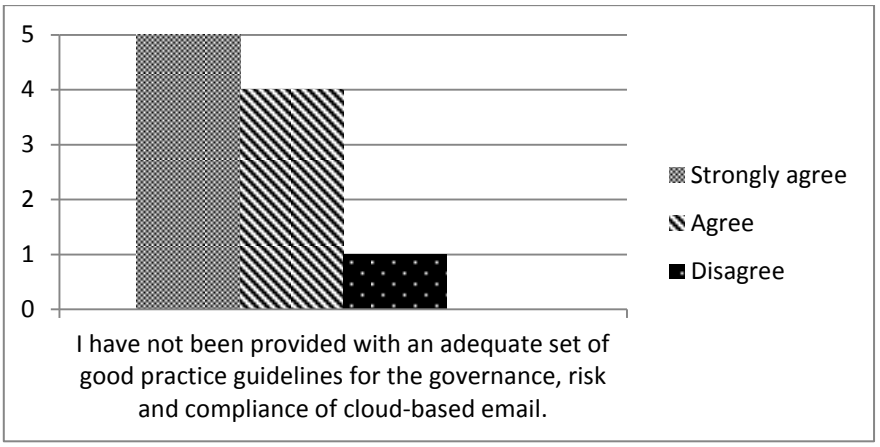


Figure 7: Need for cloud-based email guidelines

Tables

Comments regarding cloud-based email for staff at higher education institutions

- Staff email should stay on premise allowing you to implement the stricter compliance controls needed. Staff have become accustomed to the email performance received over a LAN connection. Experience over a higher latency and more restricted bandwidth will be a major problem.
- The issues could be that of low speed connections and privacy issues. Some institutions could be adamant to hand over control of email to the 3rd party.
- Concerns about backups/archiving.
- Still a new concept. Give it 18 months. Concerns about bandwidth.
- I think it is a question of confidence. I am not worried.
- Concerns are legitimate. Concerned about data security and IP management.
- Need management buy in.
- Security, legislation, reliability and integration are key issues.
- Concerns regarding security of information, control of intellectual property, high availability and backup/restore.
- There are still some challenges such as legal requirements.
- We are approaching this by building confidence in related cloud services (calendaring, docs) first.
- This is dependent on the university bandwidth and ability for the ICT department to deliver an efficient, seamless service.
- The dependence on bandwidth is a concern; we would not want to compromise quality of service to our campus community.

• I would like a "mail for life" service. If the domain reflects the institutions name, it complicates staff mail.

Table 1: Comments regarding cloud-based email for staff

Concerns regarding cloud-based email at South African higher education institutions
• Standard email address formats and display details. Address the risk of institutional reputation damage if user behaviour is non-conformist to policy.
• Vendor lock-in. What happens if you want your email/data back? Will the vendor transfer the data/information to another vendor?
• Privacy issues. Compliance - how are you going to handle this? Content of the contractual agreement.
• Availability is the major concern - need to improve internet access availability first.
• Location of servers/data centers with relation to e.g. Patriot act; Institutional readiness/culture.
• Be aware that international bandwidth will be used. Asaudit must lobby that both providers (live@edu & Google) should allow/plan a local staging/ proxy so that university connections are to local bandwidth.
• Governance standards, DRP, standard operating (user) guidelines, storage & retrieval, privacy, State regulatory compliance.

Table 2: Comments regarding concerns about cloud-based email

Appendix B4

Towards Cloud Computing Assurance

Author to correspond with:

Name: Rossouw von Solms

Address: School of ICT, Nelson Mandela Metropolitan University,

PO Box 77000,

Port Elizabeth 6031,

Republic of South Africa

Email: Rossouw.VonSolms@nmmu.ac.za

Telephone: 041 504 3604

Author:

Melanie Willett

Towards Cloud Computing Assurance

ABSTRACT

In organisations, the board and executive management are tasked with ensuring proper governance. This governance responsibility includes the tasks of 1) recognising and reacting to opportunities that could benefit the organisation, and 2) ensuring that this is done in a manner which they are reasonably confident is efficient, manages risks effectively and is compliant with related regulations and legislation. All of these should in the end contribute to a sense of assurance. Assurance is understood to be a part of corporate governance and provides stakeholders with confidence in a subject matter by evaluating evidence about that subject matter. Evidence will include proof that proper controls and structures are in place, that risks are managed and that compliance with internal and external requirements is demonstrated with regard to the subject matter. Decisions regarding the use of cloud computing in organisations bring these responsibilities to the fore.

Cloud computing is a computing paradigm that is associated with opportunities which could greatly benefit organisations if they can be adopted and implemented in a manner that gives stakeholders confidence that this is being done efficiently and in a manner that manages risks and is complaint. Simply put, organisations could benefit from some form of assurance when utilising cloud computing in any possible form. Standards and reputable guidelines for cloud computing adoption and use can also assist with cloud computing assurance. This paper has the threefold aim of 1) highlighting the responsibility of managers to ensure assurance when exploiting opportunities presented by IT advances, such as cloud computing; 2) serving to inform management about the advances that have and are being made in the field of cloud computing guidelines; and 3) motivating that these guidelines be used for assurance on behalf of organisations adopting and using cloud computing.

Keywords: cloud computing assurance, cloud computing guidelines, cloud computing standards, cloud computing compliance, cloud computing decisions making, cloud computing value, board IT responsibilities

INTRODUCTION

In organisations, the governance responsibilities entrusted to the board and the executive management include the tasks of both recognising and reacting to beneficial opportunities, as well as doing so in a manner that they are reasonably confident is efficient, manages risks effectively and is compliant with related regulations and legislation. The field of cloud computing illustrates and accentuates this responsibility.

This paper will:

1) Highlight managers' responsibility to ensure assurance when exploiting opportunities presented by IT advances such as cloud computing. Cloud computing is a computing paradigm which many believe will have a marked impact on organisations, as it is a field with the potential to make further strategic opportunities available to organisations. There are, however, also significant risks associated with the use of cloud computing. A computing paradigm of this nature, with the potential to have a positive impact on the operation of organisations, should be of interest to managers at all organisational levels. It is a field that highlights management's duty to balance the responsibilities of recognising and reacting to opportunities that could benefit the organisation with doing so in a manner that provides adequate levels of associated assurance.

2) Inform management about the advances that have and are being made in cloud computing

guidelines. For many years, such standards and best practice guidelines have been of value to many organisations in ensuring proper governance of the various facets of IT. In the past, the lack of standards and guidelines in the relatively new field of cloud computing was widely bemoaned. There is now, however, a plethora of cloud computing standards and guidelines available and new ones are being produced and refined. Many of these are technical in nature and not necessarily of direct interest to directors and non-IT management. Sifting through what is relevant in the form of high-level guidance for cloud computing may also prove to be a tedious task. This paper will present an overview of the guidance given on cloud computing by reputable IT governance bodies, as well as other bodies which are making a contribution to the area of cloud computing standards and guidelines. This overview will provide managers with a good indication of the high-level controls that best-practice guidelines recommend be put in place for the effective utilisation of cloud computing in an organisation. This knowledge may be helpful in carrying out governance responsibilities.

3) Support the call for organisations adopting and using cloud computing to use these guidelines for assurance purposes. In order for organisations to use cloud computing with confidence, managers need to be assured that they can do so in a manner that is effective and compliant, and that risks are properly managed. Assurance is therefore a vital element of the successful utilisation of cloud computing. Accordingly, standards and best-practice guidelines can, and should, play an important role in providing requisite levels of assurance.

This paper will thus examine some cloud computing guidelines from an assurance perspective. Assurance is a critical component of governance as it involves having the required controls and mechanisms in place to make cloud computing work effectively; hence, ensuring risk management and compliance. The recommendations of existing guidelines for risk management and compliance will be analysed and discussed. Subsequently, one way in which existing guidelines can be used to contribute to the comprehensive assurance of effective cloud computing will be concluded.

Firstly, the governance responsibilities of the board and executive management are discussed.

ASSURANCE AS A GOVERNANCE RESPONSIBILITY

A previous paper by the authors analysed some of the specific responsibilities that the board has with regard to IT governance, as espoused by *The King Report on Corporate Governance for South Africa 2009* (IoDSA, 2009), the *Board Briefing on IT Governance* (ITGI, 2003) and the ISO38500:2008 standard for *Corporate governance of information technology*. The following governance responsibility for the board was concluded: "*the board is responsible for ensuring that opportunities presented by developments in IT are recognized and exploited in a manner that adds value to an organization and is secure and compliant with regulations, policies, standards and best practice guidelines"* (Von Solms & Viljoen, Cloud computing service value: A message to the board, 2012, pp. 73,74). The aforementioned paper highlighted this responsibility and focused primarily on the aspect of this governance responsibility that ensures using cloud computing in a manner which adds *value*. That being so, this paper focuses on the

further facets of that governance responsibility – ensuring *assurance*.

According to the Business Dictionary.com, assurance is defined as the "part of corporate governance in which management provides accurate and current information to the stakeholders about the efficiency and effectiveness of its policies and operations, and the status of its compliance with the statutory regulations." ISACA similarly defines assurance as an "objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the organization" (2011). Assurance is also closely linked to confidence and trust. The international framework for assurance engagements describes an assurance engagement as "engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria" (International Auditing and Assurance Standards Board, 2004).

Figure 1 illustrates the relationship between assurance, governance, confidence and compliance as described above. As can be seen in this figure assurance is mandated by means of sound governance. Moreover, assurance is accomplished by analysing criteria and evidence about subject matter. The criteria are determined based on the subject matter but are usually influenced by laws and regulations, policies and standards and best practice guidelines relating to the subject matter. The evidence of conformance with these criteria can also come in various forms depending on the subject matter under consideration, but usually includes a set of controls and processes that ensure compliance and risk management. The outcome of the assurance process assists in promoting trust and confidence in the use of the subject matter. Done properly the process of ensuring that organisations can provide appropriate evidence that they are meeting the criteria for certain subject matter also assists management in demonstrating due diligence. The importance of assurance, as a core component of sound IT governance, is therefore clear.

Figure 1 *Concept diagram for relationship between assurance and governance* goes here.

A Subject matter which is likely to impact many organisations internationally, and for which assurance is therefore vital, pertains to cloud computing. The next section briefly introduces cloud computing and highlights the importance of management awareness of this computing paradigm and where it can possibly add value to the organisation.

CLOUD COMPUTING

A comprehensive definition of cloud computing will not be discussed in this paper. References to detailed explanations of cloud computing are given later in the work. Simply put, cloud computing is a computing paradigm which allows one to access an IT service over a network as or when it is needed, leaving the responsibility of properly provisioning this service in the hands of the cloud service provider (CSP).

Cloud computing is a term which has been generating a lot of interest in recent years. Figure 2 shows how searches on Google for the term "cloud computing" have gradually been on the rise since 2007. It is also interesting to note that since 2010 there have been more searches for "cloud computing" than for "information security," "mobile computing," or even "Barak

Obama". Not only is cloud computing a term that people are interested in, but organisations around the world are adopting various services provisioned by cloud computing. Several surveys indicate that the majority of organisations surveyed are currently adopting or planning to adopt cloud computing in the future.

Figure 2 *Cloud computing search terms on Google Trend* goes here.

Not only are individual organisations using cloud computing but government initiatives are also promoting its use. The American government has adopted a "cloud first policy", encouraging agencies to assess whether they can make use of the benefits of cloud computing before looking for other potential solutions (Kundra, 2011). Furthermore, Europe is driving the use of cloud computing by government agencies and includes plans to do so in the "Digital Agenda for Europe" (European Commission, 2012).

As stated earlier, both the board and the IT managers of an organisation have the responsibility of recognising and acting on opportunities presented by new developments in IT, such as cloud computing (Von Solms & Viljoen, Cloud computing service value: A message to the board, 2012). Cloud computing is already, and is likely to continue, having an impact on the environment in which organisations operate. As it is associated with numerous potential business benefits, it is a computing paradigm that organisations cannot afford to ignore.

It is not, however, always appropriate for organisations to adopt cloud computing solutions. Indeed, cloud computing is associated with several noteworthy risks. In addition, organisations will not always necessarily achieve the business benefits hoped for from adopting cloud computing services.

So, although cloud computing is associated with many potential business benefits and should not be ignored by organisations, its use might not always be an appropriate solution. Organisations should therefore ensure that they only utilise cloud computing in a manner that is efficient, effective, secure and compliant and that adds value to the organisation. In view of this, organisations should be assured that a service provisioned by cloud computing is indeed the best for them under the specific set of circumstances. It is for this reason that it is important for organisations to have a mechanism in place for ensuring cloud computing assurance, since failure to do so could constitute a governance oversight.

The previous section highlighted the core relationships concerning assurance. The fact that standards and best practice guidelines play a role in the assurance process was highlighted. The following section elaborates on the importance of applying reputable guidelines effectively when introducing cloud computing.

VALUE OF STANDARDS AND GUIDELINES

Standards and best practice play an important role in assurance. As was noted earlier, standards and best practice guidelines are an important element from which the criteria for an assurance engagement are derived. By using these standards and best practice guidelines to derive assurance criteria the assurance process can assist in demonstrating due diligence. Due diligence is defined as "reasonable steps taken by a person to avoid committing a tort or offence" (OECD, 2004). As explained in the OECD principles for governance, a person can show due diligence by

demonstrating that they have behaved in a way that "a reasonably prudent person would exercise in similar circumstances" (OECD, 2004). Following a set of reputable guidelines formulated by a group of experts properly gives directors and managers the ability to possibly argue for due diligence. A standards-based, best-practice approach to the governance of IT is, therefore, a wise course to follow.

Not only do standards and best practice guidelines help define criteria for assurance but they also make it clear what systems and controls an organisation should have in place to use as evidence in the assurance process. As with IT in general, in the relatively new field of cloud computing, standards and reputable guidelines can alert management to its responsibilities. Moreover, they provide management with guidance on understanding cloud computing and its implications for organisations, as well as its responsibilities regarding cloud computing. In addition, standards and best practice guidelines assist in the process of deciding about the efficient adoption and implementation of cloud computing solutions and they could also assist in identifying risks and the controls and systems for managing such risks.

Standards and guidelines for cloud computing therefore clearly add value to organisations. There are, however, a plethora of cloud computing standards and guidelines available. The next section elaborates on these and describes some reputable guidance available for cloud computing.

CLOUD COMPUTING GUIDELINES

As discussed in the previous section, guidelines for cloud computing can assist managers with the task of deciding how to proceed confidently with cloud computing in their organisation. The sheer volume of guidance becoming available for cloud computing may make the task of finding and selecting guidelines for the adoption and implementation of cloud computing more complicated than it is. This section aims to highlight how many different types of cloud computing standards and guidelines are available and will then list some of the more applicable and reputable guidelines.

There are numerous cloud computing standards and guidelines available and under development. There are also numerous bodies working on these standards and guidelines, including government bodies, standards organisations and academics. NIST hosts a wiki which describes work on cloud computing standards and lists about fourteen bodies. In addition to these bodies, academia, industry and government bodies are also involved in research on cloud computing standards and guidelines. A Google search for "cloud computing guidelines" on 25 January 2013 resulted in about 83 300 results in 0.22 seconds. A similar search for the phrase "cloud computing standards" resulted in 437 000 results and a search for "cloud computing framework" resulted in about 540 000 results. This clearly indicates that there are numerous parties actively working on standards and guidelines in this area of study.

What is available?

There are various types of cloud computing guidelines available. These guidelines range from very specific to very general, from very technical to very conceptual. For the purpose of this discussion, however, guidelines can be broadly categorised into two types, which are termed prescriptive and evaluative standards by Borenstein and Blake (2011). These authors describe prescriptive standards as those which

give exhaustive details about how things work. Standards describing SMTP and TCP are examples of prescriptive standards. Evaluative standards, on the other hand, provide a uniform manner of assessing how well something works. An example of an evaluative standard is ISO 27000. For the purpose of this paper, some evaluative cloud computing guidelines will be focused on.

As stated previously, there are various bodies (stemming from academia, industry and governmental bodies) involved in producing guidelines for cloud computing. This paper does not attempt to review the work on cloud computing by all of these bodies, nor does it attempt to provide an exhaustive list of cloud computing standards and guidelines that may be relevant to directors and management. It merely discusses some of the more influential work on cloud computing that has been done by some reputable IT governance and cloud computing bodies.

What will be considered?

Various IT governance bodies have produced guidelines that have been used successfully for a number of years by organisations internationally. They have, therefore, become *reputable* and *trustworthy* advisors in the field of IT and it would be wise to monitor any work that these bodies are involved in; in this case with cloud computing specifically. Cloud computing guidelines from bodies that provide reputable IT governance guidance can also easily be *used in conjunction with the existing guidelines for IT governance* that many organisations may already be using. In addition, guidelines from reputable IT governance bodies are *relevant* to the board and executive management, as they are *not overly technical or technology or vendor specific*. In addition, guidelines from these bodies are *most likely to be adopted* by organisations within the environment in which general organisations operate. Adherence to guidelines from these bodies may even be a mandate for your organisation. Finally, as explained earlier, adherence to guidelines from such reputable bodies assists you in demonstrating *due diligence* to some extent.

The value of considering the work on cloud computing by reputable bodies involved in the promotion of IT governance guidelines and frameworks is therefore apparent. There are a number of reputable bodies involved in such work and these include the bodies listed below. This list is by no means complete or in order of importance.

- ISACA – ISACA provides guidance for IT governance, information security and IT audit and assurance. It has developed well-known governance frameworks such as COBIT and Val IT (ISACA, n.d.).
- ISO – International Organization for Standardization. ISO develops voluntary international standards through global consensus (ISO, n.d.).
- NIST – National Institute of Standards and Technology. NIST is a federal agency within the United States of America's Department of Commerce. It encourages the use of standards and technology to promote the industrial competitiveness of the USA (NIST, 2012b).
- COSO – Committee of Sponsoring Organizations of the Treadway Commission. COSO develops "frameworks and guidance on enterprise risk management, internal control and fraud deterrence" (COSO, n.d.).

The guidelines of these bodies refer to guidance from, among others, the following bodies: CSA, ENISA, CIO Council and Commission of the European Communities, Expert Group on Cloud Computing. Some guidance from all of the above

mentioned bodies will be highlighted in the next section.

SYNOPSIS OF GUIDANCE

As described previously, this section will highlight the guidance that is available in some existing cloud computing standards and guidelines. A summary of the guidelines of the various bodies is given in Tables 1 and 2.

The guidance will be discussed from an assurance perspective. It has been previously highlighted that assurance is part of governance and involves the important facets of ensuring risk management and compliance. Since assurance is part of governance and many of the controls that affect cloud computing (such as policies, organisational structures and others) are mandated by governance, general guidance regarding the governance of cloud computing will be highlighted.

Since cloud computing may be a relatively new term for some organisations, it may be more intuitive to start a synopsis of existing guidelines with a discussion about guidance aimed at promoting an understanding of cloud computing. This will be highlighted in the next section and will be followed by a discussion related to guidance on making decisions regarding the selection and adoption of cloud computing solutions. There are significant overlaps between guidance on the selection of cloud computing solutions and the components of assurance.

Understanding Cloud Computing

Since cloud computing is a relatively new field in IT, it is not surprising that a good deal of the information disseminated by these bodies serves to clarify what cloud computing is and the potential benefits and risks that are associated with it.

NIST is arguably the one body that has done the most to promote a clearer understanding of cloud computing. It provides the most widely referenced ***definition*** for cloud computing (NIST, 2011d). In addition, NIST enables a better understanding and discussion on cloud computing by making available a cloud computing ***taxonomy*** and a ***reference architecture*** for cloud computing (NIST, 2011b). The reference architecture describes the various components, roles and actors in cloud computing and how they relate. The CSA also provides an ***architectural framework*** (CSA, 2009).

To further understanding of and discussion on cloud computing NIST provides several ***case studies*** (NIST, 2011c). These enable the examination of various possible applications of cloud computing and make the wide array of cloud computing solutions which are available to organisations more apparent.

As with any new technology, before being able to manage it properly organisations should not only understand what it is and how it works, but also how they can benefit from it and the risks that are associated with it. To this end, a large share of the guidance provided by the IT governance bodies discussed in the previous section has been dedicated to educating potential cloud computing users on the ***opportunities and risks*** associated with cloud computing. NIST (NIST, 2011a; NIST 2011e), ISACA (ISACA, 2012c), COSO (Horwath, 2012) and the CIO Forum (Kundra, 2011) have all produced work explaining what opportunities and risks are associated with cloud computing and why.

Once organisations understand what cloud computing is, how it can be used and what opportunities and risks are associated with it, they can embark on the process of deciding about the adoption of cloud computing. This is a second general area in which cloud computing guidance is given. The following subsection summarises the guidance given with regard to the selection and adoption of cloud computing.

Selecting Cloud Computing Solutions

Although significant opportunities have been attributed to the use of cloud computing in general, each organisation has a responsibility to investigate whether the adoption of a cloud computing solution would be appropriate for its specific circumstances and requirements.

A number of the cloud computing guidelines researched in this work include processes and models to assist managers of organisations to make decisions regarding the adoption of cloud computing. The CSA provides a quick ***method for evaluating the tolerance*** of organisations' cloud computing solutions for organisational assets (CSA, 2009). ENISA also provides a ***model for choosing resilient and secure*** cloud computing solutions (Cattedu, 2011). In addition, ISACA describes a ***four-step process*** to assist with making a decision about the use of cloud computing (ISACA, 2012c). This process includes some of the recommendations highlighted in other guidelines and will be described in more detail in the following few paragraphs.

The four-step approach to decision making relating to the adoption of cloud computing, as highlighted by ENISA, is as follows:

1. Preparation of the internal environment
   It is recommended that an organisation assess how a move to the cloud would affect and be affected by, among other things, existing organisational principles, policies and frameworks; processes; organisational structures; culture, ethics and behaviour and people skills and competencies. A consideration of the costs and benefits of moving to the cloud is also recommended.

Various other guidelines may assist managers to weigh up the costs and benefits of cloud computing adoption. For example, ISACA also provides assistance for making a decision regarding the potential value of a cloud computing solution in the form of a framework for calculating the return on investment (ROI) of cloud computing (ISACA, 2012a). This shows why it is difficult to calculate ROI with cloud computing and lists and explains the tangible and intangible costs and benefits of cloud computing. In addition, it provides a framework which outlines guidelines for various phases that assist managers to calculate ROI. Figure 4 shows the ***ROI framework for cloud computing***.

Figure 4 goes here.

2. Selection of a cloud service model
   A decision tree is presented that can help managers to decide which service model (SaaS, PaaS or Iaas), if any, would suit their organisation best.
3. Selection of the cloud deployment model
   Provides a decision tree to assist in deciding whether a public or private cloud would best meet requirements or whether the

organisation would be better off not using a cloud computing solution at all.

4. Selection of the cloud provider (CSP)
   It is recommended that well-established, trusted CSPs be considered and that the location of the CSP be taken into account as this may be governed by certain laws that will affect the decision. The standards and business needs should also match the service provided by the CSP.

The guidance referred to thus far will assist managers in understanding cloud computing and selecting an appropriate cloud computing solution for their organisation. NIST refers to and elaborates on a decision framework that goes beyond the selection of a solution by touching on aspects of provisioning and managing a cloud computing solution. This high-level framework, originally described by the CIO Forum, includes steps for selecting, provisioning and managing cloud computing services (NIST, 2011c; Kundra, 2011). The three steps in the decision framework for cloud migration are mapped to areas that are described by NIST as priority areas of interest for cloud computing. From this map, NIST has determined a number of considerations in each of the steps given in the decision framework. In addition to these considerations, NIST also provides a set of case studies which relates to the steps in the framework.

This section has highlighted some guidance provided by reputable bodies on making decisions about the adoption of a cloud computing solution. The previous section highlighted various sources that thoroughly explain cloud computing. The next two sections now highlight the more overarching topics of governance and assurance in cloud computing.

Governance and Assurance in Cloud Computing

Governance is defined by ISACA as "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved and ascertaining that risks are managed appropriately" (ISACA, 2011). ISACA states that the two key objectives of IT governance ensure that IT is used in such a way that it adds *value* to the business and that IT-related *risks* are properly managed. This section will highlight various guidelines regarding enterprise governance of the cloud. The previous section has highlighted several guidelines and models that organisations can use to ensure that they select cloud computing solutions that add value. This section, therefore, focuses primarily on the second main objective of IT governance for cloud computing – risk management. Firstly though, more general governance guidelines for cloud computing are described.

General governance guidelines

Cloud computing must be governed within the context of an enterprise IT governance programme using standards and best practice guidelines.

Many of the bodies considered here are responsible for producing IT governance frameworks, and recommending and describing how existing IT governance frameworks can be tailored and applied to cloud computing. ISACA describes how ***COBIT 4.1 can be applied to cloud computing*** (ISACA, 2011). Likewise, COSO recommends that the ***COSO ERM framework*** be used when dealing with cloud computing (Horwath, 2012).

ISO is also developing standards based on ISO/IEC 27002 specifically for cloud computing. These will be ***ISO/IEC 27017*** (ISO, 2012b) and ***ISO/IEC 27018*** (ISO, 2012a). The CSA also explains a "***Trusted Cloud Initiative Reference Architecture***" which is based on various best practice frameworks for IT (CSA, 2011c). The CSA defines the architecture as "both a methodology and a set of tools that enable security architects, enterprise architects, and risk management professionals to leverage a common set of solutions" (CSA, 2011b). The framework is based on standards from SABSA, ITIL, TOGAF and the Jericho Forum.

To ensure that cloud computing is properly governed *roles and responsibilities should be assigned to different levels of management.*

In the definition for governance given previously, the importance of this requirement is highlighted. If governance is, in part, "the set of responsibilities and practices exercised by the board and executive management" it is clear that for the proper governance of cloud computing, these managers will need to be aware of their responsibilities. COSO provides a ***list of the responsibilities*** of various managers such as the board of directors, the chief executive officer, the chief financial officer, the chief legal officer, the chief information officer and the chief internal auditor (Horwath, 2012). COSO also provides ***a list of questions which the board of directors and managers should consider*** regarding cloud computing.

Organisations should establish business goals and business cases for cloud computing.

ISACA provides a ***set of steps that organisations can use to determine their cloud computing business goals*** (ISACA, 2011).

Risk Management Guidelines

A system should be in place to ensure that the enterprise risks introduced by cloud computing are managed.

Cloud computing introduces a multitude of new opportunities and risks. All of the bodies considered in this work describe the opportunities and risks associated with cloud computing and emphasise the need to address such risks.

Much of the work described in the section on the selection of cloud computing solutions refers to various means of analysing risks. The decision framework mentioned earlier, provided by ENISA, shows how a **SWOT analysis** can be used in the evaluation. CSA outlines a "**simple framework** to help evaluate initial cloud risks" (CSA, 2009). However, ENISA also explains a more complete, **standards-based risk assessment process** that organisations can use (ENISA, 2009a). This process categorises several common cloud computing risks according to probability and impact and how the risk compares with the risks associated with more traditional solutions.

Once a risk assessment has been conducted, organisations need to decide on a risk response for cloud computing (as described in the process outlined in COSO's ERM framework). Once again, the bodies considered in this work have produced an abundance of guidelines and recommendations for the ways in which various cloud computing risks should be addressed. The CSA provides a document containing recommendations for dealing with cloud computing risks in thirteen different domains (CSA, 2009). NIST, on the other hand, provides a description of various risks and makes certain recommendations (NIST, 2011a; NIST, 2011e).

ENISA (ENISA, 2009a) and the Commission of the European Communities Expert Group on Cloud Computing also provides guidance on risk mitigation, especially relating to contracts and legal risks.

Compliance guidelines

This section discusses guidelines to assist in demonstrating compliance with cloud computing. The guidance considered in this work with regard to cloud computing deals largely with ensuring compliance through the use of contracts.

ENISA gives a **list of areas to pay attention** to when assessing agreements in various forms (e.g. SLAs, ToUs) with CSPs (ENISA, 2009). ENISA also provides extensive guidance on cloud computing contracts. This guidance includes a **checklist** that organisations can go through to assess and evaluate cloud computing contracts with CSPs (ENISA, 2011). The guidelines focus primarily on the security (such as availability, incident response and data lifecycle management) of these contracts from a customer perspective. The CIO Council also gives **guidelines and a checklist** of questions that organisations can apply when dealing with SLAs, CSPs and end-user agreements (CIO Council, Chief Acquisition Officers Council, 2012).

Further, ENISA provides a **methodology for legal analysis** regarding the use of cloud computing (Cattedu, 2011). This methodology includes three steps which can help organisations identify the legal risks related to the use of cloud computing, as well as a list of six fundamental questions relating to organisations' use of cloud computing aids when conducting this analysis. The methodology is applied to scenarios within the EU.

Controls for cloud computing

ISACA defines a control as "[t]he means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of an administrative, technical, management or legal nature. Also used as a synonym for safeguard or countermeasure" (ISACA, 2012b).

Some of the guidelines listed above have already highlighted controls that organisations should use for cloud computing. In fact the guidelines themselves are controls. A discussion about controls may therefore seem arbitrary here. Nevertheless, it is worth noting that ISACA has **mapped control objectives from COBIT 4.1 for cloud computing** (ISACA, 2011). Further, the CSA has released a **matrix of control objectives** which refers to controls that may be relevant to cloud computing from various other standards and guidelines, such as HIPAA, ISO/IEC 27001-2005, NIST SP800-53 R3, FedRAMP Security Controls, PCI DSS v2.0 and others (CSA, 2012). It is also worth mentioning that ENISA has produced an **assurance framework** for cloud computing (ENISA, 2009b). This provides a list of questions that organisations can ask concerning cloud computing and that can help them in the assurance process.

This section has highlighted various aspects that best-practice guidelines recommend should be considered by organisations interested in using cloud computing. The brief consideration given here may help managers to be aware their governance responsibilities with regard to cloud computing. The discussion has highlighted guidance that managers can refer to in order to help them understand what cloud computing is, what the associated benefits and risks are, how to go about making a decision about the adoption of

cloud computing and how to address some of the aspects of ensuring assurance with cloud computing by managing risk, putting controls in place and ensuring compliance.

When using cloud computing, providing assurance is an important responsibility which has not, however, been fully addressed by the guidelines considered thus far. The following section discusses this problem in more detail.

CLOUD COMPUTING ASSURANCE

The discussion thus far has highlighted what assurance is and how existing guidance from reputable bodies addresses various components of assurance for cloud computing. According to ISACA, however, there is no single framework that can be used for cloud computing assurance (ISACA, 2011). This section will highlight some of the shortcomings of possible assurance measures for cloud computing, as well as a process that organisations can use for assurance purposes.

ISACA lists various common frameworks that can be used by CSPs for assurance and highlights the shortcomings of each (ISACA, 2011). Many of these have been referred to in this work, with the CSA cloud control matrix being one. In addition, ENISA provides an ***assurance framework*** which has also been referred to in this work (ENISA, 2009b). One shortcoming of this framework, as described by ISACA, is that it is limited to the risks associated with cloud computing.

As explained earlier and highlighted in Figure 1, a set of *criteria* for specific subject matter based partly on best-practice guidelines is a vital component of an assurance engagement. Criteria for assurance can differ in terms of scope-based factors, such as the type of organisation (CSP or cloud user) and the level at which assurance is being provided. Assurance can also be provided for different functionalities (ISACA, 2011). A process that organisations can use to develop a set of best practice-based criteria for cloud computing assurance which suits their specific needs could therefore be valuable.

ISACA recommends that CSPs use a unified IT compliance approach for cloud computing assurance (ISACA, 2011). ISACA gives a list of the various components of a unified IT compliance approach and gives the activities CSPs should perform with regard to each component. The business functions listed as being essential for unified IT compliance are governance, risk management, compliance, continuous improvement and unified control processes. This list is similar to the guidelines that have been reviewed in this paper for cloud computing users.

It can be argued that since guidance provided by prominent IT governance bodies recommends that the components of unified IT compliance be addressed by cloud computing users, they, like CSPs, would benefit from an assurance process based on a unified IT compliance programme. Although not a complete set of guidelines, Table 3 illustrates how organisations could use the process of mapping cloud computing guidelines from reputable bodies to the components of a unified IT compliance approach in order to customise a best practice-based assurance process for cloud computing. Policies, regulations and other factors should also be considered when using this approach to determining criteria for a cloud computing assurance engagement. Following an approach such as the one outlined above provides a basis that can be used in

assurance engagements to promote confidence and trust in the functioning of cloud computing in organisations. Some important aspects of assurance, as depicted in Figure 1, have been discussed in this paper. Further, the relationship between assurance and governance responsibilities for cloud computing has been highlighted. It has been argued that the process for mapping requirements for cloud computing outlined in best practice guidelines and other sources (such as policies and regulations) to the components of a unified IT compliance approach can be used by organisations to determine an appropriate set of criteria which can be evidence about cloud computing can be consistently evaluated. The use of this approach can help to make management feel confident that cloud computing is being used efficiently, effectively, and compliantly. This best practice-based approach to cloud computing assurance can also assist managers in demonstrating due diligence.

CONCLUSION

Cloud computing presents significant opportunities and risks that organisations need to be aware of. To be able to adopt and use cloud computing with confidence, organisations require assurance that they can do so in a manner that is efficient, addresses risk appropriately and demonstrates compliance. Managers have the responsibility to ensure that this takes place. Moreover, standards and guidelines play a valuable role in assurance. There are many new guidelines for cloud computing and this paper has highlighted some that have emanated from reputable bodies which could be of benefit for organisations considering cloud computing adoption. In addition, it has presented executive managers with an overview of some of the guidelines available which may assist them in their responsibility of ensuring that cloud computing is used appropriately in their organisations. There are, however, currently no known assurance frameworks for cloud computing which will address all the organisation's assurance requirements. This paper has further highlighted how organisations can adopt a process in terms of which existing cloud computing guidelines are mapped onto the components of a unified IT compliance programme in order to customise a comprehensive cloud computing assurance approach for their organisations.

REFERENCES

Assurance, n.d. *Business Dictionary.* [Online] Available at: http://www.businessdictionary.com/definition/assurance.html

Borenstein, N. N. & Blake, J. J., 2011. Cloud computing standards: Where's the beef?. *IEEE Internet Computing,* 15(3), pp. 74-78.

Cattedu, D., 2011. *Security and Resilience in Governmental Clouds.* [Online] Available at: http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

CIO Council, Chief Acquisition Officers Council, 2012. *Creating Effective Cloud Computing Contracts for the Federal Government. Best Practices for Acquiring IT as a Service..* [Online] Available at: https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

COSO, n.d. *Welcome to COSO.* [Online] Available at: http://www.coso.org/ [Accessed 21 January 2013].

CSA, 2009. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.* [Online]
[Accessed 25 January 2010].

CSA, 2011a. *Quick guide to the reference architecture.* [Online]
Available at:
https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI_Whitepaper.pdf

CSA, 2011b. *Security guidance for critical areas of mobile computing version 3.* [Online]
Available at:
https://cloudsecurityalliance.org/research/security-guidance/#_overview
[Accessed 13 January 2013].

CSA, 2011c. *Trusted Cloud reference architecture.* [Online]
Available at:
https://cloudsecurityalliance.org/research/tci/

CSA, 2012. *Cloud Control Matrix.* [Online]
Available at:
https://cloudsecurityalliance.org/research/ccm/

ENISA, 2009a. *Cloud Computing Information Assurance Framework.* [Online]
Available at: http://www.enisa.europa.eu/
[Accessed 22 February 2010].

ENISA, 2009b. *Cloud computing: benefits, risks and recommendations for information security.* [Online]
Available at:
http://www.ifap.ru/library/book451.pdf
[Accessed 10 June 2010].

ENISA, 2011. *Procure Secure. A guide to monitoring of security service levels in cloud contracts.* [Online]
Available at:
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

European Commission, 2012. *A roadmap for advanced cloud technologies under H2020.* [Online]
Available at:
http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-expert-group/roadmap-dec2012-vfinal.pdf
[Accessed 3 January 2013].

Horwath, C., Chan, W., Leung, E. & Pili, H., 2012. *Eneterprise Risk Manage for Cloud Computing.* [Online]
Available at: http://www.coso.org/-erm.htm
[Accessed 13 January 2013].

International Auditing and Assurance Standards Board, 2004. *International framework for assurance engagements.* [Online]
Available at:
http://www.ifac.org/sites/default/files/downloads/b003-2010-iaasb-handbook-framework.pdf

IoDSA, 2009. *The King report on corporate governance for South Africa (The Institute of Directors in Southern Africa) September 2009,* South Africa: Institute of Directors in Southern Africa.

ISACA, 2009. *Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives,* Rolling Meadows: ISACA.

ISACA, 2011. *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud.* Rolling Meadows(IL): ISACA.

ISACA, 2012a. *Calculating Cloud ROI: From the Customer Perspective.* [Online]
Available at:

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Calculating-Cloud-ROI-From-the-Customer-Perspective.aspx

ISACA, 2012b. *COBIT 5. A Buiness Framework for the Governance amd Management of Enterprise IT.* Rolling Meadows(IL): ISACA.

ISACA, 2012c. *Security Considerations for Cloud Computing.* Rolling Meadows(IL): ISACA.

ISACA & CSA, 2012. *2012 Cloud Computing Market Maturity Study Results.* [Online]
Available at:
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/2012-Cloud-Computing-Market-Maturity-Study-Results.aspx
[Accessed 13 January 2013].

ISACA, n.d. *What we offer & whom we serve.* [Online]
Available at: http://www.isaca.org/About-ISACA/What-We-Offer-Whom-We-Serve/Pages/default.aspx
[Accessed 21 January 2013].

ISO, 2008. *ISO/IEC 38500:2008 Corporate governance of information technology.* Pretoria: SABS Standards Division.

ISO, 2012a. *ISO/IEC WD 27018.* [Online]
Available at:
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498

ISO, 2012b. *ISO/IEC WD TS 27017.* [Online]
Available at:
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757

ISO, n.d. *About ISO.* [Online]
Available at:
http://www.iso.org/iso/home/about.htm
[Accessed 21 January 2013].

IT Governance Institute, 2007. *COBIT 4.1.* [Online]
Available at:
http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx
[Accessed 23 10 2010].

ITGI; PricewaterhouseCoopers LLP, 2009. *An Executive View of IT Governance.* [Online]
Available at:
http://www.isaca.org/Knowledge-Center/Research/Documents/An-Executive-View-of-IT-Gov-Research.pdf
[Accessed 02 02 2011].

ITGI, 2003. *Board Briefing on IT Governance 2nd Edition,* USA: IT Governance Institute.

Jericho Forum, 2009. *Cloud Cube Model: Selecting Cloud formations for secure collaboration.* [Online]
Available at: www.jerichoforum.org
[Accessed 22 February 2010].

Kundra, V., 2011. *Federal cloud computing strategy.* [Online]
Available at:
http://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf
[Accessed 13 January 2013].

NIST, 2009. *Cloud Computing.* [Online]
Available at:
http://csrc.nist.gov/groups/SNS/cloud-computing/
[Accessed 13 April 2010].

NIST, 2011a. *Guidelines on security and privacy in public cloud computing (NIST Special Publication 800-144).* [Online]
Available at:
http://www.nist.gov/manuscript-

publication-search.cfm?pub_id=909494
[Accessed 13 January 2013].

NIST, 2011b. *NIST Cloud Computing Reference Architecture (NIST Special Publication 500-292).* [Online]
Available at:
http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505
[Accessed 13 January 2013].

NIST, 2011c. *NIST US Government Cloud Computing Technology Roadmap Volume III (NIST Special Publication 500-293).* [Online]
Available at:
http://www.nist.gov/itl/cloud/upload/NIST_cloud_roadmap_VIII_draft_110111-v3_rbb.pdf
[Accessed 13 January 2013].

NIST, 2011d. *The NIST definition of cloud computing (NIST Special Publication 800-145).* [Online]
Available at:
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[Accessed 13 January 2013].

NIST, 2011e. *US Government Cloud Computing Technology Roadmap Volume II Release 1.0 (NIST Special Publication 500-293).* [Online]
Available at:
http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeII.pdf
[Accessed 13 January 2012].

NIST, 2012a. *Cloud Computing Synopsis and Recommendations (NIST Special Publication 800-146).* [Online]
Available at:
http://www.nist.gov/manuscript-publication-search.cfm?pub_id=911075
[Accessed 13 January 2013].

NIST, 2012b. *NIST General Information.* [Online]
Available at:
http://www.nist.gov/public_affairs/general_information.cfm
[Accessed 21 January 2013].

NIST, n.d. *Inventory of Standards Relevant to cloud computing.* [Online]
Available at:
http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory
[Accessed 13 January 2013].

OECD, 2004. *OECD Principles of Corporate Governance 2004..* France: OECD Publishing.

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

Tables

IT Governance Body	Document Name	Summary of contents
ISACA	Cloud Computing: Business benefits with security, governance and assurance perspective	A brief document which highlights some risks associated with cloud computing and suggests some strategies to meet these risks. Suggestions include using SLAs effectively, making cloud computing considerations part of the organization overall governance program and considering assurance issues related to transparency, privacy and compliance.
	Guiding principles for cloud computing adoption and use	Explains and give recommendations regarding how the principles of trust, capability, accountability, enterprise risk, cost benefit and enablement can be applied when using cloud computing.
	Calculating cloud ROI: From a customer perspective	Explains the importance of calculating the ROI for cloud computing, the challenges of doing so and guidance on how to do it.
	Security considerations for cloud computing	Describes various risks associated with cloud computing and ways to mitigate such risks with mapping to guidance from COBIT 5. A four step process is described which organizations can use to choose a viable cloud computing solutions. Decision trees for selecting a cloud service model and selecting a cloud deployment model are given. Factors that organizations have to consider after the adoption of cloud services are also given.
	IT control objectives for cloud computing	Describes how COBIT, Risk IT, Val ITTM and the Business Model for Information SecurityTM (BMISTM) can assist organizations to adopt and use cloud computing in a way that follows the principles of good governance, is secure and provides a level of assurance. The document describes how the tools listed above can be used together for governance of the cloud. It also describes various assurance frameworks for the cloud and the advantages and disadvantages of each of these. In addition it maps control objectives from COBIT 4.1 with cloud computing.
	COBIT Process Assessment Model (PAM): Using COBIT 4.1	Has a section for cloud computing. Don't have access to.
COSO	Enterprise Risk Management	COSO provides a framework that elaborates on their

	for cloud Computing	framework for enterprise risk management. In addition they provide guidance regarding the roles and responsibilities that various managers at different levels of management in the organization should fulfil regarding cloud computing. They also suggest ways that various cloud computing risks should be dealt with.
ISO	ISO/IEC WD TS 27017	Information technology -- Security techniques -- Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002
NIST	NIST Cloud Computing Standards Roadmap SP 500-291	Provides information about cloud computing architecture and use cases before discussing the need for cloud computing standards. Focusses on standards for interoperability, security and portability. Does a gap analysis to determine what cloud specific standards are needed. Mainly technical standards are identified as missing. The work does, however, identify the need for standardization of policies and processes to ensure compliance with audit, security and legal requirements. The need for standards to help organization in the assessment of cloud services before implementation is also highlighted. Cloud-based email is referred to several times in the document to illustrate the need for standardization.
	NIST Cloud computing Reference Architecture NIST SP 500-292	As the title indicates this document provides a reference architecture which details the various actors, their roles, and architectural elements which are used for cloud computing. The document also provides a cloud computing taxonomy with various cloud computing terms and definitions.
	NIST SP 500-293. US government cloud computing technology roadmap volume 1: High-Priority Requirements to Further USG Agency Cloud Computing Adoption	Volume 1 This document defines and discusses ten high-level requirements for further adoption of cloud computing.
	NIST SP 500-293. US government cloud computing technology roadmap volume 2: Useful information for cloud adopters	Volume 2 Summarizes the work covered in the NIST documents listed previously in this document. It also lists several high-level concerns related to cloud computing adoption and suggestions to mitigate each of the listed risks. References to work done to assisting in mitigating risks are given after

		each risk is discussed.
	US government cloud computing technology roadmap volume 2 (First Working Draft) Technical considerations for USG cloud computing deployment decisions	Volume 3 Although this document is still a working draft it provides guidance that IT decision makers can use when making decisions about adopting and implementing cloud computing. It discusses a "Decision Framework for Cloud Adoption" and provides a set of use cases where the decision framework is applied. The use cases have not yet been completed.
	Guidelines on Security and Privacy in Public cloud computing NIST SP 800-144	This document highlights a number of issues, risks and concerns related to the adoption of public cloud services. It also provides a set of recommendations which organizations considering the use of the public cloud can use.
	The NIST Definition of cloud computing NIST SP 800-145	Provides a widely referenced definition for cloud computing
	Draft Cloud computing synopsis and recommendations NIST SP 800-146	Provides general recommendations for organizations considering use of the cloud. Recommendations are also given for the different cloud environments (SaaS, IaaS and PaaS) and specific recommendations with regard to general terms of use for the cloud are given.
CIO Council (https://cio.gov/building-a-21st-century-government/cloud/)	Federal Cloud Computing Strategy	The American governments decision to adopt a "Cloud first policy" is explained and justified by highlighting the benefits associated with cloud computing. Risks of cloud computing are also listed in the document. A "Decision Framework for Cloud Migration" is also given.
	Creating effective cloud computing contracts for the Federal Government: Best Practice for acquiring IT as a Service	Briefly discusses the need for and issues related to terms of service agreements, non-disclosure agreements and service level agreements. The document also lists and explains prescriptive cloud computing standards and guidelines from NIST.
	State of public sector cloud computing	Describes the work NIST is doing with regard to cloud computing and provides numerous case studies about the state adoption of cloud computing.

Table 1: Summary of guidance from IT Governance bodies

Body	**Document Title**	**Summary**
CSA	Security guidance for critical areas of focus in cloud computing version 3.	A method for evaluating tolerance before moving assets to the cloud. Describes a conceptual framework to explain cloud computing. The document also gives recommendations and guidelines in 13 critical areas of

		focus in cloud computing. These areas involve issues of governance and operation in the cloud.
	Top ten big data and privacy challenges	Describes the most critical challenges for security related to big data ("massive amounts of digital information companies and governments collect about us and our surroundings.") on the cloud.
	Cloud consumer advocacy questionnaire and information survey	The results of a survey of leading CSPs. The survey was done to determine the data governance and data security capabilities which these CSPs provide. Areas of maturity and concern are concluded from these findings.
	Top threats to cloud computing version 1.0	The documents lists, explains and provides recommendations and references to guidelines for seven threats to cloud computing.
	Mobile device management: key components, v1.0	Outlines several controls that organization should have in place when allowing the use of mobile devices.
	Security guidance for critical areas of mobile computing	Describes what mobile computing is, the various components of mobile computing and how it is affecting organizations today. It then describes threats and recommendations for each of the components of mobile computing.
	Trusted Cloud Reference Architecture Quick guide to the reference architecture	The documents present and explain a reference architecture that provide a "methodology and a set of tools that enable security architects, enterprise architects, and risk management professionals to leverage a common set of solutions."
	Top threats to cloud computing survey results update 2012	A two page document illustrating the top threats to cloud computing as discovered through a survey.
	Top threats to mobile computing	The results of a survey to identify the most critical threats from mobile devices accessing networks through cellular access networks. The threats are listed, explained and illustrated with examples.
Commission of the European Communities, Expert Group on Cloud Computing	Quantitive Estimates of the demand for cloud computing in Europe and the likely barriers to uptake	Provides a set of recommendations based on the findings of a survey of European organizations about the barriers, concerns and benefits of cloud computing. Recommendations include removing regulatory barriers to adoption, building trust and promoting standardization and interoperability.
	A roadmap for advanced cloud technologies under	This document describes how Europe plans on taking advantage of the current phase of cloud computing in the

	H2020	hype cycle. To gain an advantage in cloud computing, while the technology as a whole is going through the dip after the hike and before the wide acceptance of the hype cycle, the report list various areas that need attention in order for cloud computing to be widely used in Europe.
	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the potential of cloud computing in Europe.	This document outlines plans and recommendation which the Commission makes in order to support and encourage the adoption of cloud computing in Europe. The main areas which require attention are seen as dealing with the different legal frameworks which affect cloud computing, problems with contracts and problems related to the proliferation of standards. The work refers extensively to the Digital Agenda for Europe.
	Commission staff working document accompanying the document 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the potential of cloud computing in Europe.	"This Staff Working Paper provides supporting analysis to the political proposals in the Cloud Strategy Communication"
ENISA	Cloud Computing: Benefits, risks and recommendations for information security	A list of risks is given. These are rated according to severity and explained. A list of vulnerabilities is also given. In addition a list of questions is provided which will assist organization to ensure them of adequate information protection when using cloud computing. Furthermore the document provides a set of legal recommendation for the use of cloud computing.
	Cloud Computing Information Assurance Framework	"Provides a set of questions that an organisation can ask a cloud provider to assure themselves that they are sufficiently protecting the information entrusted to them." The same questions are provided in the document described above.
	Procure Secure. A guide to monitoring of security service levels in cloud contracts.	A subset of the guidelines provided in the assurance framework is presented. The guidelines assist in ensure security when using cloud services. Once again a checklist is provided about such issues as service availability, log management and incident management.

	Security & resilience in governmental clouds.	Presents a decision making model that can assist in comparing cloud services and making a decision about cloud services which will meet organizational needs for resilience and security. The report provides a good description and methodology to help analyse legal requirements.
	An SME perspective on cloud computing.	The results of a survey of SMEs in Europe about cloud computing. The analysis of the findings are included in the report entitled "cloud computing: business benefits, risks and recommendations for information security" described above.

Table 2: Summary of guidance for cloud computing by other bodies

Unified IT Compliance Components		
Business function	Key Activities	Possible Guidelines
Governance	Govern cloud computing within context of an enterprise IT governance program using standards and best practice guidelines.	(Horwath, 2012; ISACA, 2011; CSA, 2011a; CSA, 2011c)
	Assign roles and responsibilities to players at different levels of management for cloud computing activities	(Horwath, 2012)
	Establish business goals and businesses cases for cloud computing	(ISACA, IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, 2011)
Risk Management	Follow an accepted approach that includes a risk assessment for the selection of cloud computing services, deployment models and CSPs.	(Cattedu, 2011; NIST, 2011c; ISACA, 2012)
	Determine the value of potential cloud computing solutions, taking into account risks and opportunities related to the solution.	(ISACA, 2012a; NIST, 2011a; NIST, 2011e; NIST, 2012a)
	Ensure that a system is in place to ensure that enterprise risks introduced by cloud computing are managed using appropriate controls.	(Horwath C. C., 2012; CSA, 2009; CSA, 2012)
Compliance	Ensure that you have a system in place for determining legal risks and other compliance risks.	(Cattedu, 2011)
	Ensure that you follow accepted guidance regarding agreements with the CSP where possible.	(CIO Council, Chief Acquisition Officers Council, 2012; ENISA, 2009a; ENISA, 2011)

	Monitor and manage compliance activities and controls.	(ISACA, IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, 2011)
Continuous Improvement	Ensure that changes in the cloud computing environment are monitored and acted on accordingly.	Importance mentioned not particular guidance given on how this should be done.
Unified control processes	Ensure that you have a set of controls in place for cloud computing based on best practice guidance.	(ISACA, 2011)

Table 3 Unified IT Compliance Approach to cloud computing assurance for cloud users

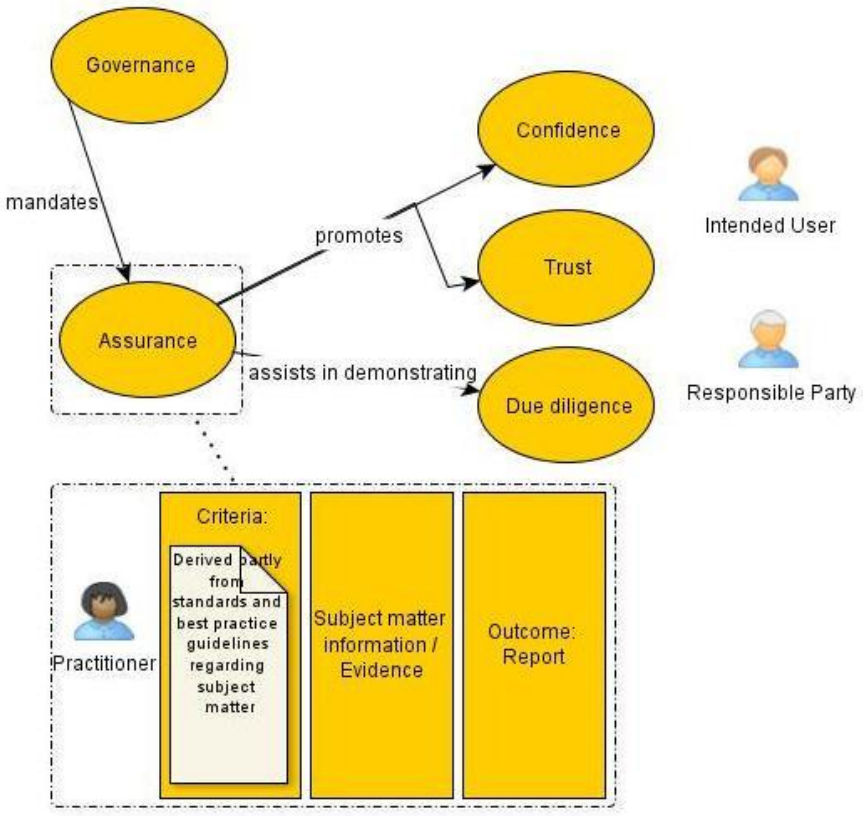


Figure 1 Concept diagram for relationship between assurance and governance

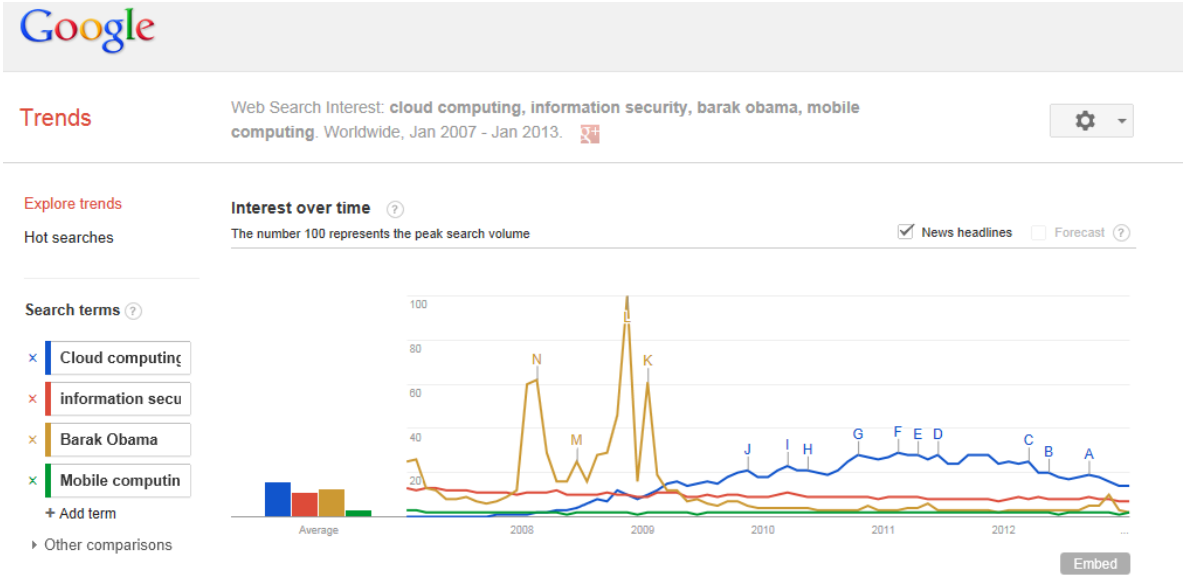


Figure 2 Cloud computing search on Google Trends

Appendix B5

A Framework for Assuring the Conformance of Cloud-based Email

Melanie Willett and Rossouw Von Solms
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth, Republic of South Africa
Rossouw.VonSolms@nmmu.ac.za

Abstract—**Cloud-based email, like various other cloud computing solutions, is associated with significant potential benefits for higher education institutions. There are, however, concerns regarding matters such as ensuring compliance and appropriate governance that can affect the level of trust that institutions have regarding the use of such services. This paper describes a framework for assuring the conformance of cloud-based email (FACCE). This framework is intended to assist higher education institutions in South Africa in addressing these problems.**

Keywords: cloud computing, cloud-based email, cloud computing assurance, cloud computing conformance, framework for cloud assurance

INTRODUCTION

In order for well-governed organisations to confidently embrace and fully benefit from any IT solution, there should be confidence and trust that this can be done in a manner that is compliant with internal and external requirements and demonstrates due care. In other words, organisations need assurance [24]. This is true for the field of cloud computing. One cloud computing solution that has great potential to benefit higher education institutions is cloud-based email. Institutions making use of this service have the ability to access email and other services free of charge, without the administrative hassle of maintaining these services in-house. There are, however, concerns relating to compliance when using such services. Accordingly, higher education institutions could benefit from a means that would assure that cloud-based email can be used in a complaint manner. This paper proposes a framework to assist with this.

Before describing this framework for assuring the conformance of cloud-based email (FACCE), the problem area addressed by this framework is described in more detail in the following section.

THE NEED FOR CLOUD-BASED EMAIL ASSURANCE

The potential benefits associated with many of the vast array of cloud computing solutions available to individuals and organisations are widely recognised and reported on [5, 8, 10, 17, 20]. Some countries demonstrate an appreciation of these potential advantages by promoting the adoption of such services at government level [2, 7, 13]. For example, the American and UK governments have gone as far as having a 'Cloud first' policy [13, 15].

The potential advantage of being able to access IT-related services as needed, at reduced rates, with less administrative hassle, is appealing to many education institutions globally [3, 16, 22]. Consequently, higher education institutions have been among the first adopters of cloud computing [4].

One cloud computing service that is now widely adopted by education institutions is free cloud-based email. Two popular providers of cloud-based email are Google Apps for education [6] and Office 365 education [14]. Further, the use of cloud-based email and related services has become widely accepted in higher education institutions in South Africa as well. A survey of higher education institutions in South Africa found that of the sixteen respondents, only one institution was not planning on implementing cloud-based email. The results of the survey are shown in Fig 1.

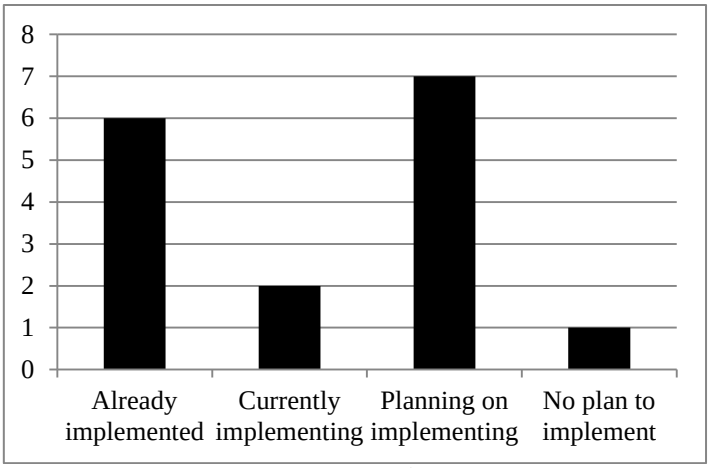


Figure 1. Cloud-based email adoption in South African higher education institutions in 2012

There are still, however, significant concerns regarding cloud computing, despite the tremendous uptake of cloud computing services such as cloud-based email. The fact that institutions relinquish a degree of control but remain responsible for their information when entrusting it to a cloud service provider (CSP) raises concerns regarding the governance of such information [24]. Issues related to compliance when using cloud computing is another important concern. Such compliance-related concerns are often associated with the fact that different compliance requirements may apply to the information stored, owned and administered across geographic and jurisdictional boundaries [23, 1]. These and other concerns often result in a lack of trust in cloud computing services [19, 21].

A survey of higher education institutions in South Africa regarding the use of cloud-based email conducted in 2009 and again in 2012 highlights that these concerns can be seen as applicable to these higher education institutions as well. The main concerns of respondents regarding the use of cloud-based email were identified as being regulatory compliance and record management. In 2009, seven out of eight respondents either agreed or strongly agreed with the following statement: *I have not been provided with an adequate set of good practice guidelines for the governance, risk and compliance of cloud-based email*. Participants in the survey conducted in 2012 were asked: "Do you think that South African universities would benefit from a set of guidelines for compliance in the adoption of cloud-based email?" Only one out of 17 institutions responded "no". Accordingly, the vast majority of institutions (94%) believe that such guidelines would be beneficial.

Considering the important role of email, it is perturbing that IT professionals in higher education institutions in South Africa feel inadequately equipped in terms of the governance, risk and compliance of cloud-based email and are apprehensive about compliance in particular. Such institutions could benefit from a means of gaining assurance. This paper describes a framework that aims to assist in this regard. The framework is described in the next section.

A FRAMEWORK FOR ASSURING THE CONFORMANCE OF CLOUD-BASED EMAIL (FACCE)

As described previously, the fact that cloud-based email is being used in higher education institutions in South Africa, despite the fact that there is a lack of trust that this can be done in a fully compliant manner, is a problem.

This work proposes a Framework for Assuring the Conformance of Cloud-based Email (FACCE), which aims to assist with this problem by addressing the issues of *assurance* and *conformance* as they relate to cloud-based email. The framework is described in three stages. Firstly, the primary components of the FACCE are identified and described. Secondly, the way that these components are tied together by a methodology for assuring cloud-based email conformance is explained. Thirdly, guidelines that are specific to the implementation of this framework for cloud-based email at higher education institutions are outlined.

FACCE Core Components

In order for cloud computing to be used with confidence by organisations, managers need to be reassured that they can do so in a manner that is effective, that manages risks properly and that is compliant. Assurance is therefore a vital element of the successful use of cloud computing in general and, for the purpose of addressing the problem highlighted in this work, cloud-based email specifically. According to the Business Dictionary.com, assurance is defined as "part of corporate governance in which a management provides accurate and current information to the stakeholders about the efficiency and effectiveness of its policies and operations, and the status of its compliance with the statutory regulations". ISACA similarly defines assurance as an "objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the organization". Assurance is also closely linked to confidence and trust. Therefore, assurance with regard to cloud-based email would involve organisations having systems and controls in place that give stakeholders (including directors) the confidence that this service is being used efficiently and effectively and in such a way that risk are appropriately managed and compliance can be demonstrated.

The international framework for assurance engagements (IFAE) further assists by providing a clear understanding of what is involved in assurance. An assurance engagement is defined as "engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria" [9].

The IFAE describes the primary components and relationships that are necessary for assurance. As can be seen from the definition of an assurance engagement, the IFAE identifies three actors involved: a practitioner, an intended user and a responsible party. A ***practitioner*** is the actor tasked with performing an assurance engagement. The practitioner could, but does not have to, be an auditor. The ***responsible party*** is the entity responsible for the subject matter. The ***intended user*** is the group for which the assurance report is prepared. The intended user may include the responsible party and other stakeholders. All three parties may be involved in deciding on the requirements of the assurance engagement.

As stated in the definition, a practitioner performs an assurance engagement by evaluating evidence about certain subject matter against criteria. ***Criteria*** are the benchmark against which such subject matter is evaluated. It is essential that these criteria are suitable so that the assurance engagement may be consistent and reliable. Suitable criteria should be context sensitive, relevant, complete, reliable, neutral and understandable [9]. They should also be made available to the intended users so that they can understand how the subject matter will be evaluated. ***Evidence*** comes in various forms and provides proof of the way the subject matter measures up to the criteria. The practitioner will judge the sufficiency, appropriateness and materiality of the evidence [9], while the responsible party will work with the practitioner to make evidence available. After the criteria and evidence have been assessed, the practitioner produces an ***assurance report*** which states a "conclusion that conveys the assurance obtained about the subject matter information" [9].

The primary components and relationships necessary for assurance, as described in the IFAE, can be summarised as depicted in Fig 2. Each of these components of assurance will need to be included in a framework for assuring cloud-based email conformance.

To further understand what is necessary for assuring conformance, the field of conformance should be investigated in more detail.

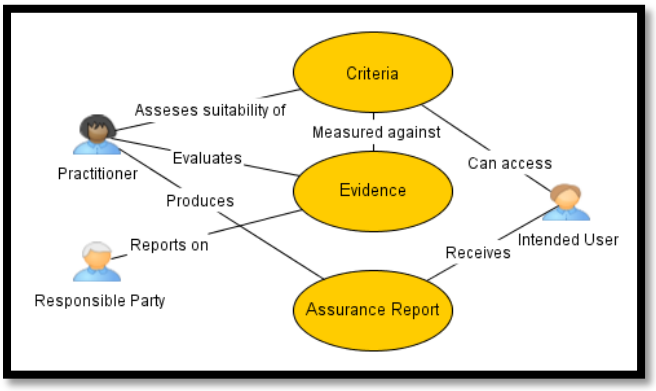


Figure 2. Components and relationships for assurance

Like assurance, conformance is a key element of good IT governance. ISO38500, an internationally recognised standard for the corporate governance of IT, identifies conformance as one of the fundamental principles for IT governance. Conformance involves ensuring that IT initiatives comply with internal and external requirements. These requirements include 1) legal and regulatory obligations (as described in applicable regulations, legislation, common law and contractual law), and 2) internal requirements as set out in internal policies, standards, professional guidelines and systems for IT governance [12].

According to ISO38500, ensuring conformance involves the following tasks:

- Evaluate – evaluating the extent to which an institution is complying with the legal and regulatory obligations and internal requirements.

- Direct – direction should be given to ensure that staff is aware of their conformance responsibilities and that policy, plans and mechanisms are in place to ensure conformance.

- Monitor – there should be appropriate reporting and assurance practices in place to ensure that IT conformance and related IT activities are adequately monitored [12].

Besides the requirements and tasks related to conformance, enablers are other components which can be used to assist with achieving conformance. Enablers are enterprise resources and other factors that influence whether IT governance will be successful [11]. COBIT 5 identifies seven enablers for IT governance. These include principles, policies and frameworks; processes; organisational structures; culture, ethics and behaviour; information; services, infrastructure and applications and people, skills and competencies.

From the preceding two paragraphs it should be clear that, to ensure conformance as part of IT governance, an understanding of the requirements for conformance (as outlined in various ***conformance requirement documents***) should influence the implementation of the tasks of ***evaluate, direct and monitor*** with the aid of ***enablers***.

All the components necessary for conformance and assurance identified in this section form the core of the FACCE. These components can be used together for assuring conformance by using the methodology described in the next section.

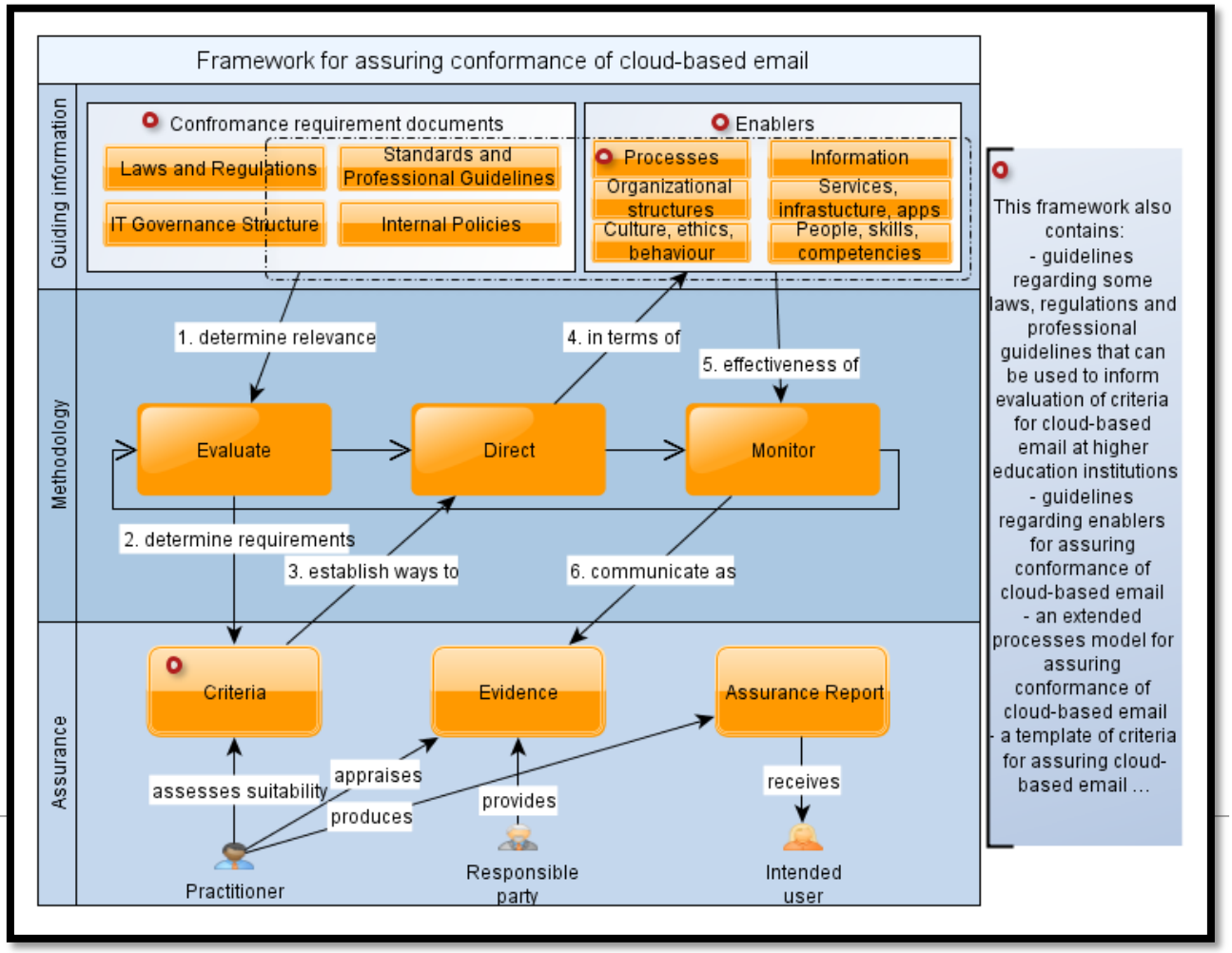
FACCE methodology

The previous section highlighted the key components of and relationships involved in a framework for assuring the conformance of cloud-based email. This section describes the manner in which these components interact to assure cloud-based email conformance. This interaction between components is described mainly in terms of the methodology that binds all these components together. The components, relationships and methodology that make up the FACCE are shown in Figure 3.

The macro methodology for assuring cloud-based email conformance, as described in the FACCE, is based on the governance tasks of evaluate, direct and monitor. The core role of these tasks becomes clear in the description of the micro methodology of the FACCE that follows.

The micro methodology for assuring cloud-based email conformance at higher education institutions in South Africa includes the six steps shown if Figure 3 and described below. For each step in the methodology the related core task for governing conformance is shown in bold in the description. The other core components are highlighted using italics for each step.

1. As per number 1 in Fig 3, the first step is to **evaluate** the *conformance requirement documents* to determine the relevance of their contents to cloud-based email conformance. This is clearly an important step since it is impossible to assure conformance unless there is a clear picture of what an institution is required to conform to. A full set of relevant requirement documents should, therefore, be identified and evaluated when attempting to assess the relevance of cloud-based email. Depending on how cloud-based email is used and implemented at various institutions, different conformance requirement documents may apply. To illustrate, the laws and regulations that would apply to institutions regarding document retention may differ depending on who is using the cloud-based email system (e.g. students only or staff and students) and the type of information that is managed solely by the CSP (e.g. if only students use cloud-based email while staff email is catered for in-house, any correspondence between staff and students would still be stored on internal email servers, therefore only email correspondence between students would be managed solely by the CSP).
2. **Evaluate** relevant conformance requirement documents to determine the requirements for cloud-based email conformance. The documents that were identified as relevant in the previous step can now be evaluated to specify exactly what is required from higher education institutions. Subsequently, these requirements should be communicated as *criteria* for assuring cloud-based email conformance. Thus, having a clear set of criteria for cloud-based email conformance provides an important basis for the rest of the conformance assurance process. Criteria can be examined from an assurance perspective to establish their relevance for an assurance engagement. Once this has been done all actors (practitioners, responsible parties and intended users) will have a clear understanding of what is required for cloud-based email conformance and therefore how to proceed as described in the next step.



3. Use the established *criteria* for assuring cloud-based email conformance to draw up directives. An examination of these criteria will assist in determining how to meet these requirements and, therefore, how to **direct** activities from then on. This is especially true if guidelines for meeting the criteria are compiled where possible when evaluating the requirements.

4. **Direct** initiatives to support cloud-based email conformance in terms of *enablers*. Directives for cloud-based email conformance should be communicated in terms of enablers. There will usually be at least a process in place to ensure that the directives are carried out efficiently.

5. **Monitor** the effectiveness of initiatives involving one or more *enablers* for cloud-based email conformance. The maturity of the processes for cloud-based email conformance should be evaluated periodically and the results recorded. Where possible tools should be used that can monitor and record cloud-based email activities and incidents automatically.

6. **Monitor** the effectiveness of activities for assuring cloud-based conformance and communicate what has been established as *evidence*. The use of a simple automated tool to record the results of any monitoring activities included in step 5 that are related to cloud-based email conformance will give institutions an indication of how they are measuring up to the criteria at any given stage. This will allow institutions to recognise easily where improvement is required and may build confidence that cloud-based email is used efficiently within the institution.

This methodology should be used in a continuous and iterative manner. It is important to reassess the relevance of conformance documents and criteria from time to time as the legal, IT and other aspects of the environment in which higher education institutions exist change and progress. As feedback is received on the effectiveness of initiatives for cloud-based conformance and as guidelines and IT capabilities change, directives for the use of enablers for cloud-based email should be updated. Both the environment and the effectiveness of initiatives should be monitored continuously and the resulting information should be made available to relevant parties.

FACCE implementation guidelines

The description of the first two stages of the FACCE has provided a high-level understanding of how it should be used to accomplish the goal of assuring cloud-based email conformance. However, to achieve real value from the FACCE, it needs to be easy to implement at higher education institutions in South Africa. Accordingly, more detailed guidance on cloud-based email at higher education institutions specifically is necessary. The FACCE provides this level of detail as well, as is illustrated by the red circles and the explanatory notes on the right-hand side of Figure 3. This detail is summarised in this last stage of the FACCE.

There are several areas in which more guidance is provided to assist in implementing the FACCE. These include:

- Recommended reference lists of the documents to consider with regard to cloud-based email conformance in South African higher education institutions. Here guidelines relating to which South African and international laws are likely to affect cloud-based email in South Africa are listed and some potential legal risks are identified. A list of guidelines from reputable bodies for the management of cloud computing that is likely to apply to the use of cloud-based email in South African higher education institutions is provided. These recommended references merely provide a basis from which requirements for cloud-based email conformance can be derived. Each institution remains responsible for ensuring that a complete and relevant list of conformance requirement documents is identified and evaluated.

- A list of guiding criteria and a template for capturing both the criteria and evidence for assuring cloud-based email conformance.

- Guidelines on the way various enablers could be used to aid the assurance of cloud-based email conformance in South African higher education institutions.

- Guidelines that can serve as a basis for creating an extended process model for cloud-based email conformance. Here guidelines for cloud-based email specific processes, such as a process for determining legal risk for cloud-based email, are outlined.

The FACCE has now been described in three stages, each providing more detail on the way in which it should be used. The first stage of the FACCE identified the core components for assurance and conformance. The second stage described a methodology that binds the components identified in the first stage together in a manner that can assure conformance. The final stage described various guidelines that assist in the implementation of the components and methodology identified in a manner that assures conformance of cloud-based email specifically. It should, therefore, now be clear how the FACCE may be used for cloud-based email assurance. The following section highlights some of the benefits of using the approach outlined in the FACCE.

VALUE OF THE FACCE

As stated in the introduction, cloud-based email is a solution that offers higher education institutions the opportunity to take advantage of a necessary service (email) being provisioned and maintained by a service provider free of charge. There would obviously be a great advantage in being able to access such a service. Accordingly, higher education institutions have a responsibility to take advantage of opportunities like this [24]. However, they also have a responsibility in that this should only be done in a manner that shows due care and that conforms to the requirements of good governance, legal and regulatory obligations and good practice. The FACCE assists in this regard by providing a means for assuring the conformance of cloud-based email in higher education institutions. Some of the characteristics of the FACCE that make it a desirable solution are outlined in the following paragraphs.

The FACCE is closely aligned with good practice for assurance, conformance and IT governance, as outlined in an international framework for assurance engagements, namely, ISO38500 and COBIT 5. Using such a best-practice-based approach assists in demonstrating *due diligence* since it can be argued that, by following such an approach for assuring conformance, reasonable steps have been taken to avoid committing a tort or offence [18].

In addition, the FACCE is based strongly on standards and guidelines for IT governance, especially in the area of conformance. It can therefore be used to assist in demonstrating good *IT governance* in the area of cloud-based email conformance.

Since assurance is closely related to building confidence and trust, the FACCE could also be used to assist in building *trust* in the use of cloud-based email at higher education institutions.

From the above it is clear that the FACCE is a framework that could assist higher education institutions with their responsibility for taking advantage of the opportunities related to the use of free cloud-based email in a manner that assures conformance.

CONCLUSION

We have proposed a framework for assuring the conformance of cloud-based email (FACCE) at higher education institutions. By providing a standards and best-practice based mechanism for assurance, the FACCE can be used to assure cloud-based email conformance in a manner that shows due diligence, contributes to overall IT governance initiatives and builds trust in cloud-based email.

The FACCE is currently being verified by a higher education institution in South Africa. The results of this verification should be available soon.

WORKS CITED

[1] Email regulation issues leaving businesses confused. (2013, January). *CPA Practice Management Forum, 9*(1), p. 22.

[2] Australian Government. (2013, May). *The national cloud computing strategy.* Retrieved from Department of Broadband, Communications and the Digital Economy: http://www.attorneygeneral.gov.au/Mediareleases/Pages/2013/Third%20quarter/5July2013-PolicyforGovernmentuseofcloudcomputingservices.aspx (Access date: 2 May 2013)

[3] Britto, M. (2012, January). Cloud computing in higher education. *Library Student Journal*.

[4] Corbyn, Z. (2009, August 20). *Second Life out as techies embrace cloud email.* Retrieved from Times Higher Education: http://www.timeshighereducation.co.uk/story.asp?storycode=407839 (Access date: 2 March 2010)

[5] ENISA. (2009, November). *Cloud computing: benefits, risks and recommendations for information security.* (D. Catteddu, & G. Hogben, Eds.) http://www.ifap.ru/library/book451.pdf (Access date: 10 June 2010)

[6] Google. (n.d.). *Google Apps for Education*. Retrieved from http://www.google.com/enterprise/apps/education/ (Access date: 1 May 2013)

[7] HM Government. (2011, March). *Government Cloud Strategy.* Retrieved from gov.uk: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85982/government-cloud-strategy_0.pdf (Access date: 1 May 2013)

[8] IBM. (2009, July). The Benefits of Cloud Computing. Somers, NY, USA.

[9] International Auditing and Assurance Standards Board. (2004). *International framework for assurance engagements.* Retrieved from IFAC: http://www.ifac.org/sites/default/files/downloads/b003-2010-iaasb-handbook-framework.pdf (Access date: 1 June 2012)

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

[11] ISACA. (2010). COBIT 5. A Business framework for the governance and management of enterprise IT. Rolling Meadows, IL, USA: ISACA.

[12] ISO. (2008, June 1). ISO/IEC 38500:2008 Corporate governance of information technology. *International Standard*. Pretoria, Pretoria: SABS Standards Division.

[13] Kundra, V. (2011). *Federal cloud computing strategy.* Retrieved from DHS.gov: http://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf (Access date: 13 January 2013)

[14] Microsoft. (n.d.). *Office 365 Education*. Retrieved from http://office.microsoft.com/en-us/academic/ (Access date: 1 May 2013)

[15] Middleton, P. (2013, May 4). *Public Cloud First*. Retrieved from HM Government G- Cloud: http://gcloud.civilservice.gov.uk/public-cloud-first/ (Access date: 2 June 2013)

[16] Mircea, M., & Andreescu, A. I. (2011). Using cloud computing in education: a strategy to improve agility in the current financial crisis. *Communications of the IBIMA, 2011*, 15. Retrieved from http://www.ibimapublishing.com/journals/CIBIMA/cibima.html (Access date: 2 June 2012)

[17] NIST. (2012, May 29). *Cloud Computing Synopsis and Recommendations (NIST Special Publication 800-146).* Retrieved http://www.nist.gov/manuscript-publication-search.cfm?pub_id=911075 (Access date: 13 January 2013)

[18] OECD. (2004). *OECD Principles of Corporate Governance 2004.* France: OECD Publishing.

[19] Pearson, S., & Benameur, A. (2010, November/December). Privacy, security and trust issues arising from cloud computing. *Cloud computing technology and science*, 693–702. doi: 10.1109/CloudCom.2010.66

[20] Shivakumar, B. L., & Raju, T. T. (2010). Emerging role of cloud computing in redefining business operations. *Global Management Review*, 48-52.

[21] Suess, J., & Morooney, K. (2009, September/October). Identity management & trust services: Foundations for cloud computing. *EDUCAUSE Review*, 25-42.

[22] Tout, S., Sverdlik, W., & Lawver, G. (2009). Cloud computing and its security in higher education. *The Proceedings of the Information Systems Education Conference 2009. 26*, p. 5. Washington DC: EDSIG.

[23] van Hoboken, J. V., Arnbak, A. M., Van Eijk, N. A., & Kruisjen, N. P. (2012, November). *Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act.* Retrieved from Institute for Information Law: http://www.ivir.nl (Access date: 13 January 2013)

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

Appendix C: Questionnaires

This appendix includes:

- Appendix C1: Questionnaire for IT representatives of South African universities attending ASAUDIT in 2009.
- Appendix C2: Questionnaire for IT representatives of South African universities attending ASAUDIT in 2012.

Appendix C1

Please take a few minutes to complete the following survey for an academic study. Your input is greatly appreciated!

Name (optional): _____ Email address (optional): _____

Name of University: _____

For the purpose of this survey cloud-based email is when an organization's email is hosted wholly or in part on the internet by a service provider (e.g. Live@edu or Gmail).

1. Are you considering the use of cloud-based email for your institution?

   ☐ Already implemented ☐ Within the next year ☐ Within the next 2 years
   ☐ Not in the near future

2. Which service provider is your institution most likely to use for cloud-based email?

   ☐ Microsoft live@edu ☐ Google Apps Education edition ☐ Other (Please specify_____)

3. Please list any guidelines for cloud-based email implementation that you would recommend:

_____
_____
_____

4. Please tick the 3 issues of greatest concern regarding cloud-based email for your institution?

   ☐ Security concerns ☐ Governance issues ☐ Compliance issues
   ☐ Availability concerns ☐ Regulatory/legal implications ☐ Functionality loss
   ☐ Integration issues ☐ Other (Please specify_____)

5. At my institution we have created cloud-based email accounts for _____% of the staff, _____% of the students and _____% of the alumni.

6. I have not been provided with an adequate set of good practice guidelines for the governance, risk and compliance of cloud-based email.

   ☐ Strongly agree ☐ Agree ☐ Disagree
   ☐ Strongly disagree

Appendix C2

Please take a few minutes to complete the following survey for an academic study. Your input is greatly appreciated!

Name (optional): _____ Email address (optional): _____

Name of University: _____

Hello my name is Melanie Viljoen. I am busy with my PHD about cloud-based email at universities in South Africa. Could I please have 5 minutes of your time to ask you just 6 very brief questions?

For the purpose of this survey cloud-based email is when an organization's email is hosted wholly or in part on the internet by a service provider (e.g. Live@edu or Gmail).

1. Are you considering the use of cloud-based email for your institution?

☐ Already implemented ☐ Within the next year ☐ Within the next 2 years

☐ Not in the near future

2. At my institution we have created cloud-based email accounts for _____% of the staff, _____% of the students and _____% of the alumni.
3. Which service provider is your institution most likely to use for cloud-based email?

☐ Microsoft Iive@edu ☐ Google Apps Education edition ☐ Other (Please specify_____)

4. What is your biggest concern regarding cloud-based email at your university?

☐ Security concerns ☐ Governance issues ☐ Compliance issues

☐ Availability concerns ☐ Regulatory/legal implications ☐ Functionality loss

☐ Integration issues ☐ Other (Please specify_____)

5. I have not been provided with an adequate set of good practice guidelines for the governance, risk and compliance of cloud-based email.

☐ Strongly agree ☐ Agree ☐ Disagree

☐ Strongly disagree

6. Are there any guidelines for cloud-based email implementation that you would recommend:

Thank you!