

**Cloud computing and innovation: its viability, benefits, challenges and  
records management capabilities**

By

**Cameron Bassett**

Submitted in accordance of the requirements for the degree of

**Master of Arts in Information Science**

At the

**UNIVERSITY OF SOUTH AFRICA**

Supervisor: Dr LM Cloete

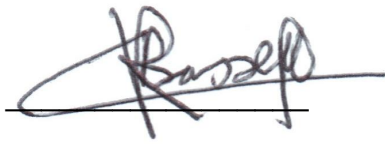
Co-Supervisor: Dr I Schellnack-Kelly

2015

## Declaration

**Student Number: 48528579**

I declare that, *Cloud computing and innovation: its viability, benefits, challenges and records management capabilities*, is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references. I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

A handwritten signature in black ink, appearing to read 'Cameron Bassett', written over a horizontal line.

**15/09/2015**

SIGNATURE (Mr.) **Cameron Bassett**

DATE

**Cameron@Cameronbassett.com**

## Abstract

This research investigated the potential benefits, risks and challenges, innovation properties and viability of cloud computing for records management on an Australian organisation within the mining software development sector. This research involved the use of a case study results analysis as well as a literature analysis. The literature analysis identified *the ten potential benefits of cloud computing*, as well as *the ten risks and challenges associated with cloud computing*. It further identified aspects, which needed to be addressed when adopting cloud computing in order to promote innovation within an organisation.

The case study analysis was compared against a literature review of *ten potential benefits of cloud computing*, as well as *the ten risks and challenges associated with cloud computing*. This was done in order to determine cloud computing's viability for records management for Company X (The company in the case study). Cloud computing was found to be viable for Company X. However, there were certain aspects, which need to be discussed and clarified with the cloud service provider beforehand in order to mitigate possible risks and compliance issues. It is also recommended that a cloud service provider who complies with international standards, such as ISO 15489, be selected.

The viability of cloud computing for organisations similar to Company X (mining software development) followed a related path. These organisations need to ensure that the service provider is compliant with laws in their local jurisdiction, such as *Electronic Transactions Act 1999* (Australia, 2011:14-15), as well as laws where their data (in the cloud) may be hosted. The benefits, risks and challenges of records management and cloud computing are applicable to these similar organisations. However, mitigation of these risks needs to be discussed with a cloud service provider beforehand.

From an innovation perspective, cloud computing is able to promote innovation within an organisation, if certain antecedents are dealt with. Furthermore, if cloud computing is successfully adopted then it should promote innovation within organisations.

### **Keywords**

Cloud computing, cloud computing's potential benefits, cloud computing's challenges, cloud computing's risks, cloud computing and innovation, records management, mining software development, cloud computing Australia.

### **Acknowledgements**

- Dr L.M. Cloete and Dr I. Schellnack-Kelly for their tireless guidance in helping me complete this dissertation.
- Alexander Johnson for her language editing.

### **Dedication**

This one is for me.

## Table of contents

<b>List of abbreviations and acronyms .....</b>	<b>xi</b>
<b>Chapter 1 Introduction and background .....</b>	<b>13</b>
<b>1.1 Introduction .....</b>	<b>13</b>
<b>1.2 Problem statement .....</b>	<b>15</b>
<b>1.3 Research problem and research questions .....</b>	<b>15</b>
<b>1.4 Purpose of the study .....</b>	<b>16</b>
<b>1.5 Research objectives .....</b>	<b>16</b>
<b>1.6 Delimitations of the study .....</b>	<b>16</b>
<b>1.7 Significance of the study .....</b>	<b>17</b>
<b>1.8 Background to the study.....</b>	<b>17</b>
1.8.1 Records and records management.....	18
1.8.2 Viability.....	20
1.8.3 Innovation.....	21
<b>1.9 Case study background .....</b>	<b>22</b>
<b>1.10 Related research .....</b>	<b>23</b>
<b>1.11 Research methodology .....</b>	<b>26</b>
1.11.1 Research approach.....	26
1.11.2 Research design of case study analysis .....	26
1.11.3 Case study analysis .....	27
1.11.4 Literature analysis .....	27
1.11.5 Ethical considerations .....	28
<b>1.12 Chapter outline.....</b>	<b>28</b>
<b>1.13 Summary .....</b>	<b>29</b>
<b>Chapter 2 An introduction to cloud computing.....</b>	<b>30</b>
<b>2.1 Introduction .....</b>	<b>30</b>
<b>2.2 Defining cloud computing.....</b>	<b>30</b>
<b>2.3 Cloud computing definitions .....</b>	<b>31</b>
2.3.1 Vaquero Rodero-Merino, Caceres & Lindner (2009:1) definition .....	32
2.3.2 Buyya, Yeo, Venugopal, Broberg, & Brandic (2009:5) definition .....	33
2.3.3 The National Institute of Standards and Technology definition.....	35
<b>2.4 Cloud computing characteristics breakdown .....</b>	<b>36</b>
<b>2.5 Researcher's definition .....</b>	<b>38</b>

<b>2.6 Cloud computing services .....</b>	<b>39</b>
2.6.1 Software-as-a-Service (SaaS) .....	40
2.6.2 Platform-as-a-Service (PaaS) .....	41
2.6.3 Infrastructure-as-a-Service (IaaS).....	42
<b>2.7 Cloud deployment models .....</b>	<b>43</b>
2.7.1 Private cloud .....	44
2.7.2 Public cloud .....	44
2.7.3 Hybrid cloud .....	44
2.7.4 Community cloud .....	45
<b>2.8 Cloud computing and records management.....</b>	<b>45</b>
<b>2.9 Summary .....</b>	<b>45</b>
<b>Chapter 3 Potential benefits of cloud computing.....</b>	<b>47</b>
<b>3.1 Introduction .....</b>	<b>47</b>
<b>3.2 Background .....</b>	<b>47</b>
<b>3.3 The ten potential benefits of cloud computing .....</b>	<b>52</b>
3.3.1 Cost efficiency .....	52
3.3.2 Scalability and flexibility .....	58
3.3.3 Modernisation of business processes .....	60
3.3.4 Availability and reliability .....	61
3.3.5 Rapid development and deployment.....	62
3.3.6 Business continuity and disaster recovery .....	63
3.3.7 Greater mobility .....	63
3.3.8 Improved power, automation and support management.....	64
3.3.9 Improved security .....	65
3.3.10 Green IT .....	67
<b>3.4 Summary .....</b>	<b>67</b>
<b>Chapter 4 Risks and challenges associated with cloud computing .....</b>	<b>70</b>
<b>4.1 Introduction .....</b>	<b>70</b>
<b>4.2 Background .....</b>	<b>71</b>
<b>4.3 The ten risks and challenges associated with cloud computing .....</b>	<b>77</b>
4.3.1 Compliance .....	78
4.3.2 Legality and auditability .....	80
4.3.3 Security .....	85

4.3.4	Everywhere accessible data .....	95
4.3.5	Incident response, notification and remediation .....	97
4.3.6	Virtualisation.....	99
4.3.7	Governance and enterprise risk management.....	103
4.3.8	Interoperability, portability and data lock-in .....	104
4.3.9	Viability.....	105
4.3.10	Availability and reliability .....	108
<b>4.4</b>	<b>Summary .....</b>	<b>110</b>
<b>Chapter 5 Cloud computing and innovation.....</b>		<b>112</b>
<b>5.1</b>	<b>Introduction .....</b>	<b>112</b>
<b>5.2</b>	<b>Background.....</b>	<b>112</b>
<b>5.3</b>	<b>Cloud computing and innovation.....</b>	<b>112</b>
5.3.1	Cloud business enablers driving innovation.....	113
5.3.2	Cloud Enablement Framework.....	114
5.3.3	Cloud computing adoption and innovation: critical factors .....	116
<b>5.4</b>	<b>Summary .....</b>	<b>118</b>
<b>Chapter 6 Cloud computing’s legislation, standards, benefits and risks for records management .....</b>		<b>120</b>
<b>6.1</b>	<b>Introduction .....</b>	<b>120</b>
<b>6.2</b>	<b>Background.....</b>	<b>121</b>
<b>6.3</b>	<b>Impact of legislation and standards on cloud computing viability for records management .....</b>	<b>122</b>
6.3.1	Australian hosting laws and international standards .....	122
6.3.2	International standards.....	123
<b>6.4</b>	<b>Benefits of records management in the cloud.....</b>	<b>126</b>
6.4.1	Reduced costs .....	127
6.4.2	Less pressure on ICT to provide increased storage capacity .....	127
6.4.3	Service access in various locations .....	127
6.4.4	Collaborative opportunities with various geographically located individuals .....	127
6.4.5	Potential for improved automation such as record keeping as part of business processes.....	128

6.4.6 Increased time for more work due to reduced server maintenance time required.....	128
<b>6.5 Risks of records management in the cloud .....</b>	<b>128</b>
6.5.1 Identification of risks with using cloud computing service providers .....	128
6.5.2 Assessing risks for different records .....	130
6.5.3 Perform due diligence when selecting a service provider .....	130
6.5.4 Contractual arrangement to manage risks .....	131
6.5.5 Monitor arrangements with service providers .....	132
<b>6.6 Summary .....</b>	<b>133</b>
<b>Chapter 7 Research methodology .....</b>	<b>135</b>
7.1 Introduction .....	135
7.2 Research type .....	136
7.3 Research philosophy .....	136
7.4 Research methodology .....	136
7.5 Research design .....	137
7.6 Research analysis .....	139
7.7 Justification for case study selection.....	139
7.8 Case study research methodology .....	142
7.9 Case study research design .....	143
7.10 Case study population and questionnaire .....	143
7.10.1 Questionnaire .....	144
7.11 Case study validity and reliability .....	145
7.11.1 Construct validity.....	145
7.11.2 Reliability .....	146
7.12 Ethical issues .....	146
7.13 Case study results analysis.....	147
7.14 Summary .....	148
<b>Chapter 8 Case study analysis and interpretation of research findings .....</b>	<b>149</b>
8.1 Introduction .....	149
8.2 Case study findings analysis .....	149
8.2.1 Common themes identified .....	150
8.2.2 Cloud computing's viability based on case study findings analysis .....	160
8.2.3 Cloud computing and innovation.....	168



8.3 Summary .....	170
<b>Chapter 9 Final conclusions and recommendations for further research.....</b>	<b>172</b>
9.1 Introduction .....	172
9.2 Potential benefits of cloud computing.....	173
9.3 Challenges and risks associated with cloud computing .....	177
9.4 Viability of cloud computing for records management.....	183
9.5 Cloud computing and innovation .....	185
9.6 Suggestions for further research .....	187
9.7 Recommendations on the use of cloud computing for records management.....	187
9.8 Value of study in closing.....	188
<b>References .....</b>	<b>189</b>
<b>Annexure A: Company X Documentation practices questionnaire.....</b>	<b>203</b>
<b>Annexure B: Company X overview .....</b>	<b>214</b>

### List of Figures

Figure 2.1: Cloud computing services .....	40
Figure 3.1: Cloud computing benefits identified by Carroll, Van der Merwe and Kotzé (2011:4).....	48
Figure 4.1: Cloud computing risks identified by Carroll, Van der Merwe and Kotzé (2011:4-5).....	72
Figure 5.1: Cloud enablement framework (Berman, Kesterson-Townes, Marshall, and Srivathsa 2012:32). .....	115

## List of Tables

Table 2.1: Cloud characteristics identified by Buyya, Yeo, Venugopal, Broberg, & Brandic (2009:6).....	34
Table 3.1: Potential benefits of cloud computing from various sources tabulated against benefits identified by Carroll, Van der Merwe and Kotzé (2011:4) .....	49
Table 3.2: Ten potential benefits of cloud computing .....	68
Table 4.1: Risks and challenges of cloud computing from various sources tabulated against risks identified by Carroll, Van der Merwe and Kotzé. (2011:4-5).	73
Table 4.2: Outages for different cloud services .....	110
Table 4.3: Ten risks and challenges associated with cloud computing .....	111
Table 5.1 Evidence relating to cloud innovation (adapted from Willcocks, Venters & Whitley 2013:194). .....	118
Table 8.1 Common themes identified.....	150
Table 8.2 Work tasks.....	151
Table 8.3 Record types .....	152
Table 8.4: Issues experienced .....	153
Table 8.5 Storage location .....	155
Table 8.6 Shared usage .....	156
Table 8.7 Solutions proposed.....	157
Table 8.8 Case study findings analysis .....	158
Table 8.9: Tasks and elements met by cloud computing's potential benefits .....	160
Table 8.10 Benefits of the cloud for records management vs. Potential benefits of cloud computing .....	162
Table 8.11 Tasks and elements effected by risks and challenges associated with cloud computing .....	165
Table 8.12 Risks of records management in the cloud vs. risks and challenges associated with cloud computing.....	166
Table 8.13: Cloud business enablers driving innovation vs. ten potential benefits of cloud computing .....	169

## **List of abbreviations and acronyms**

- Access Control Lists (ACL)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Application Program Interface (API)
- Chief Information Officer (CIO)
- Cloud Security Alliance (CSA)
- Cloud Security Alliance (CSA)
- Decision Support System (DSS)
- Demilitarised Zone (DMZ)
- Denial of Service (DOS)
- Directory Service (DS)
- Distributed Denial of Service (DDoS)
- Identity and Access Management (IAM)
- Information Communication Technology (ICT)
- Information Technology (IT)
- Infrastructure-as-a-service (IaaS)
- International Business Machines Corporation (IBM)
- International Data Corporation (IDC)
- International Organisation of Standards (ISO)
- Management Information Systems (MIS)
- Platform-as-a-service (PaaS)
- Security as a Service (SecaaS)
- Service Level Agreement (SLA)
- Software-as-a-service (SaaS)
- Virtual Machine (VM)
- Virtual private network (VPN)

## Chapter 1 Introduction and background

This dissertation reports on an investigation into cloud computing and its viability for records management. This research investigated cloud computing in the areas of viability; cloud computing's benefits as well as its challenges for organisations looking to adopt the use of this technology and services; its records management capabilities and how cloud computing could be used to help foster innovation. The research conducted was via an extensive literature analysis and the analysis of a case study's results on a mining software development company's (Company X<sup>1</sup>) current documentation practices.

### 1.1 Introduction

In today's fast changing and rapid expansion of technology and communication speed, the desire to have information anywhere and at any time is now a possibility. Harnessing the power of the Internet, a system of computing has arisen, known as cloud computing.

Many definitions of cloud computing were examined. However, a concise definition of cloud computing was constructed for the purpose of this research. The definition is:

*Cloud computing is a multi-tenancy system of (hard and soft) virtualised resources with utility properties. These rapid, on-the-go, adjustable, pooled resources are used as an alternative to onsite storage and applications and provide virtual computing services, wherever an Internet connection is present (adapted from Armbrust, Fox, Griffith, Joseph and Katz 2009:3, Buyya, Yeo, Venugopal, Broberg, & Brandic 2009:5, Mell & Grance 2011:2; Vaquero Rodero-Merino, Caceres, and Lindner 2009:1).*

---

<sup>1</sup> Company X is a pseudonym, which is used when referring to the mining software development company under investigation in the case study.

Based on the definition above, one can see that cloud computing is the ability to access data over the Internet, from any location, on any Internet accessible device. Resources, such as software, can run through the Internet and if more space is required to host data, it is acquirable at any time. The users only pay for the data they use.

However, cloud computing's capabilities go much further, with increased adoption from private and organisational use, from applications and software, to hardware being designed for its specific use. Using cloud computing as a method of accessing data hosted by third parties creates new records management possibilities, as well as concerns to be addressed.

According to Cervone (2010:162), it is becoming increasingly obvious that cloud computing is changing the way organisations implement information technology (IT). However, it is only due to the increased expansion of the Internet and peoples' ease of access, coupled with the growth of mobile computing in early 2000s, that cloud computing has been able to be brought into service (Laudon & Laudon 2011:170).

With regard to information management within organisations and the management of information systems, there have been new developments with the progression of cloud computing. Laudon & Laudon (2011:166) identify *five eras* of Management Information Systems (MIS) evolution, which correlates with five phases in computer technologies development. They are as follows:

1. Mainframe and minicomputer computing (1959 to present day);
2. Personal computing (1981 to present day);
3. Client/server networks (1983 to present day);
4. Enterprise computing (1992 to present day); and
5. Cloud computing (2000 to present day).

Cloud computing's abilities are now becoming a reality, but its possibilities and impacts may not be fully recognised to those wanting to fully embrace its benefits. The question of viability has arisen and organisations need to be aware of the

risks associated with cloud computing (Heiser & Nicolett 2008:1). Organisations need to be able to decide whether cloud computing is a viable option now, or whether there are still challenges to overcome.

## **1.2 Problem statement**

Cloud computing is becoming a fast growing technology with great benefits as well as challenges. Cloud technology is a new driving paradigm (Delic & Riley 2010:450), and its potential to drive innovation is still underdeveloped (Berman, Kesterson-Townes, Marshall, and Srivathsa 2012:27). The problem for an organisation is assessing the viability and risks of cloud computing and cloud based services, and deciding whether it is a risk worth taking (Heiser & Nicolett 2008:1). Organisations need to determine whether or not cloud computing is a viable and safe alternative for traditional data storage and records management. In this investigation, the analysis of a case study of a mining software development company's documentation practices (storage location, naming, back up, categorization etc. of files) have been used to help answer these questions in relation to similar companies. The literature analysis aimed to provide greater theoretical foundation to cloud computing and records management.

## **1.3 Research problem and research questions**

The formatted research problem statement is as follows:

*With the increase in growth of cloud computing, organisations must be aware of the potential benefits and challenges of adopting the technology of cloud computing. Organisations must be able to assess its viability as an alternative for traditional management of records. Further questions arise on how cloud computing can be used to foster innovation within an organisation.*

The research questions addressed were:

- What are the potential benefits of cloud computing?
- What are the challenges and risks associated with cloud computing?
- To what extent is cloud computing a viable option for records management?
- How can cloud computing be used to foster innovation within an organisation?

#### **1.4 Purpose of the study**

The purpose of this research was to investigate the viability, benefits, challenges and risks of cloud computing. This was in order to provide information towards answering to what extent cloud computing is a viable option for records management. In addition, this research aimed to reveal how cloud computing could be used to promote innovation within organisations.

#### **1.5 Research objectives**

The objectives of the study were:

- To determine cloud computing's potential benefits, risks and challenges;
- To determine cloud computing's viability for records management;
- To identify ways in which cloud computing can help promote innovation and innovative thinking within an organisation.

#### **1.6 Delimitations of the study**

The following section explains the delimitations of the study and its research.

- The case study was conducted on a mining software development company located in Australia and is operating under Australian legislation.
- The case study examined a specific type of company, namely a mining software development company. As such, this research is limited to generalisations to similar companies.
- As part of the investigation into the challenges of cloud computing, this study highlighted legal and compliance issues to create awareness of the risks of cloud computing. The study did not go into detail for each country's laws regarding these issues, as they are numerous for different countries. This study only examined the Australian hosting laws and standards, as the case study examined an Australian organisation. The data hosting laws for each individual country is specific to that country.
- The study identified certain ISO standards for compliance. However, it does not investigate these in detail, as it was not a direct research objective. The standards merely provide context on cloud computing as there are possible

challenges and risks, which arise when migrating personal and financial records to the cloud.

- The benefits, risks and challenges associated with cloud computing are identified but not how to mitigate them. This was because issues relating to risk management fall outside of the scope of the study.
- Due to privacy issues, the company's naming standard for documents and records was not examined in the case study's finding analysis.
- The case study did not examine the Human Resources and Finance departments of Company X, as per the company's wishes.

### **1.7 Significance of the study**

This research contributes to the broader discipline of information science and more specifically to the study field of records management.

This research involved the investigation into cloud computing's benefits, risks and challenges and its viability for records management, which is generalisable to most private organisations. However, with the investigation of the case study results, this study specifically targeted the mining software development sector in Australia. The majority of cloud research with regard to records management involved government agencies. This research focussed on the private sector. Additionally, this research sheds light on cloud computing's potential ability to foster innovation within an organisation and what precursors it may need in order to succeed.

### **1.8 Background to the study**

In the information age, individuals are increasing their use of information resulting in a rapid increase in the volume of information. These rises in information creation and flow have created a growing problem, with regard to the management of this information, as well as how it is going to be accessed when it is needed (Read & Glinn 2011:2).

Organisations need their information to be up to date, at the right time and in the right form in order to survive and make management decisions (Read & Glinn



2011:3). This is achievable through the management of information, documents and records. With the explosion of information and the expansion of the Internet, new avenues need exploration in records management. Cloud computing could be used to help improve access to records, providing the ability to access stored records regardless of the users' location.

From an innovation perspective, cloud computing as a new technology has potential. This study investigated how it could promote innovation within organisations.

The case study involved the investigation of documentation practices. This research method is explained in **Section 1.11**.

### **1.8.1 Records and records management**

For the purpose of this research the concepts of 'records' and 'records management' need to be understood.

Hurley (2004:6) gives a simple definition of a record, where he explains that

A record is documentation linked to some circumstance or event in a meaningful way.

The National Archives of Australia (2013e) give an elaborated definition for what is a record. They state that

All information created, sent and received in the course of your job is potentially a record. Records provide evidence of your agency's business. Whether something is a record depends on the information it contains and the context. Records can be in paper, digital or other formats.

Hurley (2004:6) and National Archives of Australia (2013e) both identify that a record is documentation that contains relevant information which is linked to an

event or a situation. For example, emails or letters which are linked to a business activity.

This is reinforced by Reed (2005:102), who identifies a critical characteristic of a record. Reed identifies that a record 'has to be linked to doing something – it is inherently transactional in its nature.' Furthermore, that in the context of business this 'something' is the documentation of business transactions or business activities.

For the purpose of this research the definition adapted from Hurley (2004:6) and The National Archives of Australia (2013e) will be used.

Records management is the management of records. ISO 15489-1 (ISO 2001:3) defines records management, which is also the current Australian Standard on records management (State Records of Southern Australia 2011:1), as:

*...field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.*

This corresponds with a description given by the National Archives of Australia (2013e), which breaks down the purpose of records management. They state that records management needs to be able to guarantee that records are efficiently and methodically:

- Created, captured, described and secured
- Stored for as long as required
- Finally disposed of or transferred when they no longer have business value.

Based on these definitions and descriptions, for the purpose of this research, records management is defined as: The efficient and methodical management of records from their creation, capture, maintenance and secure storage, until their disposal or transference.

In this research the focus is on cloud computing and records management. More specifically, to what extent is cloud computing a viable option for records management?

### **1.8.2 Viability**

In order to determine cloud computing's viability, issues such as best practices and international standards need consideration in relation to cloud computing and records management. Records management standards, such as ISO 15489, are designed to help guide organisations in systems and processes and in creating records policies and procedures to support records management in all formats. ISO 15489 is a benchmark standard to help organisations evaluate their records management systems and practices (National Archives of Australia 2013a). According to Adam (2007:24), 'ISO 15489 is an international standard that defines best practices for the management of both paper and electronic documents and records.' This means that ISO 15489 may be applicable to records management on a cloud-computing infrastructure, as it still records management in an electronic format. In order to contextualise the study, the investigation was on standards and examples relating to Australia, as the case study conducted was on an organisation in Australia in 2012. The paragraph below mentions these standards.

Migrating information to a cloud platform can affect existing compliance and industry standards. The standards created did not originally have cloud computing in consideration and they often require the owner of the information to be able to identify the information's physical location. Organisations will now have to assess the existing compliance certifications and standards and how the cloud service provider's certifications can assist in this (Convery 2010:13). Additional standards for consideration include:

- AS ISO 15489 is the Australian standard, which provides organisations with guidance when creating record policies and procedures, as well as creating processes and systems to support the records management of all formats (National Archives of Australia 2013b).

- AS 5044, which is an Australian Metadata Standard, is used to provide details on how online resources need to be described in order to improve their accessibility, visibility, manageability and interoperability. (National Archives of Australia 2010; National Archives of Australia 2013b).
- ISO 16175 includes the functional and principle requirements for records created in an electronic office setting (National Archives of Australia 2013b).

The above standards are discussed in more detail in **Chapter 6**. Cloud computing's potential benefits, risks and challenges also play a role in determining its viability. These aspects were investigated through a critical analysis of the literature. **Chapters 3** and **4** present those findings.

### **1.8.3 Innovation**

Within the corporate sphere, a study by Berman, Kesterson-Townes, Marshall, and Srivathsa (2012:27) found that cloud computing technology's ability to drive business innovation is still underdeveloped. New undertakings involving cloud computing, such as the NeCTAR portal (NeCTAR 2011), which is an online cloud collaboration portal can be used to promote collaboration between researchers and drive innovation. The question of how cloud computing can be used to foster innovation with an organisation can be now be addressed. Cloud computing could be a new innovative platform to help records management and further drive innovation across an organisation.

With cloud computing increasing in capabilities, the ability to capitalise on its benefits is beginning to be realised. As an avenue for records management, cloud computing may be able to provide an alternative to traditional storage methods as well as records management. However, cloud computing's practicality can still be drawn into question with regard to the following:

- Cloud computing's viability for records management services.
- What are the pitfalls of cloud computing?
- What elements directly affect it, such as privacy and security?

- Is it at a viable stage for investment, or will it be a few years before companies fully adopt it?

This research aimed to answer these questions by analysing cloud computing in the practical sense, through the investigation of a case study and in a theoretical sense through the critical analysis of the literature related to these issues. The case study analysed an organisation's current documentation practices. The investigation of the case study's findings was used to help determine if cloud computing is a viable option for similar organisations. For this research, similar organisations refer to private companies in the mining software development sector in Australia.

### **1.9 Case study background**

For the purpose of this research, the organisation granted the results of the case study for analysis. Company X, an Australian mining software development company, carried out a case study in 2012. The purpose of the case study was to analyse the company's present documentation practices and provide optimised solutions on how to improve the efficiency of departmental document storage and retrieval. The results were then analysed in order to answer the research questions and objectives, previously identified in **Section 1.3** and **1.5**. The selection of Company X for the case study was due to the specialised field in which the company operates. The mining field deals with issues from limited connectivity, remote location of clients, to security of stored data.

The case study was conducted over an eight-week period. It examined their server layout and documentation practices. This provided a unique opportunity to evaluate whether the information may be transferable to a cloud based records management system. This case study provides a detailed description of Company X's current systems layout for an analysis for the possibility of migrating from their traditional storage mediums to a cloud based system. This case study's analysis served as a basis for investigation in order to answer the research questions identified in **Section 1.3**.

Permission has been granted by the organisation to use results and findings obtained, including the server layout and document management standard (mentioned in the findings) from the case study. The organisation granted permission on the grounds that their name is replaced with a pseudonym. In accordance with this, the organisation is referred to as **Company X**.

Company X (the mining software development company) has provided its own condition for records storage due to a condition set forth by their Document management standard. Company X's *Document management standard* identifies, for their own purpose, that

*The bulk of documentation will be stored and classified as 'Records' in the document management system.*

It is in accordance with this section, and in order to use the results of the case study for analysis in **Chapter 8**, that cloud computing's records management viability was investigated.

### **1.10 Related research**

After an extensive search on national (NEXUS, SACat, SANB, Navtech, ISAP, UCT and Kovsidex) and international (UMI ProQuest Digital Dissertations, Emerald, EBSCO, ScienceDirect, NDLTD and Book Data) databases from June 2012 to July 2015, it became evident that limited research has been done on cloud computing, its benefits, challenges, risks and innovation. The research projects (completed and currently being done) identified below do not address exactly the same research questions that the proposed research intended to answer, but have similar aspects such as innovation, security, cost, adoption, risks and records management.

Similar topics on the NEXUS database include:

- Kandira, M. 2013. *A strategic framework for cloud computing security and compliances requirements to enable cloud services adoption*. (Unpublished Masters Dissertation). University of South Africa.

- Kisten, B. 2013. *Information security risk management in cloud computing*. (Unpublished Masters Dissertation). University of South Africa.
- Ramgovind, S. 2010. *What are the information security considerations in cloud computing?* (Unpublished Masters Dissertation). University of South Africa.
- Trope, J. 2013. *Adoption of cloud computing by South African firms: an institutional theory and diffusion of innovation theory perspective*. (Unpublished Masters Dissertation). Johannesburg: University of the Witwatersrand.

Similar topics on the ProQuest database include:

- Almadallah, M. 2014. *Cloud Computing: Challenges and Risk Management Framework*, North Carolina Agricultural and Technical State University.
- Asghary Karahroudy, A. 2011. *Security Analysis and Framework of Cloud Computing with Parity-Based Partially Distributed File System*, East Carolina University.
- Himmel, M.A. 2012. *Qualitative Analysis of Cloud Computing Risks and Framework for the Rationalization and Mitigation of Cloud Risks*, Pace University.
- Opala, O.J. 2012. *An Analysis Of Security, Cost-Effectiveness, And It Compliance Factors Influencing Cloud Adoption By It Managers*. PHD. Capella University.
- Ross, V.W. 2010. *Factors influencing the adoption of cloud computing by decision making managers*, Capella University.
- Sims, J.E. 2012. *Information security in the age of cloud computing*, The University of Mississippi.
- Suo, S. 2013. *Cloud implementation in organizations: Critical success factors, challenges, and impacts on the IT function*, The Pennsylvania State University.
- Zhang, K. 2012. *Security in cloud computing: New challenges and solutions*, Indiana University.

Similar topics on the ScienceDirect database include:

- Rabai, L.B.A., Jouini, M., Aissa, A.B., Mili, A. 2013. A cybersecurity model in cloud computing environments. *Journal of King Saud University - Computer and Information Sciences*, 25(1):pp.63–75. Available at: <http://www.sciencedirect.com/science/article/pii/S131915781200033X> [Accessed September 15, 2015].
- Lin, A. & Chen, N. 2012. Cloud computing as an innovation: Perception, attitude, and adoption. *International Journal of Information Management*, 32(2012), pp.533–540. Available at: <http://dx.doi.org/10.1016/j.ijinfomgt.2012.04.001>.
- Marston, S., Bandyopadhyay, S., Zhang, J. & Ghalsasi, A. 2011. Cloud computing — The business perspective. Marston, S. et al., 2011. Cloud computing — The business perspective. *Decision Support Systems*, 51(1), pp.176–189. Available at: <http://www.sciencedirect.com/science/article/pii/S0167923610002393> [Accessed July 9, 2014].
- Sun, D., Chang, C., Sun., L. & Wang, X., 2011. Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments. *Procedia Engineering*, 15, pp.2852–2856. Available at: <http://www.sciencedirect.com/science/article/pii/S1877705811020388> [Accessed November 13, 2014].

Similar topics on Emerald database include:

- Askhoj, J., Sugimoto, S. & Nagamori, M., 2011. Preserving records in the cloud. *Records Management Journal*, 21(3), pp.175–187. Available at: <http://www.emeraldinsight.com/10.1108/09565691111186858> [Accessed October 18, 2013].
- Stuart, K. & Bromage, D. 2010. Current state of play: records management and the cloud, *Records Management Journal* 20(2):217-225. Available at: <http://dx.doi.org/10.1108/09565691011064340> [Accessed 23 March 2012].
- Quddusi, S.U.H., 2014. Document management and cloud computing. *The TQM Journal*, 26(2), pp.102–108. Available at: <http://dx.doi.org/10.1108/TQM-06-2012-0038>. [Accessed January 18, 2015].



## **1.11 Research methodology**

The aim of this research was to investigate the viability, benefits, and challenges and risks of cloud computing. In addition to a literature analysis this was done through an analysis of an already completed case study. The case study was conducted on a mining software development company, which provides specialised services relating to consulting, mining shaft designs and mining software development.

The case study provided an analysis and interpretation of the results as well as a recommendation for a new server layout. This dissertation examined the results of these findings. The case study as a research method is explained in detail in **Chapter 7**.

### **1.11.1 Research approach**

The research methodology utilised was a qualitative approach. A qualitative approach takes place in a natural setting (Mouton 1996:168), as was the case with this case study which occurred at Company X offices. The use of a qualitative approach was to learn more about a situation through the gathering of in-depth data, with the goal of not trying to explain or even predict the situation but, rather to understand it (Bhattacharjee 2012:115; Creswell 2002:14-15; Connaway & Powell 2010:80; Mouton 1996:168). According to Hancock & Algozzine (2006:9-10), a case study is representative of a different type of qualitative research as it involves the use of in-depth analysis and the description of a singular system, or unit where the researcher aims to reach an in-depth understanding of the situation under analysis (Case study analysis is discussed in **Section 1.11.3**). Further research was conducted through a critical analysis of the literature (discussed in **Section 1.11.4**) to help answer research questions and objectives previously identified (see **Section 1.5** and **1.6**).

### **1.11.2 Research design of case study analysis**

The research design involved an in-depth analysis of the results of a case study. The investigation of the case study was explorative in nature and sought to develop ideas for further study (Yin 2003:120). This exploratory research was

qualitative, as its use was to build an understanding of the ideas and situation examined (Creswell 2002:33, Connaway & Powell 2010:80).

### **1.11.3 Case study analysis**

The analysis for the case study results took place through the creation of a matrix of themes. Once created, the case study findings were sorted into these themes for analysis. Once completed, the case study results were examined from a new perspective in order to answer the research questions and objectives. More detail is given in **Chapter 7**.

### **1.11.4 Literature analysis**

This research commenced with an in-depth analysis of literature and related research, followed by the case study results analysis. Two research methods were utilised: the critical analysis of literature; and the analysis of the case study, in order to answer the research questions and objectives identified.

The reported literature was analysed and themes were identified which were related to the research problem. These themes were then categorised with the relevant sub-themes and properties. The central theme of the research is cloud computing's viability, with other themes including potential benefits of cloud computing, risks and challenges associated with cloud computing and cloud computing fostering innovation.

These themes were analysed and tabulated to determine commonly identified issues. These issues may direct further research into more specific issues, which need attention that directly impact on cloud computing and answering the research questions of benefits, challenges and viability.

Research questions answered through the analysis of literature are:

- What are the potential benefits of cloud computing?
- What are the challenges and risks associated with cloud computing?
- To what extent is cloud computing a viable option for records management?

- How can cloud computing be used to foster innovation within an organisation?

#### 1.11.5 Ethical considerations

This study adhered to the ethical considerations given by Unisa (2012:9), including those of:

- **Autonomy:** respecting individual rights, autonomy and dignity of those involved in the research
- **Beneficence:** which is to maximising the benefits of the research to the research participants
- **Non-maleficence:** which is to minimise the risks (social and physiological) to those involved in the research
- **Justice** to ensure that the benefits and risks are distributed fairly to those involved in the research.

These are discussed in detail in **Chapter 7** in relation to the case study.

#### 1.12 Chapter outline

The following is a chapter outline of this dissertation:

- **Chapter 1** introduces the research topic by first explaining the background to the study followed by the problem statement, research objectives and finally the case study's background and the research methodology that is used.
- **Chapter 2** explains what cloud computing is and creates a definition for the purpose of this research. Cloud computing's characteristics are also identified and explained.
- **Chapter 3** identifies and explains the potential benefits of cloud computing.
- **Chapter 4** identifies and explains the risks and challenges associated with cloud computing.

- **Chapter 5** deals with cloud computing and innovation.
- **Chapter 6** examines cloud computing's viability for records management.
- **Chapter 7** describes the research methodology applicable to this study.
- **Chapter 8** presents the results and analyses of the case study.
- In **Chapter 9** conclusions are drawn from the findings and recommendations are made based on these findings. In addition, suggestions are made for further research.

### 1.13 Summary

In summary, **Chapter 1** highlights the outline of this research. This research was concerned with the topic: *Cloud computing and innovation: its viability, benefits, challenges and records management capabilities*

In this chapter, the introduction to the research was covered from the background to the study and the case study's background through the research problem and questions, which need to be addressed to help answer the research problem. The research objectives addressed were:

- To determine cloud computing's potential benefits, risks and challenges
- To determine cloud computing's viability for records management
- To identify ways in which cloud computing can help promote innovation and innovative thinking within an organisation

This chapter also outlined the research methodology, which was utilised in the research and finally provided a chapter outline for this dissertation.

In **Chapter 2** a definition of cloud computing will be set forth and the characteristics of cloud computing and its different models will be explained in order to provide context on cloud computing for later chapters.

## Chapter 2 An introduction to cloud computing

### 2.1 Introduction

This chapter explores the concept of cloud computing. The concept is broken down into its basic characteristics, which are utilised to formulate a definition of cloud computing for the purpose of this research. These characteristics are then explained in order to provide an overview of what makes cloud computing a unique technology. Finally, the cloud service models and cloud types are examined and explained to provide insight into the different cloud services and their implications. This is needed for a deeper understanding of cloud computing and its characteristics. Furthermore, this examination is used to provide an overview of cloud computing's structure to help explain cloud computing's benefits and challenges in the following chapters. The different cloud types are examined as well to contextualise cloud computing's viability for records management.

### 2.2 Defining cloud computing

In today's world, cloud-computing services are growing exponentially (Hickey 2010). However, with the increase in cloud computing use, there can be confusion with regard to what cloud computing actually is and why it is such a revolutionary technology. To help answer these questions, the term *Cloud* needs to be examined first.

Cloud stands for *common location independent, online utility on demand* (Cervone 2010:164). Chan (2009) provides an analysis of these terms:

- **Common** refers to a shared resource between multiple applications and customers.
- **Location Independent** refers to the notion that the physical location of the user/cloud service is irrelevant. The user should be able to access the data regardless of their physical location/hosting location.
- **Online** means that it is accessible over a network. This does not necessarily mean a virtual private network (VPN) or the Internet. *Online* also refers to availability.

- *Utility* in terms of pricing is based on the amount of resources that are being used.
- *On Demand* refers to the resources being given, as they are required.

Cloud computing is based on the idea of pooling physical resources (e.g. systems and storage) and presenting them in a virtual form (Sosinsky 2011:25). Virtualisation refers to the simulation of IT resources on a physical host server (Himmel 2012:125). Virtualisation gives applications the ability to be transferred to other hardware images, without alerting the application to this movement. These applications are “virtualised” when they are isolated from the hardware in this manner (Himmel 2012:21). Cloud service providers utilise virtualisation technologies, which is the abstraction of computing resources from the hardware on the system (Convery 2010:10). Virtualisation is discussed in more detail in **Chapter 4, Section 4.3.6 Virtualisation**.

Sosinsky (2011:25) explains these two concepts, *Virtualisation* and *Abstraction*, in relation to cloud computing as:

1. *Virtualisation*: cloud computing virtualises systems by pooling and sharing of resources. Storage space and systems are supplied, as they are required from a centralised infrastructure. These resources are adjustable and costs are based on usage and multi-tenancy is available.
2. *Abstraction*: cloud computing abstracts, from users and developers, details of systems implementation. Applications run on a physical system that is not specified and data is stored in locations that are unknown to the user. The administration of these systems is outsourced and access by users is always available.

### **2.3 Cloud computing definitions**

Cloud computing requires a concise definition. The definition also needs to be consolidated, combining all of cloud computing’s characteristics. A consolidated

cloud computing definition is important as it draws focus towards the potential benefits of cloud computing for businesses (Vaquero *et al.* 2009:1).

There is an abundance of “cloud computing” definitions available and many are conflicting. Cloud computing is defined by either a broad umbrella definition for everything related to virtual computing; or a very narrow definition may also be applied where cloud computing is viewed as “utility computing”, which harnesses the Internet to provide virtual servers from external providers (Rittinghouse & Ransome 2010:xxvii).

The definitions by Vaquero *et al.* (2009:1), Buyya *et al.* (2009:5), and The National Institute of Standards, and Technology (Mell & Grance 2011:2) illustrate these conflicts. These definitions are examined in the following sections.

### **2.3.1 Vaquero Rodero-Merino, Caceres & Lindner (2009:1) definition**

This definition was selected for review as its construction was based on an analysis of various cloud-computing definitions. Vaquero *et al.* (2009:1) provide a definition derived from analysing numerous academic definitions. This definition is:

Clouds are a large pool of easily usable and accessible virtualised resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for optimum resource utilisation. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs.

Vaquero *et al.* (2009:2) definition analysed various cloud-computing definitions to identify a minimum common denominator, in order to get an integrated definition that would contain only the essentials. They state that their definition is “an encompassing definition of the cloud”. However, after their definition was formulated they reveal that, if they were looking for the minimum common denominator, that it would lead them to no definition. This is because there is not a single feature that was proposed by all the definitions that they examined.

Vaquero *et al.* (2009:1) definition contains the following characteristics:

- Pooled, easily accessible and usable virtualised resources (hardware/ software/ development platforms)
- Dynamically scalable resources for optimum resource allocation
- Resources based on pay-per-use model
- Guarantees offered by provider through customised SLA (Service Level Agreement)

The following list illustrates the cloud characteristics identified by Vaquero *et al.* in their research. This list was adapted from a Vaquero *et al.* (2009:4).

- Virtualisation
- Internet centric
- Variety of resources
- Automatic adaption
- Scalability
- Resource optimisation
- Pay per use
- Service SLAs
- Infrastructure SLAs

These characteristics are explained in detail in **Chapter 3: Potential benefits of cloud computing.**

### **2.3.2 Buyya, Yeo, Venugopal, Broberg, & Brandic (2009:5) definition**

This definition was selected for review because of how it was constructed. According to Buyya *et al.* (2009:5), their definition was constructed based on their observations of the essence of clouds' potential. A definition provided by Buyya *et al.* (2009:5) reads:

A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers, dynamically provisioned and presented as one or more unified computing resource(s), based on service-



level agreements, established through negotiation between the service provider and consumers.

This definition was used in their paper, which compares cloud computing to cluster and grid computing in order to help provide a clear understanding of what cloud computing is (Buyya *et al.* 2009:4). They further identify the individual characteristics of each and compare them.

Buyya *et al.* (2009:5) definition contains the following characteristics:

- Parallel and distributed system of virtualised connected computers
- Dynamically provisioned computers presented as a unified resource
- Based on SLA negotiated with the service provider

**Table 2.1** illustrates the cloud characteristics identified by Buyya *et al.* in their research.

**Table 2.1: Cloud characteristics identified by Buyya, Yeo, Venugopal, Broberg, & Brandic (2009:6)**

Characteristics/Systems	Clouds
<b>Population</b>	Commodity computers and high-end servers and network attached storage
<b>Size / scalability</b>	100s to 1000s
<b>Node operating system (os)</b>	A hypervisor (VM) on which multiple OSs run
<b>Ownership</b>	Single
<b>Interconnection network/ speed</b>	Dedicated, high-end with low latency and high bandwidth
<b>Security/privacy</b>	Each user/ application is provided with a virtual machine. High security/privacy is guaranteed. Support for setting per-file access control list (ACL).
<b>Discovery</b>	Membership services
<b>Service negotiation</b>	Yes, SLA based
<b>User management</b>	Centralised or can be delegated to third party
<b>Resource management</b>	Centralised/ Distributed
<b>Allocation / scheduling</b>	Both centralised/decentralised
<b>Standards / inter- operability</b>	Web Services (SOAP and REST)

Characteristics/Systems	Clouds
<b>Single system image</b>	Yes, but optional
<b>Capacity</b>	Provisioned on demand
<b>Characteristics/Systems</b>	Clouds
<b>Failure management (Self-healing)</b>	Strong support for failover and content replication. VMs can be easily migrated from one node to other.
<b>Pricing of services</b>	Utility pricing, discounted for larger customers.
<b>Internetworking</b>	High potential, third party solution providers can loosely tie together services of different Clouds.
<b>Application drivers</b>	Dynamically provisioned legacy and web applications; Content delivery.
<b>Potential for Building 3rd Party or Value-added Solutions</b>	High potential – can create new services by provisioning of compute, storage, and application services and offer as their own isolated or composite Cloud services to users.

(Adapted from Buyya et al (2009:6)

These characteristics are explained in detail in **Chapter 3: Benefits of cloud computing**.

### 2.3.3 The National Institute of Standards and Technology definition

The National Institute of Standards and Technology (NIST) (Mell & Grance 2011:2) provide the third definition for examination. Their definition of cloud computing is as follows:

Cloud computing is a model for enabling ubiquitous, 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 cloud model is composed of five essential characteristics, three service models and four deployment models.

This definition was chosen because it was prepared for use by Federal Agencies of the United States and was intended to provide a starting point for discussion on what is cloud computing and how best to utilise it (Mell & Grance 2011:1).

The NIST (Mell & Grance 2011:2) definition contains the following characteristics:

- Ubiquitous, on-demand network access
- Shared pooled configurable resources
- Rapidly provisioned and releasable resources
- Minimal service provider interaction
- Cloud is composed of five characteristics
- Cloud is composed of three service models
- Cloud is composed of four deployment models

NIST (Mell & Grance 2011:2) identify five essential characteristics, which they believe form part of the cloud-computing model. These characteristics form part of their definition for cloud computing identified above. These characteristics are discussed in greater length in **Section 2.4 Cloud computing characteristics**. The three service models and four deployment models of cloud computing are discussed in the **Section 2.6** and **2.7**.

#### **2.4 Cloud computing characteristics breakdown**

Cloud computing characteristics are important as they identify the unique properties that make cloud computing what it is. This is important in forming a definition of cloud computing, in order to provide a comprehensive description of cloud computing's capabilities.

The characteristics provided by NIST (Mell & Grance 2011:2) present a more easily categorised outline of the characteristics of cloud computing. The characteristics are: On-demand self-service; Resource pooling; Rapid elasticity; Broad network access and Measured service. These characteristics will be examined to provide an understanding of what constitutes cloud computing. Additional characteristics of cloud computing may also be construed as a benefit of cloud computing. To this end, the characteristics not mentioned by NIST are

discussed in **Chapter 3: Potential benefits of cloud computing**, for a more detailed understanding.

The characteristics are:

- 1. On-demand self-service:** the unilateral provision of computing capabilities (e.g. storage), by the consumer, when required without the need of human interaction with every service provider.
- 2. Resource pooling:** the cloud provider pools its resources together to provide multi-tenancy support. Different virtual and physical resources are assigned, then reassigned based on the consumers' requirements. The consumer has no knowledge or control over the location of the resources. The consumer may be able to specify the location of the resources. These resources can be memory, storage, processing etc.
- 3. Rapid elasticity:** computing capabilities have the ability to be rapidly distributed and released; as well as to be automatically distributed to meet the corresponding demand and scalability requirements. On the consumer level, these computing capabilities can be altered at any time and appear unlimited allowing any quantity to be appropriated.
- 4. Broad network access:** Computing capabilities are readily accessible over the network via standard mechanisms that utilise a diverse thick or thin client platform; examples include tablets, laptops and mobile phones.
- 5. Measured service:** cloud services automatically optimise and control resources through a pay-per-use system at the level of abstraction where the service is. Resource usage can be attended to and monitored, by the consumer and the provider, which provides transparency for both parties.

These characteristics coincide with three characteristics identified by Armbrust, Fox, Griffith, Joseph and Katz (2009:3) from a hardware perspective.

1. *“The illusion of infinite computing resources available on demand”*, which in essence allows for users of cloud computing forgoing the requirement of excess planning for future resources.
2. *“The elimination of an up-front commitment by Cloud users”*. Cloud computing is a utility service where resources can be acquired as and when needed.
3. *“The ability to pay for use of computing resources on a short-term basis as needed”*. Cloud computing resources can be used for a short term and then renewed, only if and when they are needed.

Utilising these identified characteristics, a definition has been created for the purpose of this research. This definition is presented in the following section.

## **2.5 Researcher’s definition**

A definition has been constructed for the purpose of this research, which is adapted from Buyya *et al.* (2009:5), Mell & Grance (2011:2); Vaquero *et al.* (2009) as well as from characteristics identified by Armbrust *et al.* (2009:3).

The definition is:

*Cloud computing is a multi-tenancy system of (hard and soft) virtualised resources, with utility properties. These rapid, on the go, adjustable pooled resources are used as an alternative to onsite storage applications and provide virtual computing services, wherever an Internet connection is present.*

This definition contains the following characteristics:

- Multi-tenancy system
- Virtualised resources (hard and soft)
- Resources with utility properties (pay-per-use)
- Rapid on-the-go, adjustable (scalable and on-demand) resources
- Pooled resources
- Virtual computing service
- Available with an internet connection

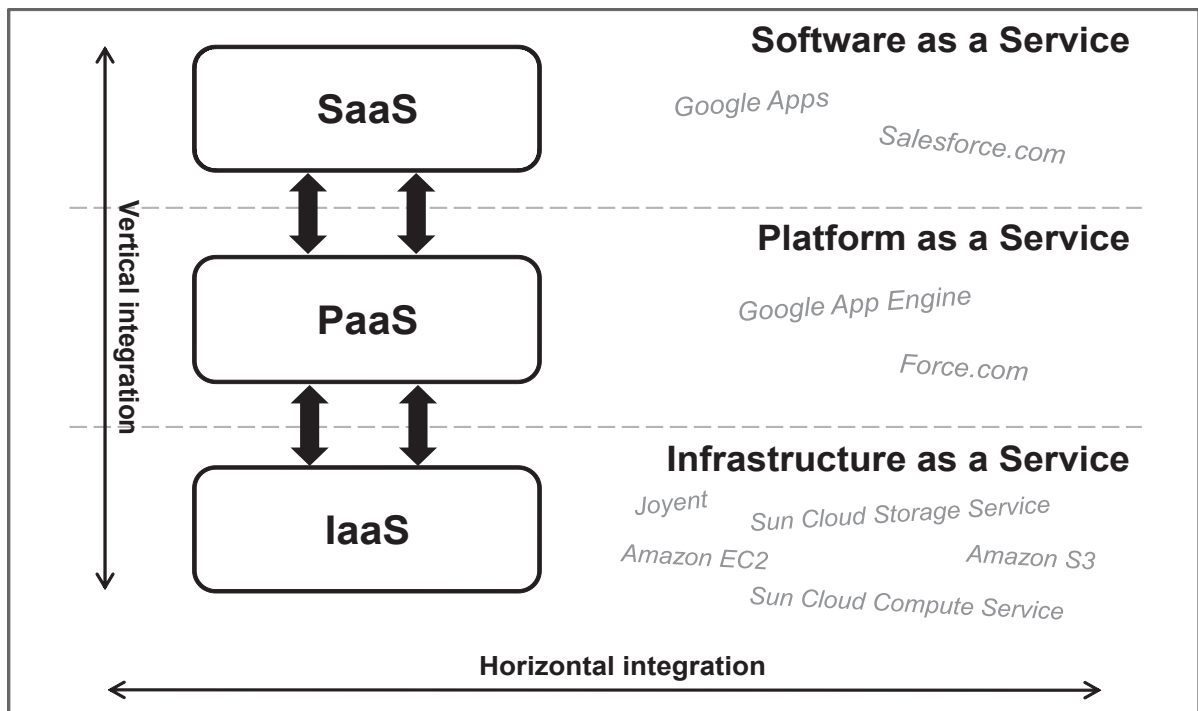
These characteristics are discussed in length in **Chapter 3: Potential benefits of cloud computing**.

## **2.6 Cloud computing services**

Cloud service models are identified by NIST (Mell & Grance 2011:2) definition (see **section 2.3.3**). They are discussed here in order to provide a greater understanding of cloud computing's capabilities. This is done in order to help with answering the research questions, as well as to provide context for the benefits and challenges to be discussed in **Chapters 3** and **4** respectively.

There are three different types of cloud computing services: Software-as-a-service, Platform-as-a-service and Infrastructure-as-a-service (Mell & Grance 2011:2 and Thomas 2010:219). These service models describe the type of service that the cloud service provider offers. This is the SPI model, which is the Software-as-a-service, Platform-as-a-service and Infrastructure-as-a-service (Sosinsky 2011:24).

**Figure 2.1** illustrates the three layers of cloud computing services, built on top of each other. Moving upwards towards the top level, SaaS, the abstraction increases whilst moving down the amount of control increases (Mahmood 2011:7). These three layers are discussed below.



**Figure 2.1: Cloud computing services**

(Staneovska-Slabeva, Wozniak & Ristol 2010:52)

### 2.6.1 Software-as-a-Service (SaaS)

The highest level of abstraction on the cloud is the software service (Dhar 2012:667). Software-as-a-service (SaaS) is the provision of applications/software over the Internet in the form of a service. These applications utilise a pay-as-you-go system, based on the *Utility Computing* paradigm. To the public these applications can be free of charge such as email services like Google mail (Gmail), where the emails and attachments are stored on a remote accessed server. Enterprise applications are created to assist business processes (such as supply-chain management and finances) and are based on already proven business architectures (Mahmood 2011:7). The cloud service providers host these applications (Aleem & Spratt 2013:10).

This type of service provides cost advantages because the consumer does not have to spend money on creating an infrastructure to support these applications (Staneovska-Slabeva *et.al* 2010:54). SaaS is used to provide the operational

environment with full applications, their management and a user interface (Sosinsky 2011:30).

According to the Cloud Security Alliance (2011:51-52) SaaS storage options are accessible through a server/client application or a web interface. If these storage options are accessed through an Application Program Interface, then it is reclassified as Platform-as-a-Service.

SaaS can utilise the following:

- **Volume storage:** data is able to be stored in the IaaS volume, which is connected to dedicated instances that are able to provide SaaS services.
- **Object/ file storage:** data is stored in object storage, however, it is only accessible through the Software-as-a-service application interface.
- **Databases:** content is stored in the database.

SaaS can supply the following:

- **Content/ file storage:** file based content is stored inside the Software-as-a-Service application, which is accessed through a web interface.
- **Information management and storage:** data is entered through a web interface for storage in the Software-as-a-Service application.

### 2.6.2 Platform-as-a-Service (PaaS)

Platform-as-a-Service (PaaS) is the second level of abstraction, which includes the essential applications, infrastructure services as well as the technical services (Dhar 2012:667). This level contains the software development tools for consumers to create and deploy their own specifically tailored applications (Mahmood 2011:8).

PaaS is used to provide the operating systems, services, applications, virtual machines, the development framework, control structures and transaction services (Sosinsky 2011:30). Consumers have control over the application packages, but not the cloud infrastructure such as server and operating systems. Examples include: Google Application Engines and Salesforce.com (Aleem & Spratt 2013:10).



PaaS is used to support the SaaS level and can be built on top of the IaaS to take advantage of the IaaS capabilities (Mahmood 2011:8). According to the Cloud Security Alliance (2011:51), PaaS is able to supply as well as depend on various storage options.

PaaS depends on:

- **Object/ file storage:** data is stored in object storage. However, it is only accessible through the PaaS Application Program Interface.
- **Volume storage:** data is able to be stored in the IaaS volume, which is connected to dedicated instances that are able to provide PaaS services.
- **Databases:** content is stored in the database, this database can be a culmination of IaaS instances which utilise a shared storage back-end.

PaaS can supply:

- **Application storage:** This includes any storage that is directly built into the PaaS application and accessed through Application Program Interfaces without a storage category.
- **Database as a service:** This is an isolated multi-tenant database system, which can be used as a service through an Application Program Interface or direct Structural Query Language.
- **Big Data as a service/ MapReduce/ Hadoop:** Big Data refers to data that has a large scale, wide and heterogeneous distribution as well as currency that need to utilise new technical analytics and architectures. Big Data and Hadoop applications can be given as a cloud system.

### 2.6.3 Infrastructure-as-a-Service (IaaS)

Infrastructure-as-a-service is used to provide computing resources such as virtual storage, virtual infrastructure and virtual machines, as well as additional hardware resources for consumers' personal provision (Sosinsky 2011:30; Staneovska-Slabeva *et al* 2010:52).

This is the lowest level or base level of cloud computing. This is the resource level such as memory and storage services. The cloud service provider will manage the physical infrastructure. They then dedicate a virtualised infrastructure to the consumer, who is given control over the virtual image. These services are offered over the Internet and can include a complete computing infrastructure (Dhar 2012:667).

These services are based on a pay-per-use model. This forms the basis of cloud computing where the PaaS is built on the IaaS Services and in turn, the SaaS is built of the services of the PaaS. This is what allows flexibility of use, where organisations are able to manage their usage and payment based on their requirements. Examples include: Amazons Elastic Compute Cloud (EC2) (Aleem & Spratt 2013:10).

The Cloud Security Alliance (2011:50-51) identifies the following storage options for private or public cloud for IaaS:

- **Volume storage:** This refers to any volumes, which are attached to the IaaS instances, often as a virtual drive. These volumes typically will utilise data dispersion, in order to support security and resiliency.
- **Object storage:** This is similar to a file share that is accessed over a web interface or an Application Program Interface. Object storage can also be referred to as file storage.
- **Raw storage:** This involves the physical media where data is stored and may be virtually mapped in private cloud configurations for faster access.
- **Content delivery network:** Is stored in the object storage and is allocated over various geographic nodes to enhance Internet consumption speeds.

## 2.7 Cloud deployment models

Cloud deployment models are identified in NIST's (Mell & Grance 2011:2) definition. These models are discussed here in order to provide a greater understanding of cloud computing's capabilities and assist with answering the research questions as well as to provide context for the benefits and challenges

chapters (**Chapter 3** and **Chapter 4**) that follow. A cloud deployment model is a type of cloud environment. A consumer or organisation chooses their cloud type based on their specific needs, or organisational requirements (Mahmood 2011:6).

There are four different cloud types or deployment models:

- Private cloud
- Public cloud
- Hybrid cloud
- Community cloud

### **2.7.1 Private cloud**

The private cloud is usually for an organisation's own specific use. It can be located on, or off, their premises and could be managed by a third party cloud provider, or by the organisation (Aleem & Sprott 2013:10; Sosinsky 2011:28). Private clouds provide a multi-tenant and shared system (Mahmood 2011:8).

### **2.7.2 Public cloud**

The public cloud is provided by a cloud service provider and is for public use, or a larger group (Sosinsky 2011:28). The cloud service provider is responsible for the operations of the cloud services as well as maintaining the security. The consumer has minimal control over a public cloud's infrastructure, however, the trade-off is low costs and enhanced data efficiency (Aleem & Sprott 2013:10). Public clouds utilise a pay-as-you-go system in order to regulate the usage (Mahmood 2011:8).

### **2.7.3 Hybrid cloud**

A hybrid cloud is a combination of cloud systems, community, private or public. These clouds are linked together as a single entity, but retain their individual albeit unique properties. This hybrid cloud can offer proprietary or even standard access to applications and/or data (Sosinsky 2011:28).

#### **2.7.4 Community cloud**

A community cloud is a cloud which is used to provide a particular service, or serve a particular purpose. Groups that share a common interest, goal, mission, or a need may use it. This cloud may be managed by a cloud service provider or by a constituent of the usage community (Sosinsky 2011:28).

#### **2.8 Cloud computing and records management**

As mentioned in Chapter 1, this research focus is on cloud computing and records management. More specifically, to what extent is cloud computing a viable option for records management. In accordance with the document management standard of the case study company, Company X provided its own condition for records storage (see **Section 1.3 Documents and records** (MineRP (Australia))) Company X's *Document management standard* identifies, for their own purpose, that

*The bulk of documentation will be stored and classified as 'Records' in the document management system.*

It is in accordance with this section and in order to use the results of the case study for analysis in **Chapter 8**, that cloud computing's records management viability was investigated.

#### **2.9 Summary**

In order to utilise cloud-computing technology, it first needs to be better understood. From the definition point of view, the definition should represent the five NIST defined characteristics:

- On-demand self-service
- Resource pooling
- Rapid elasticity
- Broad network access
- Measures service

Based on these characteristics, a concise and comprehensive definition of cloud computing has been created for the purpose of this research. *Cloud computing is a multi-tenancy system of (hard and soft) virtualised resources with utility properties. These rapid, on the go, adjustable, pooled resources are used as an alternative to onsite storage applications and provide virtual computing services, wherever an Internet connection is present.*

Understanding the various cloud services and deployment models are important for understanding the capabilities of cloud computing. They also help provide a basis for understanding the benefits and challenges associated with cloud computing. The three levels of cloud computing services are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). The four different cloud deployment models are the public cloud; the private cloud; a hybrid cloud and a community cloud.

The three services of cloud computing help create an overview of the structure of cloud computing. It is important to understand how cloud computing is structured for **Chapter 3** and **Chapter 4**. These chapters discuss the benefits and challenges associated with cloud computing. Some of these benefits and challenges refer to the individual layers of this service structure and may not be fully understood without this overview.

## Chapter 3 Potential benefits of cloud computing

### 3.1 Introduction

In Chapter 2, the definitions of cloud computing and its unique characteristics were examined and a new definition was created for the purpose of this research. In this chapter, the potential benefits of cloud computing are identified through a critical analysis of the reported research on the benefits of cloud computing. These have been examined, integrated and organised into ten potential benefit categories and further sub-benefits. The potential benefits are analysed to provide a more detailed view on the sub-benefits of cloud computing. In so doing, information was provided in order to help answer the research question:

- What are the potential benefits of cloud computing?

The term 'potential' in potential benefits of cloud computing signifies that the benefits have the possibility of being achieved given the appropriate circumstances. The potential benefits of cloud computing can only be determined by each individual organisation evaluating cloud computing's impact after implementation. Understanding the potential benefits of cloud computing is vital in assessing its viability as an alternative for records management.

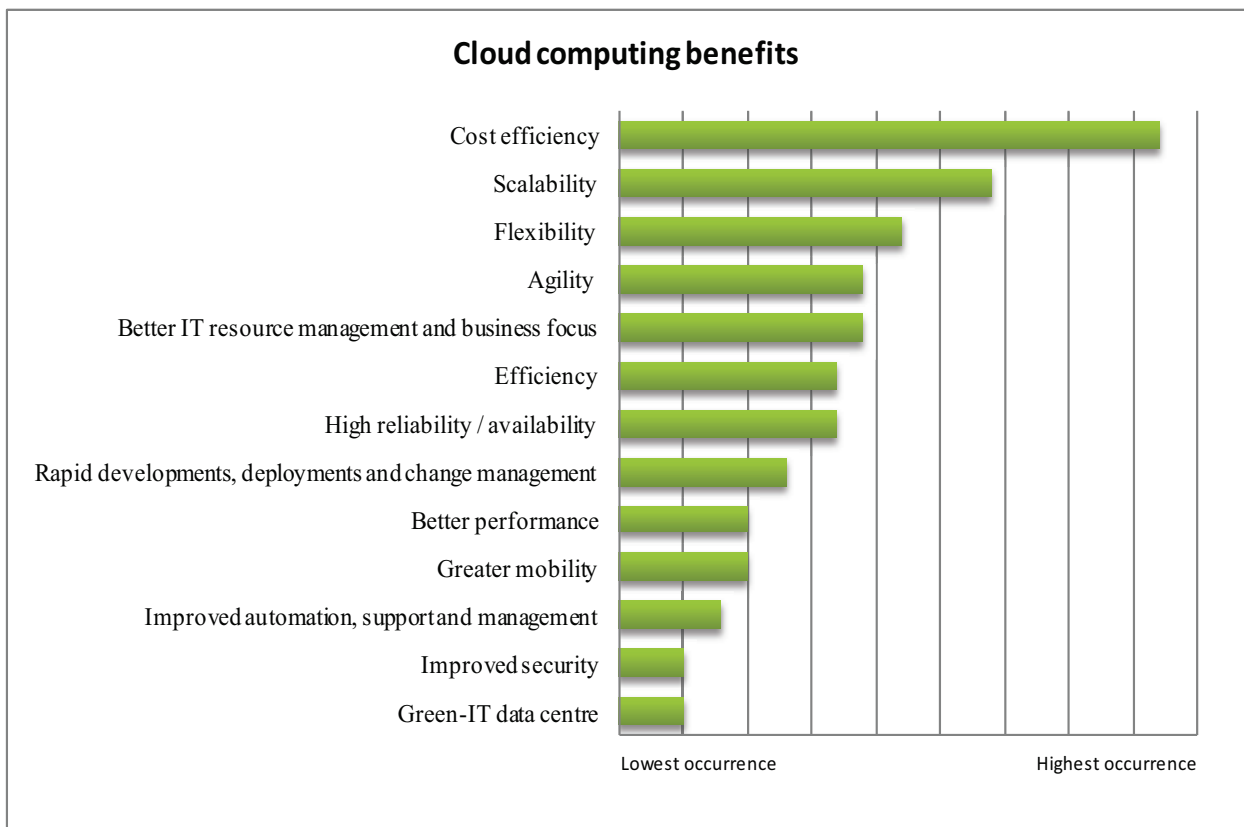
### 3.2 Background

Cloud computing's potential benefits are organisationally contextual and depend on which type of cloud computing services are utilised (Convery 2010:10), for example Software-as-a-service, Platform-as-a-service and Infrastructure-as-a-service. This means that every organisation may not gain every benefit of cloud computing, but has the potential to gain these benefits. Carroll, Van der Merwe and Kotzé (2011:4) have outlined thirteen benefits of cloud computing covered in the literature they reviewed. According to Carroll *et al.* (2011:4),

The literature review included: available subject databases, online library catalogues, published articles, relevant textbooks, industry-specific information and trusted resources from the Internet. The benefits and risks

identified from the extensive literature review were also tested against primary data collected through interviews.

These benefits were then ranked graphically according to their occurring frequency in these sources. **Figure 3.1** illustrates the cloud computing benefits identified by Carroll *et al.* (2011) in their research.



**Figure 3.1: Cloud computing benefits identified by Carroll, Van der Merwe and Kotzé (2011:4)**

Carroll *et al.* (2011:4) will be used as a starting point for identification of the potential benefits of cloud computing for the purpose of this research. This was due to the fact that the benefits identified were derived from a larger literature review on the benefits of cloud computing.

In order to identify the potential benefits of cloud computing, a critical review of the reported research by a further eleven sources was conducted. The eleven authors are: Amazon (2012); Armbrust *et al.* (2009); Cervone (2010); Convery (2010); Corsello (2012); Dhar (2012); Harmon, Demirkan & Raffo (2012); Jadeja & Modi

(2012); Mell & Grance (2011); Ross (2010); and Thomas (2010). This was done in order to identify the most often nominated potential benefits of cloud computing.

**Table 3.1** below shows the thirteen benefits identified by Carroll *et al.* (2011:4) and the eleven sources on which a critical review of the reported research was done. The eleven sources' benefits were tabulated against Carroll *et al.* (2011:4) in order to identify the most prominent potential benefits of cloud computing.

**Table 3.1: Potential benefits of cloud computing from various sources tabulated against benefits identified by Carroll, Van der Merwe and Kotzé (2011:4)**

Potential benefits of cloud computing from various sources tabulated against benefits identified by Carroll <i>et al.</i> (2011:4)													
Sources	Cost efficiency	Scalability	Agility	Better IT resource management and business focus	Efficiency	High Reliability/ availability	Rapid development, deployments and change management	Better performance	Greater mobility	Improved automation, support and management	Improved security	Green IT data centre	Flexible
(Amazon 2012)	✓	✓				✓	✓				✓		✓
Cervone (2010: 164-165)	✓	✓					✓						✓
Corsello (2012:29)						✓							
Convery (2010:10-12)	✓	✓		✓		✓	✓				✓		✓
Dhar (2012:667-673)	✓	✓		✓			✓			✓			
Harmon, Demirkan & Raffo (2012: 121-122)												✓	
Jadeja & Modi (2012:877-878)	✓	✓				✓				✓	✓	✓	
NIST (Mell & Grance 2011:2)	✓	✓							✓				
Ross (2010:8)	✓										✓		
Thomas (2010: 218- 219)	✓	✓											✓
Armbrust, Fox, Griffith, Joseph & Katz (2009:1,4,10)	✓	✓											



Based on the presentation in **Table 3.1** it was found that the benefits *Cost efficiency* and *Scalability* were mentioned most frequently. Followed by *High reliability/ availability*, *Rapid development, deployments and change management*, *Improved security and Flexibility*.

The following benefits that Carroll *et al.* (2011:4) identified, but that were not mentioned by the other authors were *agility, efficiency and better performance*.

Similar benefits were grouped together for the purpose of enhanced readability and clarity. The following concepts were grouped together in **Table 3.1**:

*Scalability*, which in accordance with the characteristics for cloud computing provided by NIST in **Chapter 2** (Mell & Grance 2011:2), includes:

- Elasticity
- Illusion of infinite resources

The benefit of *Cost efficiency*, which are in line with the characteristics for cloud computing provided by NIST (Mell & Grance 2011:2) in **Chapter 2**, includes:

- Cheaper IT costs
- Pay-per use
- Metered use
- Measured service

The benefit *Rapid development and deployments*, which in relation to Amazon (2012); Convery (2010:11) and Dhar (2012:667), includes:

- Easy to start
- Completely controlled
- Higher degree of control
- Ease of use
- Configure based on requirements

In accordance with NIST (Mell & Grance 2011:2) *Greater mobility* includes:

- Broad network access

Additional benefits identified by authors except Carroll *et al.* (2011:4) include:

- Designed for use with other Amazon Web Services (Amazon 2012) (Will be discussed in **Section 3.3.5 Rapid development and deployment**).
- Does not own hardware and/ or does not know location of hardware (Cervone 2010:164-165) (Will be discussed in **Section 3.3.3.1 Reduced ICT costs**).
- Modernisation of business processes (Convery 2010:10-12) (Will be discussed in **Section 3.3.2 Modernisation of business processes**).
- Multi-tenancy (Dhar 2012: 667-673) and resource pooling (Mell & Grance 2011:2) (Will be discussed in **Section 3.3.1.6 Shared resources reduce cost**).
- Disaster management (Jadeja & Modi 2012:880).
- On-demand self-service (Mell & Grance 2011:2) (Will be discussed in **Section 3.3.2 Scalability and flexibility**).
- Enhanced computational and information handling reliability/ Meeting growing computational needs (Ross 2012:8) (Will be discussed in **Section 3.3.8 Improved power, automation and support management**).

These thirteen benefits identified by Carroll *et al.* (2011:4) combined with the additional benefits identified during the critical review of the reported research by the authors (see **Table 3.1**) can be reclassified into ten potential benefits. They are broken down further into sub-benefits, thus providing a more detailed description of the potential benefits of cloud computing.

In particular, this new list differs from the benefits identified by Carroll *et al.* (2011:4) as it includes additional potential benefits and combines others. New potential benefits include *Business continuity and Disaster recovery* as well as the *Modernisation of business processes*. The potential benefits *Scalability and flexibility* have been combined into a single potential benefit, as they are linked.

The potential benefits *Scalability and flexibility* and *Modernisation of business processes* incorporate *IT Resource management and business focus*. In addition, sub-benefits have been identified and have been included under the individual potential benefits. These potential benefits will now be examined in detail.

### **3.3 The ten potential benefits of cloud computing**

After a critical review of the reported research by the authors identified in **Section 3.2**, combined with the areas provided by Carroll *et al.* (2011:4), the following ten most common potential benefits of cloud computing have been identified and integrated:

These potential benefits are:

1. Cost efficiency
2. Scalability and flexibility
3. Modernisation of business processes
4. Availability and reliability
5. Rapid developments and deployments
6. Business continuity and disaster recovery
7. Greater mobility
8. Improved power, automation and support management
9. Improved security
10. Green IT/ Green computing

These benefits can be further broken down into sub-benefits.

#### **3.3.1 Cost efficiency**

*Cost efficiency* refers to the potential cost saving benefits provided by using cloud computing and cloud computing services. These are discussed below in their relevant subsections.

### 3.3.1.1 Reduced ICT costs

Cloud computing utilises cloud service providers to supply hardware and software infrastructure for an organisation. This leads to lower costs on Information Communication Technology (ICT) (Convery 2010:10 and Dhar 2012:668). This can be broken down into: hardware and software.

a) Hardware

b) Software

#### a) Hardware

Cervone (2010:164) identifies an important aspect of cloud computing beneficial to organisations: the organisation does not, in most cases, own the hardware (IT) used to host the cloud services. An example for this is Amazon Elastic Compute Cloud (Amazon EC2), which is a web service designed to provide resizable cloud based compute capacity (Amazon 2012). Often organisations may not even know the actual physical location of the hardware, for example if it is located in another country, as Amazon EC2 service, which allows hosting in multiple separate geographic areas and countries. Amazon provides hosting in a variety of locations from US East, US West to Ireland (EU), Singapore, Tokyo and Sydney (Asia Pacific) to Sao Paulo in South America (Amazon 2012).

#### b) Software

The potential benefit in regards to software, according to Thomas (2010:218), is that an organisation does not have to pay licensing fees, or support and maintenance, to use software provided by the cloud service provider. The organisation pays a usage fee to the cloud service provider. The organisations do not have to purchase any software or hardware to utilise the services. Whilst Thomas (2010:218) states that this may be a cheaper way to acquire and utilise IT services, whether or not it is in fact more cost effective in the long run may be dependent on the individual organisation. The cost factor may be affected by a multitude of factors such as the number of software licences required.

As identified above in **a) Hardware**, multiple hosting in separate geographic locations can be a potential benefit for cloud computing as it can save costs if a server is subject to failure or a disaster in that area. In this case, there will be

backup copies of data in other locations. This in turn saves organisations money that would otherwise be needed for recovery and re-creation of valuable information.

### **3.3.1.2 Delayed upgrades through redistribution of computing resources**

Jadeja & Modi (2012:1) state that the primary goal of cloud computing is to efficiently utilise distributed resources and to integrate them to increase throughput in order to solve extensive computation. Dhar (2012:668) explains this as follows: Due to business processes having fluctuating IT demands their systems are engineered to handle large operations. However, these high demands are seldom met and these resources are wasted. Cloud computing addresses these resource fluctuation requirements through its elastic services, which can be adjusted as the computational need grows.

A large portion of cost savings in cloud computing occurs through utilising the variable transaction demands that exist with a majority of applications. This is done through the reallocation of unused computing cycles, during a slower period of one application to another application that may require more resources at the time. Due to this resource redistribution system, additional hardware costs may be postponed until more computing power is needed overall, rather than for a single application (Cervone 2012:164). The redistribution of resources can affect cloud computing's viability, as an organisation can adjust its resources based on its needs and save on costs.

### **3.3.1.3 Lower implementation costs**

According to Dhar (2012:669), the upfront investment on cloud computing initiatives can be kept minimal. The services allow for rapid deployment of services and infrastructure on demand, which in turn provides further cost cutting benefits to the organisation (Carroll *et al.* 2011:4; Cervone 2010:164).

Convery (2010:64) illustrates this in a case study on the Guardian News & Media (GNM). The GNM chose to utilise Google Apps. This was due to its low costs

achieved by savings from outsourced support, infrastructure and yearly renewable licences at a fixed price.

GNM migrated to Google Apps, more specifically Google Docs and Sites, and then at a later stage migrated their email from Lotus Notes to Google Mail (Gmail). This allowed GNM to negotiate a fixed annual price for a license as well as save on further costs on their internal infrastructure and support fees, as the support is now provided 24/7 by Google. GNM further held only informal training sessions. Due to the similarity between traditional office products and Google Docs, in combination with the easy user interface, GNM believed that regular training sessions would not be necessary. After a few months GNM found Google Docs so successful that they began switching to Google Mail as well (Convery 2010:64).

#### **3.3.1.4 Reduced software costs and application developments**

Costs are reduced in relation to application development (Carroll *et al.* 2011:4). The cloud service provider is able to provide software and / or have specific applications developed to suit an organisation's needs, resulting in this reduction.

Examples of such software include Google Apps (Google Docs and Sites), which were provided to Guardian News & Media (GNM) when they migrated their systems to Google (Convery 2010:63-63). Google, in fact, maintains this software, thus it frees up the organisation from having to keep the software updated (Convery 2010:64).

#### **3.3.1.5 Less IT skills required for implementation**

Cloud computing has a low set up cost for the user and due to the cloud service provider hosting the data, it becomes the service providers' responsibility to maintain their technology. This allows for further cost-cutting benefits to the organisation (Carroll *et al.* 2011:4; Cervone 2010:164) as less IT staff may be needed to help maintain the internal systems and software. An example of this is from Guardian News & Media (GNM), who found that after migrating from Lotus Notes to Google Mail that the support calls to the IT department had declined (Convery 2010:63-64).

Cloud computing adoption can create a steep learning curve for organisations. While less IT skills may be required for and after implementation, additional IT support may at first be needed to train staff. This is seen in a case study analysed by Convery (2010:65-67) on the organisation Melrose Resources plc. The organisation Melrose Resources plc. embraced an Amazon web service and cloud computing approach. The Systems Manager for Melrose Resources plc. found that utilising the cloud required an alternate approach to managing IT services and this required assistance from the service provider.

#### **3.3.1.6 Shared resources reduce costs**

A cloud service provider uses a multi-tenancy model in order to serve multiple clients through the pooling of computing resources. Multi-tenancy refers to a single piece of software run on a server that can be simultaneously used by multiple clients (Dhar 2012:667). This is done through the rapid reallocation of virtual and physical resources, which are distributed and redistributed, based on a client's demands (Mell & Grance 2011:2). This sharing of computer resources and sharing of costs between multiple clients allows for a well-organised use of the cloud infrastructure (Jadeja & Modi 2012:878).

Multi-tenancy does, however, have its own problems: from blacklisting of the service providers' IP addresses, which is marking them for exclusion (Oxford Dictionaries 2013) due to spam attacks (Armbrust *et al.* 2009:18); to the exploitation of vulnerabilities in order to obtain sensitive information from other clients' systems (Cloud Security Alliance 2011:64; Himmel 2012: 40,104). These risks are discussed in detail in **Chapter 4** under **Section 4.3.6 Virtualisation** and **Section 4.3.9 Viability**.

#### **3.3.1.7 Pay-per-use model**

Cloud computing utilises a pay-per-use model, as identified in the characteristics of cloud computing identified by NIST (Mell & Grance 2011:2), which was discussed in **Chapter 2**. Also known as "utility computing", this is where users pay only for what they need and use, similar to water and electricity utilities accounts

(Thomas 2010:218). These resources can be controlled and monitored and then reported to the user and service provider (Mell & Grance 2011:2). This allows organisations to purchase resources only when they are required. It also enables them to start out on a lower level and eliminate any advanced commitment costs (Armbrust *et al.* 2009:1).

Armbrust *et al.* (2009:4) provide examples of utility computing:

- Google AppEngine
- Amazon Web Services
- Microsoft Azure

In an example provided by Convery (2010:67) from a case study on Melrose Resources plc., it could be shown that their on-going costs had decreased by utilising Amazon Web Service (Convery 2010:67).

A pay-per-use system can be a viable benefit for organisations looking to utilise cloud computing, as an alternative to traditional data storage. This is due to the client only having to pay for the space they require. With regard to records management this could be a potential benefit where clients are able to upgrade their storage based on their needs as and when more space is required.

### **3.3.1.8 Decreased operating costs**

Operating costs are costs that the manager has direct control over for the utilisation of resources, for example labour, equipment, systems etc. (Armistead, Bowman & Newton 1994:19). Due to hardware being located off-premises and provided by the cloud service provider, there is a decrease in operational costs. This is due to the elimination of the need to provide power for cooling (to prevent the hardware from overheating) or to providing floor space, or even storage resources (Carroll *et al.* 2011:3).

Furthermore, the cloud service provider hosts cloud-computing software. Thus, this software does not need to be installed on every user's computer, leading to a reduction in maintenance costs (Carroll *et al.* 2011:4). This is illustrated in the case



study conducted by Convery (2010:64), on the Guardian News & Media (GNM) who chose to utilise Google Docs. Google Docs provided them with online documents and spread sheets (see **Section 3.3.1.3**).

In conclusion, the potential benefit of *Cost efficiency* seems one of the most promising potential benefits for cloud users. The real world examples provided by Convery (2010:63, 65) on the Guardian News & Media (GNM) and Melrose Resources plc. provide evidence on the cost saving potential of cloud computing in hardware (infrastructure), software, as well as on training costs. These infrastructure saving costs provide an excellent benefit, with regard to cloud computing's viability when considering it as an alternative for traditional data storage and records management.

### **3.3.2 Scalability and flexibility**

*Scalability* means that the resources of cloud computing can be scaled up or down (increased or decreased) based on users' needs (Convery 2010:10-11). *Flexibility* refers to the user being able to acquire the resources they need, when they need them, as the resources such as storage capacities and computing power appear to be unlimited (Convery 2010:10-11). These benefits are broken down into:

- Effective resource monitoring (Jadeja & Modi 2012:878; Mell & Grance 2011:2).
- Rapid elasticity of resource provisioning (Armbrust *et al.* 2009:1; Mell & Grance 2011:2).

*Scalability and flexibility* are potential benefits of cloud computing because cloud applications are hosted on virtual servers. Organisations are able to start out with one virtual server, then expand or retract the number of servers or resources they need within a few minutes. This enables an increased amount of *Scalability and flexibility* to organisations requiring extra resources for a short period of time. This may occur during a large work project, or seasonal work periods (Cervone 2010:164, Convery 2010:10). This equips organisations utilising cloud computing with a competitive advantage providing improved performance on resources, as well as higher levels of reliability and scalability (Carroll *et al.* 2011:3).

However, although cloud computing providers may state that they are able to provide unlimited resources on demand, the cloud provider may not have the ability to scale these resources (increase or decrease) at a fast enough pace. The available speed of scaling resources, needs to be a known and be a proven measure for the organisation (Convery 2010:11). Due to operational requirements, for example data storage and records management, organisations can require a large increase in resources quickly. If the cloud service provider cannot keep up with the required speed of scalability, it can lead to data loss or even a halt in business proceedings. It is therefore, imperative to ascertain prompt scalability early on.

### **3.3.2.1 Effective resource monitoring**

The utilisation of a measured service (pay-per-use model) enables the monitoring of cloud-computing resources. This allows for greater control and transparency for the client and the cloud service provider on resource utilisation. Performance can thus be monitored allowing resources to be adjusted based on requirements (Jadeja & Modi 2012:878; Mell & Grance 2011:2).

An organisation may need to keep a close eye on the usage of cloud services, as the services are metered costs and if necessary, usage may have to be restricted. This would ensure that the benefits of utilising the cloud are not overshadowed by the costs (Convery 2010:11). Monitoring of resources is essential for organisations that wish to utilise the cloud for data storage and records management, as the costs may rise as more resources are required over time. This in turn can affect the cloud's perceived viability over time.

### **3.3.2.2 Rapid elasticity of resource provisioning**

Cloud service providers allow for on-demand adjustable resources. This creates the illusion of infinite resources being available to the client. Organisations do not need to plan in advance to calculate their resource requirements. The service provider is able to provide resources when required. Furthermore, these

resources can be automatically adjusted when required (Armbrust *et al.* 2009:1; Mell & Grance 2011:2).

As previously stated in **Section 3.3.2.1**, although a cloud service provider may claim to provide unlimited or infinite resources on demand, their ability to scale these resources needs to be determined for the client (Convery 2010:11).

The potential benefit *Scalability and flexibility* is a prominent feature of cloud computing. There may be minor concerns such as having to monitor resources to ensure that costs do not rise unnecessarily. This is however a minor hindrance in comparison to the bigger potential benefit. The ability to scale resources up or down based on one's flexible needs can save on costs. Organisations should however, determine the pace at which these resources can be scaled to ensure that they are selecting a cloud service provider that can meet their needs.

### **3.3.3 Modernisation of business processes**

*Modernisation of business processes* as a potential benefit refers to a change from traditional methods to modernising business processes, such as no longer having to acquire software licences for a provider's proprietary product. Instead the cloud service consumer is able to select new innovative applications and services, which address their needs and are provided by the cloud service provider, for example Software-as-a-Service (SaaS) (Convery 2010:12). This is advantageous for short and long-term projects, which often involve procuring licenses for business software and relating them to the providers' proprietary products (Convery 2010:12).

This ability to integrate various cloud services to address specific needs can be beneficial, for example, integrating customer relationship management services, which are applications that allow for the management of present and future customers (Salesforce 2013), with cloud based security and performance monitoring. This forms a customisable service that can help to have a beneficial impact on organisational productivity and efficiency (Convery 2010:12).

However, Convery (2010:11-12) contradictorily states that due to these services and applications being created to service a wide customer base there is a decreased ability of customisation. Unfortunately catering for their individual needs can lead to a lack of standardisation for the cloud computing's services. This lack of standardisation can cause issues with interoperability and even raise costs and implementation time for the client's products (Convery, 2010:12). It is therefore, important for an organisation to discuss any services with the cloud service provider before making a decision. This should be done in order to determine if there are services and applications that can be tailored to suit their needs. If it is not done it could affect cloud computing as a viable alternative to traditional data storage and records management. If the specific needs of an organisation cannot be met, then cloud computing may not be the viable choice.

The potential benefit *Modernisation of business processes* allows integrated cloud services to address individual organisational needs. Furthermore, this customisable service can positively affect productivity and efficiency. Organisations should however, identify and discuss their needs with the cloud service provider to ensure that they can be met before they make a decision on whether or not to utilise cloud computing as an alternative to traditional storage for records.

#### **3.3.4 Availability and reliability**

*Availability* as a concept refers to cloud computing's ability to provide always-accessible data. *Reliability* in the context of a potential benefit of cloud computing refers to the reliability of service (Convery, 2010:11). If a cloud service provider's server fails, this would not necessarily affect a client because of access to ample computing resources. The service provider would be able to switch automatically to another server. The clients' data is usually stored in multiple geographic locations in order to prevent information loss, server outages and for disaster recovery. It is due to this practice, that a majority of cloud service providers offer 99.9% availability (Convery, 2010:11; Jadeja & Modi, 2012:877).

The utilisation of cloud computing creates an always available or always “on” feature for access because a cloud service provider hosts and runs the applications. This allows work to be done at any time and in any location through the Internet (Corsello, 2012:29).

It needs to be noted that cloud service providers do have service outages. When outages do occur, the client does not control the restarting of these services. Often, if the cloud service provider cannot meet the stipulations of the Service Level Agreements (SLAs), then the customer may only be recompensed in free service time (Convery 2010:11). These outages can draw into question the viability of cloud computing especially for data storage and records management. For example:

- In 2009, lightning struck one of Amazon’s Elastic Compute Cloud service data centres causing damage to a power unit, which affected some users. These users were, however, able to launch replacement instances in other US Region Availability Zones to continue work (Donoghue 2009).
- In February 2008, the Amazon service S3 (Simple Storage Service) was down due to an overload in processing authentication requests, which pushed the system past its capacity before more resources could be allocated (Dignan 2008).

These examples illustrate that when services are down business operations can be affected. This should be carefully considered, as it may not be viable for every organisation to take such a risk. Despite the high availability and reliability of service, there can still be outages that may be unacceptable for some organisations or applications.

### **3.3.5 Rapid development and deployment**

*Rapid development and deployment*, as a benefit for cloud computing, refers to cloud computing’s ability to provide pre-tested, configured and installed software. This software is made instantly available once the client signs up for the cloud service (Convery 2010:11). Cloud service providers supply resources such as the

hardware and in some cases the software to their clients. Therefore, providers have the ability to deploy new applications and/or services much quicker than the client would be able to on their own. In cloud computing, resources are on-demand self-service features, wherein the client simply selects the services they require and provisions where they are needed. Examples of these resources can include network storage and server time. Another potential benefit is that in many instances, there is no long-term commitment. A client can test out a cloud service and cancel it if it does not address their needs (Convery 2010:11; Mell & Grance 2011:2). This rapid deployment and resource management feature allows organisations to adapt to fluctuations based on their needs and be able to continue business operations with minimal hindrance.

### **3.3.6 Business continuity and disaster recovery**

Cloud service providers handle information storage. The service provider is responsible for disaster recovery of clients' information should anything happen. Due to the cloud service provider replicating information to prevent outages and server failures, the availability of information is improved if a disaster does occur as the information is replicated across various servers (Convery 2010:12).

In a case study of Melrose Resources plc. a natural resource company found that utilising cloud services and its decentralised storage facility provided the organisation with excellent automatic replication of information servers. This was found to be a quick and cost effective way to cater for business continuity and disaster recovery in case of any system failures (Convery 2010:67). The *business continuity and disaster recovery* capabilities are positive examples of the viability of cloud services for data storage and records management, in particular with regard to the automatic replication of data and its decentralised storage.

### **3.3.7 Greater mobility**

Cloud computing allows for broad network access. A client is able to access cloud computing services over the Internet, through a browser. This access is achievable using multiple devices with Internet capabilities, such as computers, mobile phones or tablets. Services are available regardless of the clients'

geographic location (Convery 2010:11; Jadeja & Modi 2012:877; Mell & Grance 2011:2).

This was a key consideration factor for the Guardian News & Media (GNM) who needed to implement a solution to allow document collaboration across multiple and dispersed locations. They decided on migrating to Google Apps and Google Mail (Convery 2010:63-64).

Access to data from any location via the Internet is an advantage for any organisation that has employees who may work from various locations. Access to stored data from any locations is a great potential benefit for records management, as they can be accessed, updated and stored from anywhere. This can help eliminate reduced copies of records and can be an excellent factor when accessing cloud computing's viability for records management, where individuals can collaborate and share documents with one another, despite their geographic location. This is enhanced further through access over multiple devices with Internet capabilities.

### **3.3.8 Improved power, automation and support management**

*Improved power, automation and support management* refers to cloud computing's processing power, resource capabilities, task automation and support management.

#### **3.3.8.1 Improved power and calculation ability**

Cloud computing services have nearly limitless resources and increased processing capabilities. This allows for larger tasks, such as large computations, to be performed at a much faster pace saving time and money. This can signify time saving on a considerable scale. A single system may take hours to run, however cloud services are able to perform identical tasks in minutes. This in turn allows for projects on a deadline to be completed rapidly (Mell & Grance 2011:2; Ross 2010:19).

### **3.3.8.2 Improved automation and support management**

Cloud computing services utilise a multi-tenancy model. This provides the benefit of reducing maintenance on services such as repairing, upgrading and troubleshooting. In addition, it allows the cloud service provider to manage their resources more efficiently (Dhar 2012:668). Due to cloud computing's on demand self-service feature for resource procurement, resource management can be automated based on a client's demands, for example increasing or decreasing storage size based on the clients' requirements (Mell & Grance 2011:2).

Automation does unfortunately have its own risks, for example when utilising an automation script to perform a task. If the script contains an error, then that error is replicated (Himmel 2012:104-105). The risks will be analysed in detail in **Chapter 4, Section 4.3.6.2 Automation and standardisation.**

*Improved power, automation and support management* identifies cloud computing's potential to handle larger workloads through its increased power and calculation ability provided by its near limitless resources and processing power. Furthermore, its improved level of automation helps reduce maintenance and speed up resource procurement.

### **3.3.9 Improved security**

The potential benefits offered by cloud security can be superior to normal computing systems. The cloud service provider has increased resources (such as increased IT skills) that may be dedicated to solving issues of security, thus providing a level of service that customers cannot afford on their own. The service provider is able to provide greater expertise and experience in information security practices to individual customers (Convery 2010:11; Jadeja & Modi 2012:877). Resources can be dedicated to improving application security processes and improving the network, as security measures will be easier and more cost effective to put into place on a larger scale. In particular, there are defence measures such as hardening of virtual instances, patch management and virus protection, which can be implemented rapidly over the entire cloud provider's infrastructure. This is done through automation and virtualisation, which enables the fast execution and



replication of security configurations for the service provider. In addition, the cloud service provider is able to utilise early incident detection mechanisms, which enables them to respond to security incidents and breaches much faster (Convery 2010:11; Jadeja & Modi 2012:877). Dedicated security resources from a cloud service provider can be a potential benefit for records management. Improved security can help prevent the loss of sensitive documents that have been shared within an organisation over the Internet.

With cloud computing, the client transfers the responsibility for information security to the cloud service provider. However, they are still responsible for ensuring that the service provider is able to provide the necessary security, as well as, for encryption of the data. Unfortunately, by transferring the responsibility of security to the cloud service provider, the client loses some control. This loss of control can affect the organisation's ability to comply with regulatory and even legislative procedures (Convery 2010:13-15). Security is a large concern for cloud services and an organisation considering its use needs to pay special attention to the security of their data (Convery 2010:13-15; Jadeja & Modi 2012:878).

Furthermore, there are privacy concerns with regard to cloud computing and security, in particular with regard to confidential information (Jadeja & Modi 2012:878). Other risks and challenges to cloud security include privileged user access (Heiser & Nicolett 2008:2); security attacks (Opala 2012:47); identification authentication and access management (Cloud Security Alliance 2011:136).

According to the Cloud Security Alliance (CSA) (2011:103) which is a not-for-profit organisation (2013), cloud based applications, in having to provide their own security, will face an increased amount of threats compared to applications in a traditional data centre. Thus, increased security practices must be adhered to when migrating or developing cloud applications. Security risks are discussed in detail in **Chapter 4 Section 4.3.3 Security**.

In conclusion *Improved Security* for cloud computing is a potential benefit due to cloud service providers having the capacity to dedicate large amounts of resources (e.g. IT skills) to security. Cloud computing has defence measures in

place, such as patch management and the hardening of virtual instances that can be activated across the entire cloud infrastructure, at a rapid speed. In addition, cloud service providers utilise early incident detection mechanisms that allow them to respond to incidents faster.

### **3.3.10 Green IT**

The practice of “*Green IT*” or “green computing” emphasises the reduction of energy costs of IT operations (Harmon, Demirkan & Raffo 2012:121-122). The means to achieve this include, for example: decreasing the use of energy by retiring old computer systems, or the adoption of more efficient cooling systems and hardware (Deloitte Touche Tohmatsu 2009: 3-4). “Going Green” is becoming a focus area of organisations, as large enterprises are looking at reducing their negative impact on the environment (Deloitte Touche Tohmatsu 2009:3). Companies such as IBM, who according to (Baroudi 2009:8), have been concerned with green IT for years, are a founding member of the Green Grid, a group of organisations pushing for greater energy efficiency in business computing and data centres.

When using cloud computing, outsourcing to the cloud service provider enables the efficient use of power through resource sharing between clients. Sharing of resources in cloud computing contributes to reducing cooling, storage, power and space through utilising a multi tenancy system. It thus creates a more environmentally friendly data centre (Carroll *et al.* 2011:4; Ross 2012:19). Overall, it appears that if organisations are concerned with *Green IT*, then cloud computing’s energy saving through resource sharing makes it a viable option for data storage and records management.

### **3.4 Summary**

In this chapter the ten potential benefits of cloud computing were identified, as were the sub-benefits of each. After a critical analysis the reported research of eleven sources was tabulated against the thirteen benefits identified by Carroll *et al.* (2011:4) in **Table 3.1**.

**Table 3.2** provides a summary of the ten potential benefits identified in this chapter as well as examples of their corresponding benefits.

**Table 3.2: Ten potential benefits of cloud computing**

Ten Potential Benefits of Cloud Computing	Examples
1) Cost efficiency	Savings on infrastructure such as: hardware, software
2) Scalability and flexibility	Easily adjustable resources based on fluctuating needs
3) Modernisation of business processes	Specific services to match individual business needs
4) Availability and reliability	99.9% Server up time
5) Rapid developments and deployments	Faster application and service deployment
6) Business continuity and disaster recovery	Improved data recovery through multiple site hosting
7) Greater mobility	Multiple device accessibility from any location through the internet
8) Improved power, automation and support management	Increased system capabilities for tasks e.g. computational power
9) Improved security	Dedicated security with increased response capabilities
10) Green IT/ Green computing	Lower energy costs and lowering carbon footprint

(Adapted from Amazon (2012), Armbrust *et al.* (2009), Cervone (2010) Convery (2010), Corsello (2012), Dhar (2012), Harmon, Demirkan & Raffo (2012), Jadeja & Modi (2012), Mell & Grance (2011), Ross (2010), Thomas (2010), and Carroll *et al.* 2011).

The potential benefits and sub-benefits were subsequently analysed and some were found to have a potential impact on records management. The strongest potential benefit for improving records management was *Business continuity and disaster recovery*, where records can be backed up to multiple servers and still be accessible, if a disaster occurs. *Greater mobility* stood out as the most applicable potential benefit allowing for access to records regardless of the user's geographic location, as well as through any Internet-capable devices. In addition, various case

studies and examples were utilised when discussing these potential benefits to illustrate their potential impact on organisations.

These potential benefits are further explored in **Chapter 6**, when discussing cloud computing's viability for records management. **Chapter 7** deals with the methodology of the research. The potential benefits discussed in this chapter are considered, when analysing the case study findings in **Chapter 8**.

The potential benefits of cloud computing, identified in this chapter, draw attention to the fact that cloud computing capabilities are growing and have the ability to cater for multinational organisations by providing access through the Internet to a multitude of geographically hosted data. This is demonstrated in the various case studies and examples included in this chapter. Nonetheless, although cloud computing has many potential benefits, there are still risks that need to be considered in detail before being able to determine cloud computing's viability, in particular for records management. **Chapter 4** discusses the challenges associated with cloud computing.

## Chapter 4 Risks and challenges associated with cloud computing

### 4.1 Introduction

In **Chapter 3**, the potential benefits and sub-benefits of cloud computing were identified through a critical analysis of the reported research. In this chapter, the risks and challenges associated with cloud computing are identified in the same manner. The risks and challenges of cloud computing are then examined, integrated and organised into ten risk categories and additional sub-risks. These sub-risks are analysed to provide a more detailed view on the specific risks of cloud computing. In doing so, information will be provided in order to help answer the research question:

- What are the challenges and risks associated with cloud computing?

The Oxford Dictionary (2013) defines the term “risk” as “a situation involving exposure to danger” and “a person or thing regarded as a threat or likely source of danger”. The dictionary further defines the term “challenge” as a “task, or situation that tests someone’s abilities” and “a call to prove or justify something” (The Oxford Dictionaries 2013).

This coincides with the Cambridge Business English Dictionary Online (2014), where a “risk” refers to the possibility of a danger or bad instance occurring. It also refers to a “challenge” as a situation, a job or duty, which presents difficulty because a large amount of determination, effort or skill is required in order for success to be achieved (Cambridge Business English Dictionary Online 2014). Based on these definitions, the terms “risks” and “challenges” will be used interchangeably for cloud computing. In the context of this study, a risk and challenge are defined as:

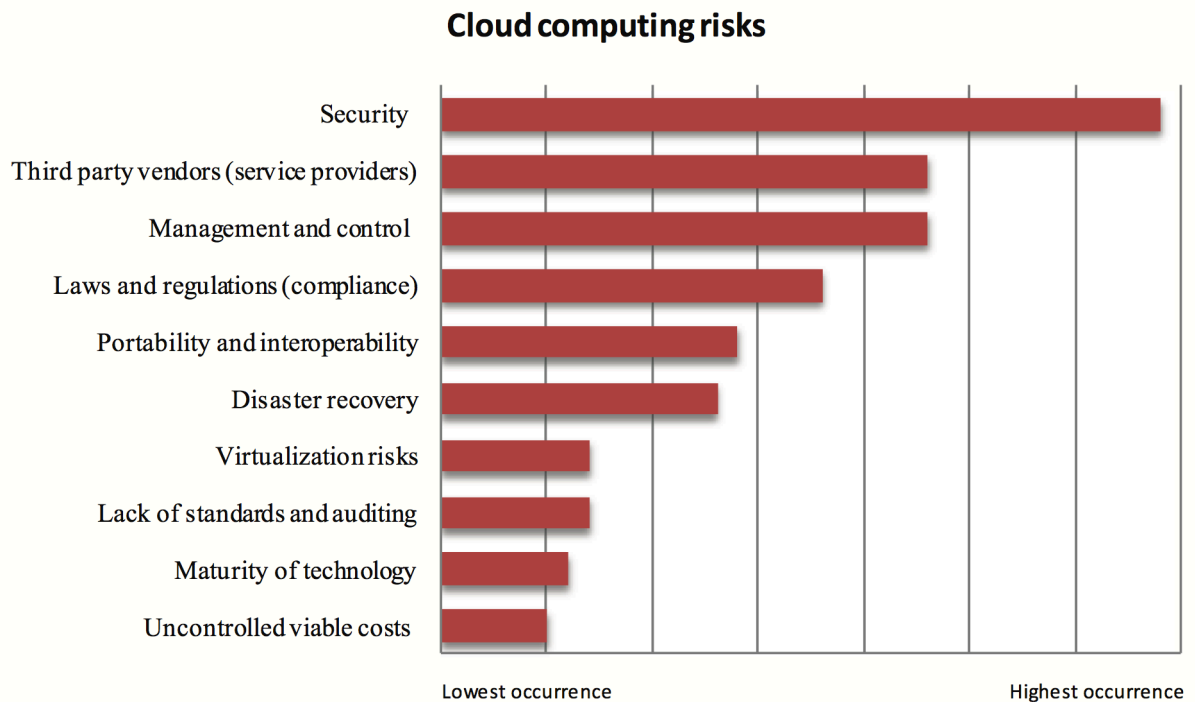
*The threat, or danger that the use of cloud computing can pose to tasks or situations, which might test cloud computing’s abilities by presenting difficulties in allowing for success to be achieved (such as what needs to be overcome to allow cloud computing to prove or justify itself).*

Understanding the risks and challenges associated with cloud computing is vital in assessing its viability, as an alternative method for records management.

## **4.2 Background**

According to Convery (2010:13), the outsourcing of information storage and services to the cloud creates challenges; in particular, for information security, the availability and security of the cloud service providers' systems. Additionally, Convery (2010:13) states that there are other challenges such as network security, infrastructure and unauthorised access. However, these are not new challenges to information security managers and IT departments. Some challenges are, however, specific to the cloud, such as interoperability and availability.

In order to evaluate the viability of cloud computing as an alternative to traditional storage and records management, a better understanding of its risks and challenges is required. As in **Chapter 3**, Carroll *et al.* (2011:4-5) will be used for the identification of the crucial points on this topic of risks, to be discussed in this chapter. The risks identified were derived from a larger literature review on the risks of cloud computing, thus adding to the range of this research. **Figure 4.1** illustrates the cloud computing risks identified by Carroll *et al.* (2011:4-5) in their research ranked graphically, according to their frequency of occurrence.



**Figure 4.1: Cloud computing risks identified by Carroll, Van der Merwe and Kotzé (2011:4-5)**

For the purpose of identifying the most often nominated risks and challenges of cloud computing, a critical review of the reported research by a further sixteen sources was conducted. These sixteen sources are: Armbrust, Fox, Griffith, Joseph & Katz (2009); Biggs & Vidalis (2009:2); Bouayad, Blilat, El Houda Mejhed & El Ghazi (2012:30); Cervone (2010:165); Chaput & Ringwood (2010:243); Cloud Security Alliance (2011:23-25); Convery (2010:10-12); Gagliardi & Muscella (2010:261); Gellman (2009:5); Heiser & Nicolett (2008:2-5); Himmel (2012:101-110); Mollah, Islam & Islam (2012:4); Onwubiko (2010:266); Opala (2012:47); Thomas (2010:219); and Velte, Velte & Elsenpeter (2010:36).

**Table 4.1** below shows the ten risks identified by Carroll *et al.* (2011:4-5) and the sixteen sources which were critically reviewed for the reported research. The risks and challenges identified by the sixteen sources were tabulated against those of Carroll *et al.* (2011:4), in order to identify the most prominent risks and challenges of cloud computing.

**Table 4.1: Risks and challenges of cloud computing from various sources tabulated against risks identified by Carroll, Van der Merwe and Kotzé. (2011:4-5).**

Risks and challenges of cloud computing from various sources tabulated against risks identified by Carroll <i>et al.</i> (2011:4-5)										
Sources	Security	Third party vendors (service providers)	Management and control	Laws and regulation (compliance)	Portability and interoperability	Disaster recovery	Virtualisation risks	Lack of standards and auditing	Maturity of technology	Uncontrolled viable costs
Cloud Security Alliance (2011: 23-25)	✓		✓	✓	✓	✓	✓	✓		
Convery (2010:10-12)	✓		✓	✓	✓					
Heiser & Nicolett (2008:2-5)	✓			✓		✓	✓	✓		
Himmel (2012:101-110)	✓			✓			✓			✓
Chaput & Ringwood (2010:243)	✓		✓	✓	✓	✓		✓		
Cervone (2010:165)	✓			✓				✓		
Onwubiko (2010:266)	✓			✓		✓	✓	✓	✓	
Thomas (2010:219)	✓			✓				✓		
Gagliardi & Muscella (2010:261)	✓			✓	✓		✓	✓		
Biggs & Vidalis (2009:2)	✓			✓					✓	
Bouayad, Bilal, El Houda Mejhed and El Ghazi (2012:30)	✓			✓		✓	✓			
Mollah, Islam and Islam. (2012:4)	✓		✓	✓			✓	✓		
Velte, Velte and Elsenpeter (2010:36)	✓			✓						✓
Opala (2012:47)	✓			✓			✓	✓		✓
Armbrust, Fox, Griffith, Joseph and Katz (2009)	✓			✓	✓			✓		✓
Gellman (2009:5)	✓			✓				✓		



The information from **Table 4.1** indicates that the risks and challenges, such as *security, laws and regulation (compliance)* were mentioned most frequently. Followed by *lack of standards and auditing, virtualisation risks* and *disaster recovery*. The only risk identified by Carroll *et al.* (2011:4) not mentioned by the other authors was *third party vendors (service providers)*.

Similar risks and challenges were grouped together for the purpose of enhanced readability and clarity. The following concepts were grouped together in **Table 4.1**:

*Lack of Standards and auditing*, which in accordance with Bouayad, *et al.* (2012: 30); Cervone (2010:165); Cloud Security Alliance 2011:103,162; Heiser & Nicolett (2008:3); Mollah, *et al.* (2012:4); and Opala (2012:46), includes:

- Investigative support
- Open standard
- Auditability

*Management and control*, according to Chaput & Ringwood (2010:253); Cloud Security Alliance 2011:30); Convery (2010:13-16) and Mollah, *et al.* (2012:4), includes:

- Governance and Enterprise Risk Management
- Loss of governance
- Integration and management
- Freedom
- Governance structure

The risk and challenge of *Security*, which in relation to Bouayad, Blilat, El Houda Mejhed & El Ghazi (2012:30); Cloud Security Alliance (2011:136); Chaput & Ringwood (2010:246-7); Convery (2010:13-16); Heiser & Nicolett (2008:2); Himmel (2012:102-105); Mollah, *et al.* (2012:4); Opala (2012:47); Onwubiko (2010:277); and Velte *et al.* (2010:36), includes:

- Identity authentication and access management
  - Privileged User Access
- Authentication and Authorization

- New Surface of Attacks and Vulnerabilities
- Integrity and confidentiality of information
- Encryption and key management / Cryptographic keys
- Security as a Service
  - Transparency
- Application security
- Traditional Security, Business Continuity and Disaster Recovery
  - Recovery

*Virtualisation*, which in line with Armbrust (*et.al* 2009:17); Bouayad *et al.* (2012: 30); Cloud Security Alliance (2011:64); (Himmel 2012: 40,104); and Mollah, *et al.* (2012:4), includes:

- Multi-tenancy
- Hypervisor risks/security
- Automation and standardization
- Privacy
- Performance unpredictability

The risk and challenge of *Laws and regulation (compliance)*, which in keeping with Armbrust *et.al* (2009:15); Bouayad *et al.* (2012: 27); Chaput & Ringwood (2010:243); Cervone (2010:165); Cloud Security Alliance (2011: 23-25); Convery (2010:13); Gellman (2009:5); Heiser & Nicolett (2008:3); Himmel (2012:101-110); Onwubiko (2010:266-279); and Thomas (2010:219), includes:

- Hosting laws / data location
- Legal Issues: Contracts and Electronic Discovery
- Compliance and Cyber Forensics
- Compliance and e-discovery
- Service Level Agreements

*Portability and interoperability of cloud services*, in agreement with and Armbrust *et.al* (2009:15) and Convery (2010:13) include:

- Information retrieval and destruction (exit strategy)
- Vendor/Data lock-in

Additional risks and challenges identified by authors, except Carroll *et al.* (2011:4-5) include:

- Availability and reliability of service (Armbrust *et.al* 2009:14) (will be discussed in **Section 4.3.10 Availability and reliability**)
- Viability (Armbrust *et.al* 2009:17; Heiser & Nicolett (2008:4); (will be discussed in **Section 4.3.9 Viability**)
- Support in reducing risk (Heiser & Nicolett 2008:4) (will be discussed in **Section 4.3.5 Incident response, notification and remediation**)
- Enterprise Risk Management (Cloud Security Alliance 2011:30; Convery 2010:15) (will be discussed in **Section 4.3.7 Governance and Enterprise Risk Management**)
- Information Management and Data Security (Cervone 2010:165; Cloud Security Alliance 2011:65; Convery 2010:34) (will be discussed in **Section 4.3.2 Legality and auditability**)
- Data centre operations (Cloud Security Alliance 2011:81,94,162; Himmel 2012:108) (will be discussed in **Section 4.3.3 Security and Section 4.3.5 Incident response, notification and remediation**)
- Incident response, notification and remediation risk (Chaput & Ringwood (2010:254) (will be discussed in **Section 4.3.5 Incident response, notification and remediation**)
- Endpoint access (Himmel 2012:106-107) (will be discussed in **Section 4.3.4 Everywhere accessible data**)
- Massive Amount of Data Accessible Everywhere (Himmel 2012:107) (Will be discussed in Section 4.3.4 Everywhere accessible data)
- Human factors (Himmel 2012:47-48) (will be discussed in **Section 4.3.3 Security**)
- Concentrated attack value (Himmel 2012:108) (will be discussed in **Section 4.3.3 Security**)
- Privacy (Chaput & Ringwood (2010:243; Thomas 2010:220) (Will be discussed in in **Section 4.3.2 Legality and auditability, Section 4.3.3 Security, Section 4.3.5 Incident response, notification and remediation and Section 4.3.6 Virtualisation**)

- Denial of service attacks (Armbrust *et.al* 2009:14) (will be discussed in **Section 4.3.3 Security**)
- Scaling quickly (Armbrust *et.al* 2009:17); (will be discussed in **Section 4.3.9 Viability**)
- Reputation fate sharing (Armbrust *et.al* 2009:17); (will be discussed in **Section 4.3.9 Viability**)
- Data ownership (Onwubiko 2010:277) (will be discussed in **Section 4.3.8 Portability, interoperability and data lock-in**)
- Hackers (Velte *et al.* 2010:36) (will be discussed in **Section 4.3.3 Security**)
- Bot attackers (Velte *et al.* 2010:36) (will be discussed in **Section 4.3.3 Security**)

These ten risks identified by Carroll *et al.* (2011:4) combined with the additional risks and challenges identified during the critical review of the reported research by other sources (see **Table 4.1**) can be reclassified into ten risks and challenges. They are broken down further into sub-risks, thus providing a more detailed description of the risks and challenges associated with cloud computing.

New risks and challenges include *incident response, notification and remediation* as well as *viability, availability and reliability*. The risk, laws and regulations (compliance), lack of standards and auditing have been combined and reclassified into the following risks and challenges: *compliance, legality and auditability*; as they can overlap with each other. The risk portability and interoperability has been widened to include data lock-in, making it, *interoperability, portability and data lock-in*. The risks management and control have been reclassified to include *governance and enterprise risk management* and finally, the risk and challenge of *everywhere accessible data* has been included. In addition, sub-risks have been identified and have been included under the individual risks and challenges. These risks and challenges will now be examined in detail.

### **4.3 The ten risks and challenges associated with cloud computing**

The following ten most common risks and challenges associated with cloud

computing have been identified and integrated for the purpose of this research. These risk and challenge areas are:

1. Compliance
2. Legality and auditability
3. Security
4. Everywhere accessible data
5. Incident Response, Notification and Remediation
6. Virtualisation
7. Governance and enterprise risk management
8. Interoperability, portability and data lock-in
9. Viability
10. Availability and reliability

These can be further broken down into sub-risks.

#### **4.3.1 Compliance**

The Cloud Security Alliance (2011:46) defines compliance as:

...the awareness and adherence to obligations (e.g. corporate social responsibility, applicable laws, ethical guidelines), including the assessment and prioritization of corrective actions deemed necessary and appropriate.

According to the Queensland Government (2013a), if a business is utilising an overseas cloud service provider, they need to be aware of the regulation requirements and legislation pertaining to that specific geographic area. If cloud computing is used for storage and utilisation of personal information, there can be an impact on compliance issues. One such example is in the United Kingdom, with regard to the Data Protection Act 1998:

The UK Data Protection Act 1998 provides an outline of the duties and rights, which need to be adhered to in order to protect personal data. This outline is used to create a balance between the individuals' right to privacy and an organisation's need to collect and utilise personal data for business

use (ICO n.d:2). The issue of compliance with cloud computing arises in relation to:

- The stored location of the information on the providers' servers; and
- Proving that the cloud service provider has the necessary security in place, for the protection of this data (Convery 2010:13).

The UK Data Protection Act 1998 calls for personal information to not be transferred to a country outside the European Economic Area, unless that country is able to provide a suitable level of protection for the individual's freedom and rights when the personal data is processed (ICO n.d:9). However, this particular *Compliance* issue can be addressed by certain cloud service providers, who allow their customers to select which countries they would like their data stored in (Convery 2010:35).

An update to the Australian Privacy Act 1988 now follows a similar path where stored personal information has to adhere to a set of Privacy Principles. If information is stored in a different legal jurisdiction the organisations will now have to draw up a contract to ensure that the stored personal information adheres to these Privacy Principles (Australia 2014:299).

Cloud computing's adoption may be increased if issues of *Compliance* and *Security* are attended to through a contractual delegation. There are however, only a number of pre-existing regulations concerned with cloud deployments and virtualised environments. A cloud client needs to have a thorough grasp of the interaction of the regulatory environment with cloud computing, as auditors can question them to prove organisational compliance (Cloud Security Alliance 2011:45).

When a client moves data to the cloud, certain security processes may be affected with regard to compliance with certain standards (Convery 2010:13). Due to the fact that the case study is based on an Australian business office, the Australia laws and standards will be examined, in particular with regard to the state of Queensland (see **Chapter 6 Section 6.3**).

In general, existing compliance and information security standards may not be applicable as they were not designed with cloud computing in mind. For example, the owner of the data may be required to identify the physical location of the stored data. However, because it is on a multi-tenant system, this may not be possible, which can cause failure to achieve a certification of compliance (Convery 2010:13). The National Archives of Australia (2013b) does however endorse a variety of international standards that need to be adhered to, which directly relate to records and information management. For example, AS ISO 15489 is an Australia and an international records management standard. It is used to provide a descriptive benchmark standard to help organisations evaluate their records management systems and practices. The standard provides guidance towards the creation of records procedures, its policies and its systems and process. It caters for records in all types of format. The standard should be used to help an organisation, from the creation and capture, to the management of their records, in accordance with legal requirements. (National Archives of Australia 2013b). ISO standards and records management compliance issues are discussed in detail in **Chapter 6: Cloud computing's viability for records management.**

Taking the above into account, it is clear that *Compliance* and legality are big challenges for cloud computing. Clients may not wish to do business with an organisation that does not comply with international standards or with legal requirements. (This is discussed in **Section 4.3.2 Legality and audibility.**) Ultimately, it is important for each organisation to investigate what standards affect them and whether or not they can comply with these standards when utilising cloud computing.

#### **4.3.2 Legality and auditability**

*Legality and auditability* refer to whether or not an organisation is operating in accordance with the law and, if inspected, be held accountable. *Legality and auditability* are great challenges for cloud computing. Organisations need to comply legally with acts and regulations in their home country. However, with cloud computing, data can be hosted offshore, in various geographic locations and jurisdictions. This creates further legal implications requiring consideration, as data

hosted in those countries are subject to local laws. The specific laws and regulations related to cloud computing in Australia are discussed in **Chapter 6**. These are applicable to this research study conducted on an Australian-based organisation.

The following legal issues represent challenges for cloud computing use:

#### **4.3.2.1 Hosting laws**

Hosting laws, as a risk, have been broken down into the following subsections for enhanced clarity:

##### **a) Hosting locations**

A unique feature of cloud computing is its data hosting, which can be based in various locations worldwide (Heiser & Nicolett 2008:3 and Thomas 2010:219). However, information that is hosted in the cloud is subject to the jurisdiction of the country where the data is being physically hosted.

This could present a problem. For example, due to cloud computing utilising a multi-tenant system, a drive may be shared with other clients. If a drive is seized by law enforcement, then many of the clients will not be able to access their information (Convery 2010:13 and Gellman 2009:5). This can impede daily business operations, which contests cloud computing's viability for records management.

##### **b) Information Privacy and confidentiality**

Cloud computing can significantly affect information privacy and confidentiality. Where information is being hosted by a third party, the cloud service provider may be hosted offshore. This service provider may transport the information over other geographic boundaries, which could in turn affect the regulatory and legal requirements of the stored information (Onwubiko 2010:276). According to Chaput & Ringwood (2010:243): "It is nearly impossible to list all of the relevant regional laws, which may shape or otherwise affect the requirements necessary to consider when



outsourcing to the cloud.” An example of jurisdictional law of a country where the data is being hosted is that of the USA. Data hosted in the USA is subject to the US Patriot Act of 2001, Public Law 107–56 (Cervone 2010:165). This opens the data up for access by external forces, such as government entities. Thus, if Company X hosted data in the USA then their data could be accessed by the US government.

Within Australia, cloud-computing providers are using this concern to try to dissuade organisations from storing their data overseas in the United States. This is because The US Patriot Act of 2001, Public Law 107–56, allows national security agencies and the police to secure and access electronic data held by electronic service providers (Foo 2012, United States of America 2001). Allowing external entities access to sensitive organisational data may be considered an invasion of privacy.

#### **4.3.2.2 Service Level Agreement**

The service level agreement is a challenge for clients utilising cloud computing. The cloud service provider should provide a minimum service level to the client (Chaput & Ringwood 2010:253). Meanwhile, the service level agreement (SLA) needs to be specific to ensure privacy and compliance. For example, if another cloud client is undergoing audit proceedings, the cloud service needs to be able to ensure the privacy of other clients utilising the same drive for their data storage (Himmel 2012:109). This can be an essential factor for cloud computing’s viability, as clients may not wish to do business with a service provider that does not protect their privacy, or does not have a SLA that ensures their continued service in the case of, for example, audit proceedings. Furthermore, Himmel (2012:109) states that this agreement must include stipulations for data location, data management, backups and how the service provider can assist in auditing.

#### **4.3.2.3 Legal Compliance and auditability**

*Legal compliance* and *auditability* refer to the user’s accountability for the integrity and security of its data, even when they utilise a service provider. Traditional service providers participate in external security certifications and audits. A cloud

computing service provider should be able to provide their client with this information for their clients' audit purposes. If they are unable, or unwilling to, they are indicating that their services are only applicable for basic functions and services (Heiser & Nicolett 2008:3). Furthermore, they may be unwilling to provide this information, as they may not be adhering to the law. The sub-risk *legal compliance* and *auditability* is broken down into the following aspects:

**a) Pre-existing industry standard**

A pre-existing industry standard can be affected by organisations moving their data to a cloud environment, as many standards were not created with cloud computing in mind (Convery 2010:35). For example, a standard such as ISO27001 or ISO9000 may require that the owner of the information be able to show the physical location of the stored information. These compliance issues can be problematic to cloud adoption (Convery 2010:35). Without well-defined industry standards, further adoption of cloud computing will develop very slowly (Gagliardi & Muscella 2010:261) as organisations might see cloud computing as too risky. Industry standards will be discussed in detail in **Chapter 6**.

**b) Industry regulations and regional laws**

Industry regulations and regional laws can be complicated and can often overlap (Chaput & Ringwood 2010:244). For example, in the United Kingdom, the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Data Protection Act 1998 require public sector organisations to make selective information available to the public, within a certain period of time. Organisations which do not conform are subject to financial penalties as well as legal action through the Information Commissioner's Office (Convery 2010:34). For example:

On the 5 July 2012, the Information Commissioner's Office issued a penalty notice of £150,000 to Welcome Financial Services Limited. This was due to a breach of the Data Protection Act, where the personal data of over 500 000 customers was lost (ICO 2012).

In order for organisations to comply with these regulations and acts, they need to be aware of the geographic location where their information is stored, what type of information is being stored and how it can be accessed and made readily available to the public. As mentioned in **Section 4.3.2.1a)** organisations are subject to the laws of the country where their information is being stored, thus an Australian organisation would need to be aware of relevant industry regulations and regional law. Organisations utilising cloud storage need to determine its impact on regulatory and legal compliance and/or alter the processes to continue being compliant (Convery 2010:34). However, when an organisation uses the cloud to store information, it can make it increasingly difficult to specify what information is being stored in the cloud, as well as determine whether or not it has been correctly classified in compliance with the organisation's records and information management processes (Convery 2010:34).

Convery (2010:34) gives an example of ensuring cloud compliance concerning the United Kingdom's Data Protection Act 1998. Organisations that are using the cloud to store personal information need to assure that the information is:

- Up to date and accurate
- Processed for limited purpose
- Secure
- Lawfully and fairly processed
- Retained no longer than is required
- Not transferred to another country, without being secured
- Processed in conjunction with individual rights

#### **4.3.2.4 eDiscovery**

The term eDiscovery refers to the procurement of any electronic data for its use as evidence in a legal case (Biggs & Vidalis 2009:2). Organisations need to be able to provide access to electronic information for legal purposes, such as litigation (Convery 2010:35). The hosting location of cloud data is an area that needs careful attention, with regard to such factors as compliance, auditability and eDiscovery (Cervone 2010:165). An organisation needs to ensure that their records and information management system is extended to their cloud based

storage (Convery 2010:35). However, an organisation needs to have the same amount of control over their information, such as identification, retrieval and halting destruction of information, in the cloud as they would in a traditional storage system (Convery 2010:35). There could be serious consequences if an organisation is unable to provide the necessary electronic data when required. Furthermore, if an organisation is unable to have control over their information stored in the cloud, then the issue of the cloud's viability will be questioned.

In conclusion, *legality* and *auditability* issues are a challenge for organisations looking at utilising cloud computing. Organisations need to comply with the law in order to operate. With cloud computing, the legal requirements can be considerably more complicated due to organisations having to comply with the laws of the country in which the data is physically stored. In many cases, this cloud storage location is overseas, or in another country. Furthermore, due to cloud computing utilising a multi-tenant system, if a drive is seized for legal matters then, this may prevent other organisations from accessing their data, stored on the same drive. Each individual organisation will need to look at the specific laws of the country, where their data will be hosted. These investigations are necessary in order to determine whether cloud computing is a viable alternative for traditional storage and records management. Viable options for one organisation may not apply to another.

#### **4.3.3 Security**

Information stored in the cloud has many *Security* concerns. The *Security* of the cloud and keeping stored client information secure is the responsibility of the cloud service provider. It is the client's responsibility to ensure the provider is able to protect their stored data and encrypt their data (Convery 2010:13-14).

The cloud service provider needs to be able to establish the authenticity, reliability, integrity and the confidentiality of information being stored. They should furthermore, demonstrate that the information will not be accessed, or tampered with by any unauthorised party (Convery 2010:14). If a service provider is able to address these issues then, their viability for organisations may be credible. There

are, however, other security concerns associated with cloud computing which need to be considered. These are discussed in the following sections.

#### **4.3.3.1 Identity authentication and access management**

According to the Cloud Security Alliance (2011:136), when moving from a traditional computing environment to implementing a cloud-based environment a change in thinking needs to occur (with regard to such concepts as access management, entitlement and identity). Identity authentication and access management, as a sub-risk of *Security* is broken down into the following subsections:

##### **a) Identity authentication**

The cloud-based platform needs to utilise a powerful and stable identity management system. The system needs to include: identity information privacy, identity provisioning, e-provisioning, identity linking and mapping, identity federation and attributes, a login system, authorisation and authentication systems (Bouayad *et al.* 2012:30).

In 2011, the cloud service provider Dropbox had an authentication issue. At the time of the incident, Dropbox had over 25 million users and for nearly four hours any person was able to access any Dropbox account without using the correct password (Ludwig 2011). However, when the incident was discovered, the Dropbox co-founder Arash Ferdowsi wrote on the company blog that as a precaution all logged-in sessions were ended. Furthermore, in the following days all users that had their accounts compromised were notified. Upon final review, Ferdowsi reported that less than 100 users were affected and that neither their files, nor account settings, were modified (Ferdowsi, 2011).

Organisations need to evaluate whether their data will be safe if a cloud service provider houses it. Furthermore, the organisations should establish whether information can indeed remain confidential and not be accessed by

anyone. This example of Dropbox shows that there is the potential for information to be compromised.

#### **b) Access management**

Cloud applications should utilise multiple sources of data for identification, such as management components and authorisation procedures. This is done in order to map the access privileges to the processes, data and systems within the cloud application or cloud system. Utilising multiple sources of data for this identification is an obstacle for organisations that want to utilise a cloud-based service. Organisations might rather implement a virtualised service that may already be linked to their internal Directory Service (Cloud Security Alliance 2011:136), which contains the necessary access restrictions. Two examples of this are Novell's eDirectory and Microsoft's Active Directory (Cloud Security Alliance 2011:136). Microsoft's Active Directory Domain Services runs on Windows servers. It stores directory data including user login information and authentications (Microsoft 2013). This is an obstacle for organisations that want to utilise a cloud-based service, due to the amount of time and resources which are required in utilising multiple sources of data for this identification. This can draw into question the viability of cloud computing in relation to records management, where organisations with a large number of employees will have to set user access for all their employees as well as set up multiple sources for identification.

However, there is an issue with privileged user access. When an IT service is sourced externally, it circumnavigates the personnel, logical and physical controls that IT usually provides for in-house applications or services (Heiser & Nicolett 2008:2). Any user could access restricted data that is housed externally if they acquire the credentials from another user, regardless of their own access restrictions. This brings into question the viability of cloud computing for records management.

Although there are a few remote authentications services and identity management systems available for cloud services, such as Azure and

OAuth. There are no standardised enterprise graded tools (Himmel 2012:118). However, a web-based delivery service, or application can be used. This application can provide its own authentication system. Unfortunately, users would have to remember multiple sets of credentials for access to this application as well as for their usual systems (Cloud Security Alliance 2011:136).

#### **4.3.3.2 Human factors**

The weakest link in compliance, as well as in security risks, is human error. Even though there are fewer people involved in cloud computing than in a traditional IT environment, the risk of human error can still be great and have a large impact (Himmel 2012:47-48). Himmel (2012:48-49) provides an excellent example of human error in reporting on Amazon.

On 21 April 2011, Amazon was conducting an upgrade to one of their routers, which was connected to one of the Elastic Block Storage Systems (Amazon EC2 block storage systems). In the process of this routine upgrade, an Amazon engineer routed a high capacity network to a secondary backup network service. This caused a loop for hosts attempting to replicate their data to the new secondary backup network. This in turn caused data loss for many organisations and the Amazon service to be unavailable for more than a day (Himmel 2012:49).

Due to this outage, other companies were also affected such as Foursquare and Dropbox, who were down for days as these companies' business models are based on Amazon's cloud. Some customers even lost data, in addition to having their services being unavailable (Mohan 2011). This scenario illustrates the potential impact of human error and its consequences, drawing into question cloud computing's viability for records management.

#### **4.3.3.3 Surface attacks and vulnerabilities**

With cloud technology still being new there remains uncertainty around the important issue of security. New applications as a service are being developed for an IT model that is still maturing. Unfortunately, this is leading to new security

risks, such as the creation of new browser extensions, which have security vulnerabilities (Himmel 2012:102-103).

Opala (2012:47-52) identifies nine types of security risks or attacks that can occur:

- **Root kit attacks:** A root kit attack has great potential for DOS (Denial of service) attacks and for service denial impacts. This kit is a combination of attack tools such as malware, viruses, spyware and cyber warfare software.
- **Denial of service attacks:** tend to attack resources causing resource exploitation, resource starvation and an over utilisation of a system's resources, which cause system shutdown. The second generation of DOS attacks, the distributed denial of service attacks (DDoS) utilises botnets. This attack is undetectable and utilises multiple resources for attacks with a goal of service disruption.
- **Malware attacks:** Malware attacks infiltrate software and tracks users' activities and report transactional information through a backdoor in the system.
- **Viruses:** The virus is a system process disruptor, which is primarily used to cause production loss and eliminate data.
- **Botnets:** These are infected systems, which are brought under the control of a malicious user often for illegal activities (Velte *et al.* 2010:36).
- **Trojans:** Trojan software appears legitimate at first but contains a hidden code. Trojans spy on the systems and report back and can be used by the attacker/ hacker at a later time.
- **Hackers:** Hackers circumnavigate information security in order to gain access to data. Hacking has evolved to include identity theft, network disruption and the placement of spyware on hacked systems. A hacker can



also utilise virtualised systems as a type of launching platform for new attacks (Mollah *et al.* 2012:4).

- **Cyber warfare:** This usually refers to a large-scale attack. It includes taking advantage of vulnerabilities in an infrastructure, through the Internet as a medium for attacks on larger enterprise networks. These attacks can include denial of service attacks, logic bombs and theft of data.
- **Spyware** have similar characteristics to viruses and worm software. They do however operate in stealth mode to prevent any interaction with the user and to prevent service interruption. Their primary focus is on information gathering to execute additional attacks.

Concentrated attack value is a further concern for security. With more and more organisations moving data into the cloud, there are greater rewards for attackers to target these consolidated IT centres. This is causing new threats to emerge and for data centres to be constantly under attack (Himmel 2012:108). For records management, this can be a great concern where the cloud data centres are more likely to be targeted, placing clients' data at greater risk.

#### **4.3.3.4 Security-as-a-service**

Cloud computing requires the global adoption of Security-as-a-Service (SecaaS), in order to identify how security can be enhanced to secure it as a platform for business operation. This is needed in order to close the gaps in security and its discrepancies (Cloud Security Alliance 2011:162). Cloud service providers offer a security service, yet these services may lack transparency over the security controls being used (Cloud Security Alliance 2011:162). In order to protect themselves, organisations should only work with cloud service providers dedicated to being transparent. This means that the service providers should have no reason not to disclose their hosting procedures, or security methods to their clients (Cervone 2010:165). The clients are accountable for their own data integrity and security. Without such assurances, organisations may be placing themselves at

risk. The approach by cloud service providers to transparency may impact on their potential viability for an alternative to traditional storage and records management.

#### **4.3.3.5 Application security**

Application security in cloud computing needs to be designed with similar austerity to an application that connects directly to the Internet. The application must provide a level of security, without any assumptions being drawn about the environment. Cloud applications will face greater threats than applications in a traditional data centre environment (Cloud Security Alliance 2011:103).

The Cloud Security Alliance (2011:109) identifies the following areas that need to be understood when assessing security risks, within a business and application environment.

- **Lack of visibility/transparency:** Cloud users lack visibility into the cloud security policy enforcement (Discussed in Section **4.3.3.4 Security as a service**).
- **Lack of manageability:** Cloud users are unable to fully manage cloud application security, such as access policies (Discussed in Section **4.3.7 Governance and enterprise risk management**).
- **Lack of control:** Cloud users lack control of security policies (Discussed in Section **4.3.7 Governance and enterprise risk management**).
- **Loss of governance:** Users have no control over the infrastructure (Discussed in Section **4.3.7 Governance and enterprise risk management**).
- **Isolation failure:** Multi-tenancy, as well as the sharing of pooled resources is a key characteristic of cloud computing (see **Chapter 2, Section 2.4 and 2.5**). Based on this, rival companies may be utilising the same cloud services and are in fact running their systems in parallel to each other. Keeping these instances isolated is vital to prevent information being leaked

to one another. (Discussed in Section **4.3.6.3 Hypervisor security and multi-tenancy** in relation to hypervisor security failure).

- **Data protection:** Users give control of their data over to the service provider and rely on their security alone (Discussed in Section **4.3.3 Security**).
- **Compliance risk:** The service provider may affect the organisations' ability to comply with laws and regulations, as the data is no longer in their own control (Discussed in Section **4.3.2 Legality and auditability**).
- **Management interfaces and access configuration:** Applications are managed and controlled through the Internet, increasing the risk of a security breach (Discussed in Section **4.3.3.1 Identity authentication and access management** with regard to restricted access).

These criteria are regarded by the Cloud Security Alliance (2011:109) as essential to dealing with privacy and security issues, in cloud applications and services.

#### **4.3.3.6 Traditional security**

When utilising cloud computing, the traditional security must be assessed to mitigate risk factors. Proper security for IT equipment, communication technology and network technology for a cloud environment needs to be implemented correctly. This responsibility needs to be handled by the cloud service provider (Cloud Security Alliance 2011:75).

The client must evaluate the traditional security of a cloud service provider. Factors such as the physical location of the cloud service provider's data facility, any documentation recovery concerns and critical risk need to be evaluated (Cloud Security Alliance 2011:76). For example, the cloud hosting facility's physical location should be geographically sound, for example, not in areas of high seismic activity or areas that are often affected by natural disasters, such as flooding.

#### **4.3.3.7 Business continuity**

Business continuity deals with the three aspects of information security: integrity, availability and confidentiality. The continuity of business services is essential for an organisation. Even though a cloud service provider may commit to a Service Level Agreement and boast a high level of uptime for availability, there can still be service outages (see **Section 4.3.10 Availability and reliability**) (Cloud Security Alliance 2011:84). The client should ensure when they select a cloud service provider where their data is backed up to other servers to ensure they are able to continue work, should outages occur.

#### **4.3.3.8 Disaster recovery**

Disaster recovery in cloud computing is paramount to a cloud provider's success. Recovery documentation must be readily accessible to ensure that an organisation can recover its data in an unforeseen event (Cloud Security Alliance 2011:76). If such documentation does not exist, then clients may unintentionally add to the consequences by interfering with disaster recovery processes. The challenge to cloud storage, are:

- Disaster recovery
- A backup system involving information transfer to and from the cloud systems
- Mobility
- Availability
- Scalability
- Assuring business continuity
- A metered payment system

(Cloud Security Alliance 2011:84).

If data cannot be recovered, the impact can be catastrophic for an organisation. Cloud service providers must be able to provide the client with information about what will happen to their data when a disaster occurs. These providers must demonstrate whether or not they can make a complete recovery and provide a time frame on the recovery process (Heiser & Nicolett 2008:3). This should be done for all organisations utilising cloud storage, for records management.

#### **4.3.3.9 Encryption and key management**

When data is stored in the cloud it is subject to a multi-tenant environment. With various administrators under the employment of various organisations the need for data encryption is greatly increased. However, encrypting all data may be unnecessary and can greatly increase complexity (Cloud Security Alliance 2011:129). It is important to encrypt certain information, such as login credentials. For example:

In April 2012 a security flaw was discovered in the Cloud service provider Dropbox IOS application. This flaw allowed anyone with physical access to a client's phone to copy their login credentials, as the credentials were being stored in unencrypted text files (Marshall 2012).

This risk in *Security* draws attention towards cloud computing's viability for records management, as any person could gain access to secured information if the phone was acquired by a third party (with reference to the example above).

According to the Cloud Security Alliance (2011:129-130), the loss of control of data through outsourcing increases the risk of compromise and the difficulty of protecting the data. Encrypting the transfer of data that is being moved to the cloud does not mean data is sufficiently secured in the cloud. It is important to encrypt data files, such as metadata and log files, as these can be areas of data leakage.

The encryption in cloud applications can present issues for business applications that the software creator must investigate. If the cloud application contains a series of processes that utilise sensitive data or batch type jobs, or if the application uses its data for search methods on objects or records, then the use of an encrypted key can cause further complications (Cloud Security Alliance 2011:132).

In conclusion *Security* is perhaps the biggest risk faced by cloud computing. With cloud computing, the provider must ensure that client data is secure. However, it is the clients' responsibility to ensure that the provider is able to provide the

necessary security for their data. Data must remain secure, authentic, confidential and reliable.

Privileged user access is one of the various issues that could affect *Security* in a cloud environment. When data access remains in-house, there are IT controls that prevent unauthorised access to data from users. When data is stored in the cloud, these controls can be circumvented and allow other users to access private data.

Most of these challenges are not new to IT and data security. Challenges such as surface attacks e.g. Viruses, DDOS attacks, Trojans etc., affect both in-house data storage as well as cloud-based storage. However, the concentrated attack value increases the risk. This is attributed to the fact that because many organisations are utilising cloud storage, these cloud storage centres have become targets for attack. Organisations need to evaluate their cloud service provider security to determine whether their data is secure. This can be aided by cloud computing service providers being transparent. One provider may not be a viable option for an organisation, while another provider may be.

#### **4.3.4 Everywhere accessible data**

*Everywhere accessible data* means exactly what it says. The ability to gain access to data everywhere and anywhere. This risk is broken down into the following subsections:

- a) Mobile devices
- b) Collaboration tools

##### **a) Mobile Devices**

With the expansion of cloud computing use, more and more mobile devices, such as the cellular phones or tablets (i.e. iPad, Surface tablet etc.), are being utilised for mobile access. These devices bring about their own security concerns, as they may not comply with security standards as the software is still immature and vulnerable (Himmel 2012:106-107). Gartner (2013) has predicted that 90% of organisations will endorse the use of

corporate applications on various personal devices, such as tablets, cell phones, laptops etc., by 2014.

Furthermore, Gartner (2013) predicts that at least 60% of information workers will utilise a content application through a mobile device by the year 2015. The risk arises when, due to the large increase in mobile solutions and productivity tools, organisations are being persuaded to migrate their data to the cloud. Often there may not be sufficient security in place or issues relating to compliance (Buckley 2013). The issue of cloud computing's viability for records management can also be drawn into question. In a recent survey on mobile business users, conducted by the company Harmon.ie (2013), it was found that 41% of mobile users admitted that they ignored company policies and stored and shared corporate documents on unapproved cloud services such as GoogleDocs and Dropbox. This can lead to serious issues related to confidentiality of secured data.

#### **b) Collaboration tools**

Document management collaboration tools are enhanced by cloud computing (see **Chapter 3, Section 3.3.5 Rapid development and deployment**). However, in a study of the social collaboration habits of a thousand businesses and IT decision makers, consulting firm Avanade found that a large majority of the users were using third party tools, such as Facebook, instead of enterprise collaboration tools (Buckley 2013; Avanade 2013). This draws into question the security and privacy of what could be organisational intellectual property that is being shared and made accessible to anyone. Organisations need to be aware of this and decide how they can encourage collaboration through their own systems and prevent the loss of organisational intellectual property. This is an issue that can affect cloud computing's viability as it presents a risk of the loss of intellectual property.

Organisations need to be aware of the capabilities of mobile devices as well as the risk of *Everywhere accessible data*. With increasing mobile device usage,

organisations must get ahead of the expansion, incorporating device use into the organisation and not being forced into its use as a result of increased adoption. Getting in front and leading adoption can allow security concerns to be dealt with before they occur, and not as a result thereof.

#### **4.3.5 Incident response, notification and remediation**

It is not only the fact of an incident occurring but, also the way in which it is handled that can pose a risk. An incident refers to an event occurring, which may have an effect, positively or negatively, on something. In the context of this section, an incident will be used as an event or instance occurring, which has a negative impact. If an incident is handled incorrectly, or at a delayed pace, the damage it can cause could be increased. Clients who utilise cloud computing, in particular organisations, should be aware of how incidents are responded to by the cloud service provider. The service provider should notify the clients when there is an incident and inform them of how the incident is being remedied. For example, if there is a server crash, the client should be contacted, and informed that an alternate server will be made available to ensure that the clients' data can still be accessed.

This risk is divided up into the following aspects:

##### **a) Incident response & notification**

Although cloud computing does not require a new method of conducting an incident response to be developed, the organisation must adapt the existing incident response processes to include the new cloud environment (Cloud Security Alliance 2011:93). The incident response plan must be formalised and documented, outlining all the roles of those involved (Chaput & Ringwood 2010:253).

There are characteristics of cloud computing that directly influence incident response activities (Cloud Security Alliance 2011:93-94). They are:

- On-demand-self-storage
- Rapid elasticity and resource pooling



- Data crossing geographic boundaries

Cloud computing's *on-demand-self-storage* feature can make it difficult for a client to acquire the necessary support from their cloud service provider when a security incident needs attention. This may depend on the service provider's deployment and service model, where the actual scope of a service provider's incident detection, analysis, as well as their containment and recovery abilities may be dependent on the service level they provide (Cloud Security Alliance 2011:93-94).

*Rapid elasticity and resource pooling* offered by cloud services may directly increase the difficulty of the incident response processes, particularly forensic activities that are conducted in conjunction with incident analysis. These activities need to be conducted in a highly dynamic environment that can challenge the essential forensic activities (i.e. collection of data, devising scope of incident, preserving data integrity and stability). Due to cloud computing operating in a non-transparent environment, these problems are intensified when cloud clients endeavour to conduct these forensic activities themselves, because the cloud service provider is unable to provide any support (Cloud Security Alliance 2011:94).

Cloud computing can cause a client's data to *cross a geographic or even jurisdictional boundary* based on its data centre's location. This may occur, without the client's knowledge. This, in turn, can cause the data to be impacted in incident response procedures due to legal limitations on what may, or may not be done, or what can, or cannot be done (Cloud Security Alliance 2011:94). Reed (2011:19) provides an example of this where, due to geographically distributed services, there can be difficulties in network path investigation. Vendors may not have the tools to conduct this investigation. Furthermore, if there is no visibility of the network path information (historically or real time), investigation of an incident can become difficult.

In addition, when data crosses jurisdictions and is hosted in other countries, such as the US, it may be liable to unwanted access from third parties. This is due to the data being subject to the US Patriot Act of 2001, Public Law 107–56 (Cervone 2010:165). This in turn, can affect the cloud's viability for records management for organisations, in terms of privacy and confidentiality.

#### **b) Incident remediation**

Incident remediation refers to how an incident can be remedied once it has occurred. Cloud computing does however create an advantage for incident response where the continual monitoring of the systems can reduce the amount of time to handle an incident response. Furthermore, due to virtualisation, the containment and recovery can be expedited with less interruption. The enquiry into an incident could be significantly easier in certain areas. For example: virtual machines can be transported into a laboratory environment where forensic images are examined and an analysis conducted (Cloud Security Alliance 2011:94).

In order to determine cloud computing's viability, organisations need to be fully aware of how their cloud service providers respond to incidents that may occur, how they may deal with situations as well as who may be involved in the incident response plan. Remediation rules must be negotiated with the cloud service provider, in order to ensure that the client's needs are met. This will be an important factor in evaluating a cloud service provider's viability for records management.

#### **4.3.6 Virtualisation**

*Virtualisation* in cloud computing terms refers to a virtual, non-physical system, where resources are pooled together and shared (Sosinsky 2011:25). The cloud client is responsible for the security of the virtual machine. The cloud service provider is however, responsible for the secured virtual machine images (Bouayad, *et al.* 2012: 29). This section discusses some of the risks that were

briefly identified in **Chapter 3 Section 3.3.1.6** where the sub-benefit of shared resources and multi-tenancy were discussed under the benefit of *Cost efficiency*.

#### **4.3.6.1 Virtualisation Risks**

The Cloud Security Alliance (2011:157) identifies the following *Virtualisation* risks:

- **Performance concerns:** When running virtualised systems, resources are pooled and the use of security software (such as antivirus securities), may utilise a large amount of resources. This may cause performance issues as resources may be shared to other virtual systems. This software must be virtualisation-aware and/or only perform its security tasks on an individual virtual machine, in order to support other virtual machines that are also operating simultaneously (Cloud Security Alliance 2011:158).
- **Virtual machine guest hardening:** To be done in order to protect the virtual machine (VM) from attacks, such as unwanted connections, viruses and unwanted file access and manipulation (Cloud Security Alliance 2011:158).
- **Inter-VM attacks and blind spots:** VMs have the ability to communicate with other VM through a hardware backbone, instead of a network infrastructure. This however, may cause security issues because the traditional network monitoring tools for security purposes are blind to this communication (VM do not see it or monitor it). When migrating a VM, an attack could also occur where a malicious VM is allowed to migrate into a trusted VM zone. There are certain applications to assist in this problem, such as In-line virtual appliances and installing security tools on every individual virtual machine (Cloud Security Alliance 2011:158).
- **Operational complexity from VM sprawl:** VM can be easily created. This has led to a greater demand for them within clients' organisations. There can, however be issues caused by clients managing multiple VMs due to the increased chance of misconfiguration through human error. The organisation requires a policy-based management framework to help further

reduce security breaches caused by human error (Cloud Security Alliance 2011:158).

- **Virtual machine encryption:** VM vulnerability to modification or theft requires the images to be constantly encrypted to prevent attacks and data intrusion. While encryption readily caters for audibility trails and administrative controls, it is also liable to cause performance issues (Cloud Security Alliance 2011:158).
- **Instant-on gaps:** With threats evolving rapidly, a VM may be secured when shut down and unsecured when it starts back up. In order to ensure the VM's network-based security, virtual patching applications are needed. The patching checks the traffic to the VM for currently known attacks, before they start. A form of Network Access Control can also be utilised to monitor network traffic and isolate stale virtual machines, while updates are being done (Cloud Security Alliance 2011:158).
- **Virtual machine data destruction:** When data is migrated from a VM, it is essential to thoroughly destroy any trace of the previous owner's data from the template, or drive which is being given to a new client. (Bouayad *et al.* 2012:29; Cloud Security Alliance 2011:158).
- **Virtual machine image tampering:** VM are still at risk when they are offline and preconfigured virtual machines images could be tampered with, or misconfigured, before they are run (Cloud Security Alliance 2011:158).
- **In-Motion virtual machines:** VM are able to migrate from one server to another at any location. However, this does create a complication for security monitoring and for audits when VMs are moved to another server without leaving traceable audit trails or even alerting security (Cloud Security Alliance 2011:160).

#### **4.3.6.2 Hypervisor security and multi-tenancy**

Hypervisor security and multi-tenancy systems in cloud computing are linked. The hypervisor refers to the software in-between the operating system, the hardware that is used to map resources between the system and the VM risk (Bouayad *et al.* 2012: 29; Himmel 2012:21,26). Multi-tenancy is where resources are shared between VMs on a server, such as memory, CPU, storage, firewalls and even software services (Cloud Security Alliance 2011:64; Himmel 2012:40,104). The hypervisor is used to create isolation between the VMs on the server. This is done to prevent cross exploitation of isolated VMs which may be hosted on the same sever. Otherwise users may be able to exploit these security vulnerabilities and obtain sensitive information from other VMs through shared resources (Cloud Security Alliance 2011:64; Himmel 2012:40,104). This can draw into question privacy issues for users (Mollah *et.al* 2012:4), and cloud computing's viability for records management, where restricted documents or records could be accessed by outside users. Unfortunately, if the hypervisor is no longer secure then all VMs are at risk (Bouayad *et al.* 2012: 29; Himmel 2012:21, 26). Clients may choose to utilise their own security configurations for their VMs. However, when they do not utilise the security controls of the cloud service provider, it can result in breaches in the security system. This can arise due to conflicts with the client's security configurations (Bouayad *et al.* 2012: 30).

#### **4.3.6.3 Automation and standardisation**

The rapid *scalability* of cloud computing is an advantage, especially with automation processes such as VM creation and backups. However, if there is a problem in the automation scripts, there can be major risk factors as mentioned in **Chapter 3 Section 3.3.8.2**. For example, if an error is contained in the script relating to VM creation, then that error is replicated (Himmel 2012:104-105). Standardisation can help lower the risk. This is achieved by creating a more consistent environment, through limiting the number of different types of VMs that are available in the cloud. Unfortunately this does present its own risks where due to a more constant environment, there is a greater risk for the spread of malicious software and viruses (Himmel 2012:104-105). If one VM is breached, then VMs of the same type are also open to the same security exploit.

*Virtualisation* can present many risks to cloud computing. In particular, with regard to records management, where hypervisor security and cross VM exploitation can allow access to stored information on other VMs, security and privacy seems to come forth as the biggest concern. For example, if VMs utilise templates which contain the previous clients' information, this information would then be accessible to the new client. These issues impact on cloud computing's viability for an alternate method for records management and storage, where a client would need to carefully evaluate these risks with their cloud service provider, to determine if their data would be secure and inaccessible by others.

#### **4.3.7 Governance and enterprise risk management**

*Governance and enterprise risk management* is concerned with the establishment and execution of organisational processes, structures and controls which are used for the maintenance of information security governance, compliance and risk management (Cloud Security Alliance 2011:30). A loss of governance over the process, structures and controls can lead to a loss of control over these issues. This provides a risk for prospective cloud users.

When an organisation uses the cloud to store information, it transfers the responsibility of information security to the cloud service provider. The extent of this loss of control for the organisation over the information's security is determined by the kind of cloud service model and services being used. For example: Infrastructure-as-a-Service (IaaS) would allow for more control than Software-as-a-Service (SaaS) (Convery 2010:15). SaaS provides software, such as Google Apps, whereas IaaS provides mainly the system to run software that can be configured specifically to a client's needs. However, Macvittie (2009) states that the loss of control in cloud computing is related to infrastructure or IaaS. This is due to the cloud service provider focus on application infrastructure, such as operating systems, databases, application servers etc., as opposed to acknowledging real infrastructure which includes application and network infrastructure. In addition, prospective cloud computing clients are likely to be worried about the fact they are unable to select and utilise the necessary

application-network focused services they require, in order to meet their own SLA targets. Simultaneously, cloud computing may improve security and performance to levels more superior to those in a traditional data centre.

The loss of governance can compromise the organisation's ability to comply with regulatory and legislative procedures. The organisation's capacity to show integrity, reliability and authenticity of the information that they are storing in the cloud must be demonstrated. Cloud service providers, who may not want to share usage and access logs for auditability with their users, further complicate this. Unfortunately, it can be just as difficult for clients to utilise their own monitoring software for this (Convery 2010:15). These issues need to be considered by organisations. If the service provider is unable to share information, which may affect the auditability of the stored data, then the traditional data centre may be the more viable option.

#### **4.3.8 Interoperability, portability and data lock-in**

*Interoperability and portability* are closely connected. *Interoperability* is concerned with all the components of cloud computing having the ability to exchange with different, as well as new components from alternate providers and continue to function. *Portability* refers to the ability of the applications' components to be moved and recycled in another location, despite the operating system, provider, location, infrastructure or Application Program Interface (API). However, absence of interoperability and portability can lead to data lock-in with a cloud service provider (Cloud Security Alliance 2011:64-65). This is due to a lack of standardised APIs, or procedures, which can make it expensive, or very difficult for users to migrate to another service provider, as they are now "locked-in" to the current cloud service provider's development environment (Convery 2010:14,71).

*Portability* is an important aspect for consideration with a cloud service provider. This feature can deliver business benefits through multiple identical cloud deployments across various service providers as well as prevent *data lock-in* (Convery 2010:14; Cloud Security Alliance 2011:65). Additionally, data ownership must be established. In the event that one party no longer wishes to do business

with the other (client or cloud service provider), there must be an easy transition where the data is returned in a usable format (Chaput and Ringwood 2010:252). Lack of standardised APIs can mean that when a client wants to move its cloud services, they first have to migrate all their services back in-house before they can outsource it again (Convery 2010:14; Cloud Security Alliance 2011:65).

With cloud computing still maturing, standardised API and procedures are lacking. This makes it difficult for clients to transfer their data, or service, from one cloud service provider to another and often at great cost. This is known as data lock-in/ vendor lock-in, where the cloud service provider has an interest in retaining customers by being locked into their products. This does present certain issues such as the cloud service provider ceasing to operate, or raising the price of their services (Armbrust *et al.* 2009:15; Convery 2010:14-15). Organisations will need to ensure that their data being hosted in the cloud retains its validity, despite a service provider going out of business (Mollah *et al.* 2012:5).

#### **4.3.9 Viability**

Cloud computing is perceived as viable, as discussed in **Chapter 3**, but there are also risks associated with *Viability*.

In this section, sub-risks that may affect viability are discussed:

##### **a) Hidden variable costs**

For instance, where companies are not acutely aware of what exactly they are charged for in the cloud's pay-per-use model, hidden costs can render what looks to be a viable solution into a costly decision. Cloud service providers charge per hour, which may include time when a client's instances are idle (Armbrust *et al.* 2009:18). Cloud computing's low costs have caused a rise in its adoption by organisations looking to outsource their data to save on IT costs. The downside of this low cost model is the hidden variable cost risk. Organisations' scalability may be based on workload, which could fluctuate at unpredictable intervals and cause unpredictable costs due to more resources being required (Himmel 2012:109).



### **b) Bugs in distributed systems**

One of the most challenging issues for cloud computing is the elimination of errors on large-scale distributed systems. Errors, or bugs, often cannot be replicated in a smaller configuration because debugging needs to be done at a larger scale in data centres (Armbrust *et al.* 2009:18).

### **c) Shared reputation and accountability**

Due to shared resources and multi-tenant virtualisation, various issues can arise with a shared effect. For example: if a cloud client causes a spam attack, which in turn causes the cloud service providers IP address to become blacklisted, this may limit what applications could be hosted. Applications (such as spam filters) could block the provider's IP address and prevent applications from running. A further issue would be legal accountability, where the cloud service provider would not want to be accountable and would want the client, or perpetrator, to be held accountable for their action (Armbrust *et al.* 2009:18).

#### **4.3.9.1 Cloud computing rights and responsibilities**

Another issue that may affect cloud computing's viability for organisations is that of responsibilities. For example, what is the cloud service provider responsible for, and what is the client's responsibility. Gartner (2010) released a Press Statement, which outlined six rights and one responsibility for cloud-computing services. They are:

- **The right to Service-Level Agreements (SLA) which address liabilities, remediation and business outcomes:** Cloud service providers must create SLAs, which are extensive regarding the services offered. They do not need to be customer specific.
- **The right to retain ownership use and control one's own data:** The client must retain all rights and ownership of their data. The provider must

state specifically what they can do with the client's data and the SLA must consider what will happen to the data if the service provider goes out of business.

- **The right to understand the technical limitations or requirements of the service up front:** Providers and clients must keep each other informed of their technical limitations in order to adjust for long term, or complicated projects.
- **The right to notification and choice about changes that affect the service consumers' business processes:** When systems are upgraded the provider must notify the client in advance so that the systems can be taken offline. Clients should also be informed if there are any changes they may need to make, which may affect business processes.
- **The right to understand the legal requirements of jurisdictions in which the provider operates:** Due to data being stored in various geographic locations, the client must be assured that no laws are broken for which they the client may be held liable.
- **The right to know what security processes the provider follows:** Clients must have an understanding of what security processes are in use, in order to ensure that they do not affect security at a different level, such as the security between the servers and the network. The clients must also be aware of the business continuity plan to ensure that their own business operations can continue, in the event of an emergency.
- **The responsibility to understand and adhere to software license requirements:** There must be an understanding between the service provider and the client with regard to software licenses. If the client violates a license agreement by utilising it in the cloud, then the service provider should not be held accountable. However, the service provider should not

allow the vendor to audit them if the client owns the licence for the software; it should be done through the client.

Organisations must discuss these issues with the prospective cloud service provider. If the service provider does not meet minimum requirements regarding the rights and responsibilities, then an alternate provider may be a more viable option.

In conclusion, the *Viability* of a service provider is usually a concern for organisations. For cloud service providers, this concern is no different. If a cloud service provider goes out of business, or is acquired by a competitor, then this will affect the users' data and/or their accessibility (Heiser & Nicolett 2008:4). For organisations looking to utilise cloud computing for records management it may be problematic. For example, if the service provider does go out of business then data could be lost or in an unusable format. Organisations cannot afford to lose their stored records, as it can cause issues related to liability and daily operations. An example of this occurred with the company *Linkup*, an online storage service:

On 8 August 2008 *Linkup*, the company previously known as *MediaMax*, shut down after it lost access to an unspecified amount of client data. Their website reported that they were no longer offering a service. The company's CEO reported that at least 55% of the data was safe but, for the remaining 45% it was unclear how much was actually saved. Some users lost all their files. Linkup had ±20000 users (Brodkin 2008).

This example shows the risk of cloud computing and data loss, and illustrates the damage that can occur to organisations. Organisations need to evaluate carefully what service providers they may select.

#### **4.3.10 Availability and reliability**

*Availability and reliability* of service is a core benefit of cloud computing discussed in **Chapter 3 Section 3.3.4**. It can, however present its own risks. An important issue is service level commitments, which are required for critical business processes. Often the case may be that the cloud service provider may not include

these offerings in their actual service. In that case, the client must define what service level requirements the cloud service provider requires and ensure that if these are not met, that there are penalties for the cloud service provider (Heiser & Nicolett 2008:3).

Due to the nature of their business, cloud service providers are a high target for malicious attacks and hacking. They need to be able to prevent and react quickly to malware attacks, hacking, Distributed Denial of Service (DDoS) attacks and other security threats. If the service provider goes down, there is nothing the organisation is able to do but wait for the service to be restored (Convery 2010:14). For example:

In August 2013, China was hit by what the BBC News (2013) called its “biggest ever” cyber-attack. The distributed denial of service (DDoS) attack targeted servers, which hosted websites, which had the domain name “.cn”. This attack caused many websites hosted in China to go offline.

This example illustrates the potential damage of a DDoS attack. If targeted towards a cloud-based system, data could be inaccessible, compromised, or even lost.

If a cloud service provider ceases operations and goes out of business, there is no regulated process for returning the information to its clients. Thus, contingency planning is required for these instances (Convery 2010:14). Organisations utilising cloud services may need to draw up a contingency plan on how they are able to continue business operations, in the event of an outage, and how they will back up existing data or access critical files, in order to conduct daily operations.

**Table 4.2** illustrates a few examples of recorded cloud service outages. The table gives examples of service providers affected, the causes of the outages, and time of affected services. Even though some outages were 40 minutes (See Google in table below), business operations were affected or even came to a standstill.

**Table 4.2: Outages for different cloud services**

Cloud service and cause of outage	Outage duration	Outage date
Google Apps engine and Gmail	2.5 hours	24 Feb 2009
Microsoft Azure: malfunction in Windows Azure	22 hours	13-14 Mar 2008
Gmail: site down from outage in contact systems	1.5 hours	11 Aug 2008
Google search outage: due to programming error	40 minutes	31 Jan 2009
Google App Engine partial outage: from programming error	5 hours	17 Jun 2008
S3 outage: single bit error causing gossip protocol blow-up	6-8 hours	20 Jul 2008
S3 outage: authentication service overload causing unavailability	2 hours	15 Feb 2008
FlexiScale: core network failed	18 hours	Oct 31 2008

(Adapted from Armbrust *et al.* 2009:14; Rimal, Choi and Lumb 2010: 32)

Although outages can affect business operations, they are rare. For instance, only a single outage during a two-year period was reported in Convery's (2010:64) case study of Guardian News & Media (GNM), who migrated to Google Apps, Google Docs and Sites because of its low costs.

#### 4.4 Summary

In this chapter, ten risks and challenges of cloud computing, as well as the related sub-risks, were identified. After a critical analysis, the reported research of sixteen sources was tabulated against the ten risks identified by Carroll *et al.* (2011:4-5) in **Table 4.1**.

**Table 4.3** provides a summary of the ten risks and challenges associated with cloud computing identified in this chapter as well as examples of each.

**Table 4.3: Ten risks and challenges associated with cloud computing**

Ten Risks and challenges associated with Cloud Computing	Examples
1. Compliance	Comply with international standards
2. Legality and auditability	Unable to point to physical location of data
3. Security	Viruses, bot attacks, DDoS
4. Everywhere accessible data	Utilisation of unauthorised cloud applications
5. Incident response, notification and remediation	Response to risks/disaster such as viruses or floods
6. Virtualisation	Cross image exploitation
7. Governance and enterprise risk management	Loss of governance or control over network
8. Interoperability, portability and data lock-in	Data lock in and transferability issues
9. Viability	Lower cost for efficiency
10. Availability and reliability	Downtime and service outages

Armbrust, Fox, Griffith, Joseph and Katz (2009); Biggs & Vidalis (2009:2); Bouayad, Blilat, El Houda Mejhed and El Ghazi (2012:30); Carroll *et al.* (2012:4-5); Cervone (2010:165); Chaput & Ringwood (2010:243); Cloud Security Alliance (2011: 23-25); Convery (2010:10-12); Gagliardi & Muscella (2010:261); Gellman (2009:5); Heiser & Nicolett (2008:2-5); Himmel (2012:101-110); Mollah, Islam and Islam. (2012:4); Onwubiko (2010:266); Opala (2012:47); Thomas (2010:219); and Velte, Velte and Elsenpeter (2010:36).

The risks and challenges identified in this chapter draw attention towards the risks that organisations need to carefully evaluate before adopting cloud computing. Consideration must also be given as to what needs should be addressed when selecting a cloud service provider. Despite all these risks and challenges, cloud computing does appear to be viable. However, each organisation is unique and each service provider may present its own ethos, or procedures of dealing with these risks and challenges which may be acceptable for one organisation but not for another. The risks impacting on records management are further discussed in **Chapter 6**, with more focus on compliance and international standards, in order to help determine cloud computing's viability.

## **Chapter 5 Cloud computing and innovation**

### **5.1 Introduction**

This chapter focuses on how cloud computing can foster innovation within an organisation. In order to achieve this, an analysis of the relevant literature was performed. This chapter reports on this analysis in order to provide information to help answer the research question:

- How can cloud computing be used to foster innovation, within an organisation?

In order to do this, the features that help drive innovation in organisations are analysed. The chapter then identifies what antecedents, or precursors need to be addressed within an organisation, before cloud computing's adoption can be used to as a tool to help foster innovation.

### **5.2 Background**

Innovation as a concept refers to how an individual or organisation can create money from creativity. To do this, the individual or organisation needs to create something which is new and provides outstanding value to the target market. This market could be an individual, an organisation, industry, or even society in general (Higgins 1995:33). With cloud computing being a relatively new technology, there are opportunities to promote growth and innovation within organisations.

### **5.3 Cloud computing and innovation**

Cloud computing can have a positive effect on innovation, with regards to application development. Cloud computing can lower upfront costs and investments, which may be needed on infrastructure due to the cloud's scalable resource ability (Convery 2010:12). The Australian Government is an example of this positive effect of innovation. They have noticed cloud computing's potential to drive innovation. They have begun with the creation of a National Research Cloud aimed at providing a portal to support collaborative Australian research (NeCTAR 2011:2). Research conducted during this National Research Cloud project

highlights the prospective use of cloud computing as a portal for collaboration, a data repository and as a platform to promote innovation.

Delivering the correct knowledge, in the correct innovation process at the correct time is a challenging issue for business innovation leaders. An innovative organisation must promote innovation with haste as well as be effective and efficient, while still sourcing and managing their resources on a global platform in the competitive environment (Soliman 2012:2).

This presents a challenge for the cloud system where different components have to be implemented at various stages. For example, organisations need to decide what Software-as-a-Service (SaaS) must be implemented first. While most organisations would utilise cloud systems for reduced costs and speed benefits, their desire for the cloud systems implementation would also involve the effective and efficient utilisation of the system for knowledge transfer activities (Soliman 2012:2).

In the following sections, cloud computing's impact on innovation will be analysed. This is done through analysing the six cloud business enablers that help drive innovation in an organisation. These enablers are from the Cloud Enablement Framework created by IBM. They do, however, link with the potential benefits identified in **Chapter 3**.

### **5.3.1 Cloud business enablers driving innovation**

Some organisations are utilising the cloud in order to create additional revenue streams through improving, extending and creating new customer value propositions. The use of cloud technology has resulted in a shift from value creation to who creates the value, how it is created as well as how it is delivered and finally captured. Cloud technology is being utilised to enhance, modify and create new industry and organisation value chains (Berman *et al.* 2012:31).

Berman *et al.* (2012:30-31) identifies six cloud business enablers that are already being used to help drive innovation. These cloud business enablers are similar to



the potential benefits identified in **Chapter 3**. This indicates cloud computing's ability to support innovation through its inherent benefits, and is achieved by allowing organisations to take advantage of these benefits and drive future growth within their organisations.

The enablers are:

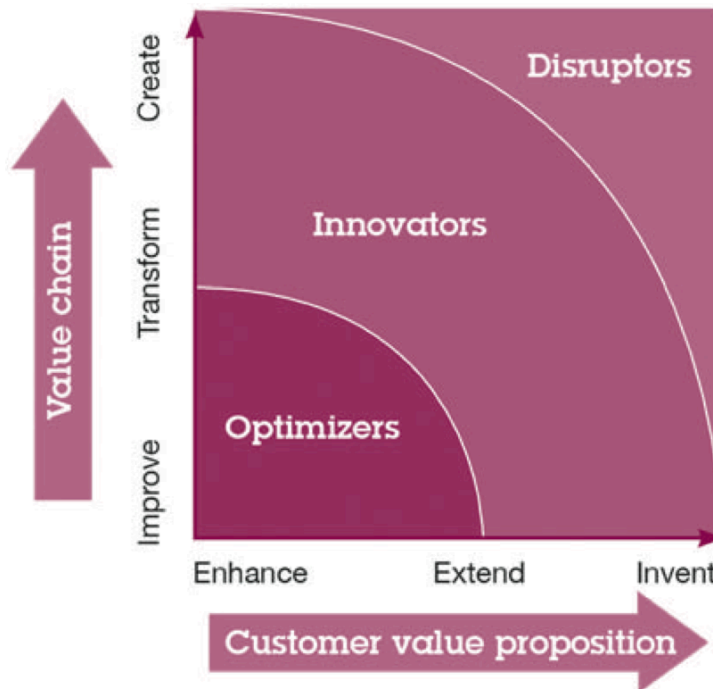
1. *Cost flexibility*: Cost savings and cloud computing's pay-per-use structure (see **Chapter 3 Section 3.3.1**). This allows for more capital to be used in operations as opposed to traditional IT costs.
2. *Business scalability*: Easy resource scalability (see **Chapter 3 Section 3.3.2**). This enabler allows organisations to expand their resource requirements rapidly.
3. *Market adaptability*: Ability to adjust rapidly based on customer needs (see **Chapter 3 Section 3.3.3**). This creates a competitive advantage allowing organisations to adjust to changing markets.
4. *Masked complexity*: Hiding complexities from customers such as not needing to involve them in upgrade details and requirements (see **Chapter 3 Section 3.3.1**). As an enabler this allows the customer to not have to be involved with any changes that may occur within the organisations.
5. *Content-driven variability*: Ability to provide customer tailored products and services, enabling the targeting of more markets (see **Chapter 3 Section 3.3.3**).
6. *Ecosystem connectivity*: Promoting collaboration between users, which improves productivity and helps drive innovation (see **Chapter 3 Section 3.3.5**).

(Berman *et al.* 2012:31).

### 5.3.2 Cloud Enablement Framework

Berman *et al.* (2012:31) draws attention to the IBM's "Cloud Enablement Framework" which can be used to determine the impact of an organisation's cloud supporting business strategy. The extent to which an organisation utilises the cloud can affect value chains and value propositions. The Cloud Enablement Framework explains three organisational archetypes, which characterise this impact. They are:

- **Optimisers:** to help improve value to the customer and improve the organisations efficiency.
- **Innovators:** used to generate new streams of revenue through improving value to the customer.
- **Disruptors:** to create new revolutionary means of providing value to the customer and creating new customer needs. (Berman *et al.* 2012:31; Lala 2012:21) (see **Figure 5.1**).



**Figure 5.1: Cloud enablement framework (Berman, Kesterson-Townes, Marshall, and Srivathsa 2012:32).**

As business leaders begin to identify how cloud services can best be utilised to optimise, innovate or disrupt their business models, they will need to challenge the pre-existing realities and approaches in place (Berman *et al.* 2012:34). This is achieved through cloud computing's potential benefits, where leaders need to consider new avenues for conducting business, for instance by utilising benefits such as cloud computing's unlimited resources and its everywhere accessible data (see **Chapter 3, Section 3.3.2 Scalability and flexibility** and **3.3.7 Greater mobility** for further details on cloud computing benefits).

### **5.3.3 Cloud computing adoption and innovation: critical factors**

In a recent research paper by Willcocks, Venters & Whitley (2013:184), an investigation was carried out to determine what factors are driving and preventing cloud computing's adoption, in relation to its innovative practises. Willcocks *et al.* (2013:184) discovered that while cloud computing has features which encourage its adoption and use for innovative purposes by organisations there are also, precursors that need consideration before cloud computing can be successfully adopted. These so-called precursors are derived from the technological aspects of cloud computing (Willcocks *et al.* 2013:184). According to Willcocks *et al.* (2013:185) there are three antecedents, or precursors, that need to be addressed before cloud computing adoption and its innovation can be successful in business. These are:

#### **5.3.3.1 Innovation through infrastructure and service**

Due to cloud computing's scalable and flexible infrastructure (see **Chapter 3 Section 3.3.2**), there are fewer constraints around an organisation's risk profile in relation to innovation (Willcocks *et al.* 2013:192). For example, the case study on Company X deals with the findings analysis to help determine if cloud computing is a viable option for records management. Due to the lowered risk profile, Company X could take on cloud computing as a records management option. Utilising traditional data storage options may have required extensive computing resources. However, due to cloud computing's pay-per-use model and scalable resources it can now be more affordable to gain storage options through cloud computing. If the adoption of cloud computing is unsuccessful, then the service can be discontinued. Capital would not have been required to purchase additional hardware for the project.

#### **5.3.3.2 The executive perspectives on the cloud innovation agenda**

Research conducted by Willcocks *et al.* (2013:189) found that an overall 65% of business executives surveyed believed that cloud computing had the ability to keep down the cost of business applications.

In the case study results analysed in **Chapter 8**, the support from the key

decision-makers and technology drivers, within the organisation, would allow for cloud adoption to have a greater chance of being accepted and utilised. This support is reinforced by Rogers (2003:131) *Diffusion of Innovation Theory*, which under the societal aspect of innovation adoption states that, “Influential persons can lead in the spread of new ideas, or they can head an active opposition”. Within an organisation, the key decision-makers and managers are the influential players that will be needed to drive cloud computing’s adoption.

### **5.3.3.3 The changing role of the IT department**

With cloud computing, IT departments need to be able to adapt to an organisation’s changing business needs. In order to achieve this, IT professionals need to acquire a more diverse skills base, shifting to a deeper understanding of business roles with emphasis on business skills and business understanding (Willcocks *et al.* 2013:190). These IT professionals will need to provide business solutions, in addition to just “mandating” an IT infrastructure. With the business environment evolving, there needs to be new solutions to problems.

Willcocks *et al.* (2013:193-196) found that the use for cloud innovation beyond IT operational benefits present more issues. They have identified factors that affect their antecedents to cloud computing adoption and innovation, which are described in **Table 5.1**.

**Table 5.1 Evidence relating to cloud innovation (adapted from Willcocks, Venters & Whitley 2013:194).**

	Executive perspectives on the cloud innovation agenda	The changing role of the IT department	Innovation through infrastructure and service
<b>Attributes of innovation</b>	+ Focus back on business requirements	- Greater 'operational readiness' required	+ "Low-friction" innovation
<b>Collaborative innovation</b>	+ Increased focus on customer needs along supply chain	- Too much emphasis on headcount/cost reduction	+ Changing risk profile supports experimentation
<b>Innovation implementation process</b>	- Requirements for high levels of service  - Challenge of managing BYOD	- IT staff need greater business orientation  - Skills shortage/retention problems	- Challenge of moving from demonstrators to production systems  + Automated marketplace for provisioning
<b>Notes: + Supports faster cloud innovation; - could result in delays in cloud innovation</b>			

#### 5.4 Summary

Cloud computing is promoting innovation within organisations and is shown through the IBM Cloud enablement framework. This framework has the ability to provide new, more productive, proactive and innovative methods of conducting business. As organisations are beginning to realise the cloud's power to create new business models, as well as to promote sustainable competitive advantages, they will begin to utilise cloud capabilities to drive business success and value, whether they are optimisers, innovators or disruptors (Berman *et al.* 2012:34).

There are, however, antecedents that need consideration before cloud adoption within an organisation should happen. Willcocks *et al.* (2013:197) concluded that cloud computing as an innovation provides organisational units, with the ability to alter their pre-existing business services through collaboration and innovation beyond the enterprise. Furthermore, the unique features of cloud computing provide business innovation opportunities which can adjust the risk profile of these business innovations. This allows for new business processes and their service

levels to be tested and expanded, or disbanded if they are unsuccessful.

An organisation's cloud system must drive innovation and still serve normal organisational needs. Berman *et al.* (2012:30-31) identified six cloud business enablers that help drive innovation across industry and company value chains and customer value propositions. The enablers identified were:

- cost flexibility
- business scalability
- market adaptability
- masked complexity
- content-driven variability
- ecosystem connectivity

These are similar to the potential benefits identified in **Chapter 3**, indicating the inherent ability of cloud computing to support innovation through its potential benefits. However, cloud computing has features which encourage its adoption for innovative purposes, as well as challenges. These challenges do need attention before cloud computing can be successfully adopted (Willcocks *et al.* 2013:184).

The chapter analysed the Cloud Enablement Framework which discussed what business enablers help drive innovation within an industry.

An alternative perspective was also analysed which was given through discussion of a research paper by Willcocks *et al.* (2013: 184). Willcocks *et al.* (2013) identified the factors driving and preventing cloud computing's adoption, in relation to its innovative practices.

In the next chapter, **Chapter 6**, the viability of records management in cloud computing will be discussed.

## Chapter 6 Cloud computing's legislation, standards, benefits and risks for records management

### 6.1 Introduction

There is continuing growth of cloud computing being used for records management. This is illustrated by Business magazine *Forbes* (Hilton 2010) and *IDC Cloud Research* (Underwood & Isikdag 2011:253), in their predictions on cloud spending in today's market place. *Forbes* identifies that the growth of enterprise-based cloud computing services will increase from 12.1 billion USD in 2010 to \$35.6 billion in 2015 (Hilton 2010). Meanwhile, the IDC has found that global expenditure on public cloud based services has exceeded \$16 billion in 2009 and is predicted to rise to \$55.5 billion in 2014 (Underwood & Isikdag 2011:253). These figures draw attention to the fact that cloud computing is on the rise. An increasing number of organisations as well as public users are embracing the technology, this indicates the potential viability for cloud computing in more and more applications.

This chapter is concerned with cloud computing's viability for records management. The aim of this chapter is to provide information to help answer the research question:

- To what extent is cloud computing a viable option for records management?

The viability of cloud computing (in the context of this study) is determined by two overall aspects, namely the laws and standards and the benefits and risks.

Only the laws and standards which directly affect records management in Australia, in a cloud environment, are highlighted. Australian laws and standards, such as AS ISO 15489, AS 5044, ISO 16175 and The *Electronic Transactions Act* 1999 (Australia 2011:14-15), are highlighted as they affect the research objective as to whether or not cloud computing is a viable option for records management for Company X.

The chapter then examines the benefits and risks affecting records management and whether these benefits, risks and challenges are similar to those outlined in **Chapter 3** and **Chapter 4** respectively. These benefits and risks are generalisable to organisations similar to Company X (organisations operating in the mining software development field in Australia).

## **6.2 Background**

As stated in **Chapter 1**, the empirical part of this research deals with a case study analysis of Company X's server layout and documentation practices. The case study was executed in 2012 at an Australian mining software development company. This is a private organisation and the case study examined their Australian office in the state of Queensland. The case study analysed their server layout and their documentation practices that they are currently using. The server layout was not examined in this dissertation as it falls outside the scope of this research.

In **Chapter 1, Section 1.8.1** multiple definitions of records and records management were given to clarify what records consist of and what is considered as records management for the purpose of this research. This was done according to a definition which was given by Company X in **Chapter 1, Section 1.9**, due to a condition set forth in Company X Document management standard. To reiterate Company X's Document management standard identifies, for their own purpose, that

*The bulk of their documentation will be stored and classified as records.*

In accordance with this, cloud computing's records management capabilities will be investigated in order to use the organisation's documentation practices for analysis in **Chapter 8**.



### **6.3 Impact of legislation and standards on cloud computing viability for records management**

As cloud computing is a relatively new concept, many challenges are still being addressed (see **Chapter 4**). In 2011, the Cloud Security Alliance (CSA) began participating in the development of cloud security and privacy standards (CSA 2011). These standards are still currently being developed.

As Company X is an Australian organisation, only the Australian laws and international standards which impact on private organisations were examined. This was done to determine what laws, if any, may affect the viability of cloud computing for records management. It should be noted that if records were hosted outside of the local jurisdiction, an organisation would need to examine that country's hosting laws specifically (Queensland Government 2013a).

#### **6.3.1 Australian hosting laws and international standards**

Keeping good records is important. According to the Australian Taxation Office (2012) keeping good records helps a company benefit in three ways:

1. It helps a company in meeting its obligations towards tax;
2. It allows a company to evaluate the state of their business; and
3. It can lead to creating good business decisions.

According to the Queensland Government (2013a), when considering cloud computing for business the organisation must be aware of Australian regulatory requirements and legislation. Australian law requires a company to retain its records for a minimum period of five years, in either electronic or paper format (Australian Taxation Office 2012). Essentially this means that cloud computing could be used by Company X for records management and would have to retain their records for this minimum period.

There are six types of records that a company needs to keep:

1. Income tax records
2. Income sales records
3. Expense or purchase records

4. Year-end records
5. Bank records
6. Other records
  - a. Goods and services tax (GST) records
  - b. Employee and contractor's records
  - c. Fuel tax records

(Australian Taxation Office 2012).

The Queensland Government (2013a) states that if the business is utilising an overseas cloud service provider, they need to be aware of the regulations requirements and legislation in that geographic area. This is due to the possible impact that local legal jurisdiction may have on the records. This may affect cloud computing's viability for records management.

Furthermore, if cloud computing was selected for records management, an organisation (Company X included) would need to make sure that they are able to comply with the *Electronic Transactions Act 1999* (Australia 2011:14-15). Under Section 12 of the Act it states that if a record is kept in an electronic format, it must:

- Remain intact, meaning that the integrity of the information is not compromised. It must remain complete and unaltered.
- Remain accessible, where the information contained can be readily accessed.

It is important to establish these issues with the cloud service provider before utilising their services.

### **6.3.2 International standards**

When organisations like Company X conform to international standards, it helps to reassure their clients that their products are efficient and safe (ISO n.d.). For records management it assures that a company is compliant with best practices. The National Archives of Australia issues, as well as endorses, a variety of

international standards that directly relate to records and information management (National Archives of Australia 2013b).

The following international standards are applicable for Company X:

- AS ISO 15489 (Australian and international standard for records management)
- AS 5044 (AGLS Metadata Standard)
- ISO 16175 (Information and documentation)

The relevance of the above-mentioned standards are explained in the following sections and need to be considered for Company X, when determining the viability of cloud computing for records management.

#### **6.3.2.1 Australian Standard AS ISO 15489 (Records Management)**

The AS ISO 15489 is used by Australian public and private organisations. It provides organisations with guidance when creating record policies and procedures, as well as when creating processes and systems to support the records management. The standard is used to provide a descriptive benchmark standard, which should be used to help organisations compare against their own records management systems and practices (National Archives of Australia 2013b).

This standard is used to provide best practices for both paper and electronic records, and the management thereof (Adam 2007:24). An organisation, like Company X, needs to ensure that their records stored in the cloud comply with these standards. ISO 15489 (ISO 2001:7) states that

Records management policies, procedures and practices should lead to authoritative records...

ISO 15489 (ISO 2001:7) also identifies four characteristics for records that is required to create authoritative records. They are:

- **Authenticity:** An authentic record is a record that can be proved.
- **Reliability:** This is a record which can be trusted to represent a full account of what it is claiming to represent.
- **Integrity:** The record must not have been altered, tampered with and is complete.
- **Usability:** A record needs to be locatable, have the ability to be retrieved, produced and be interpreted.

In order to determine if cloud computing is viable, these characteristics need to be considered when selecting a cloud service provider for records management. Cloud service providers should be questioned if they do comply with International Standards, such as ISO 15489.

#### **6.3.2.2 AS 5044 (AGLS Metadata Standard)**

Metadata is known as “data about data” (National Archives of Australia 2010:2). The Australian Standards AS 5044 is also known as the AGLS (Australian Government Locator Service) Metadata Standard. The AGLS Metadata Standard is a national standard, which is used to provide details on how online resources need to be described in order to improve their accessibility, visibility, manageability and interoperability (National Archives of Australia 2010:3; National Archives of Australia 2013b).

The manner in which documents are tagged with metadata (search keywords) may determine how they can be found and filtered more efficiently in a search engine. Furthermore, this may ensure that if an organisation needs to provide any records for legal issues, such as eDiscovery, then the required records may be retrieved with haste (see **Chapter 4 Section 4.3.2**).

### **6.3.2.3 ISO 16175 (Information and Documentation)**

The Information and Documentation Standard ISO 16175 includes the functional and principle requirements for records created in an electronic office setting (National Archives of Australia 2013b).

These functional requirements in ISO 16175 are based on the record keeping requirements stipulated in ISO 15489. However, it does not include the requirements for preserving records for long periods of time (National Archives of Australia 2013b).

In order for organisations to access the viability of cloud computing for their records management needs, they must assure that the cloud service provider selected is compliant with these ISO standards. Furthermore, cloud service providers must be able to establish the authenticity, integrity and confidentiality of information that they are hosting (Convery 2010:4). If the provider complies with international standards, then the risk of any legal complications towards them may be reduced.

## **6.4 Benefits of records management in the cloud**

For records management, the use of cloud computing, its cloud based applications and services can allow access to computing resources at any time of day. In addition to this, cloud computing helps improve business processes and promote a collaborative and geographically independent work environment (Convery 2010:10). This is beneficial for records management, as records being stored in the cloud will also gain these benefits (see **Chapter 3**).

In **Chapter 3**, the ten potential benefits of cloud computing were identified. With regard to record keeping and cloud computing, the following benefits have been identified.

- Reduced costs
- Less pressure on ICT to provide increased storage capacity
- Service access in various locations
- Collaborative opportunities with various geographically located individuals

- Potential for improved automation such as record keeping as part of business processes
- Increased time for more work due to reduced server maintenance time required.

These are elaborated on below:

#### **6.4.1 Reduced costs**

Reduced costs are identified in **Chapter 3, Section 3.3.1**, under the potential benefit *Cost efficiency*. Reduced costs in areas from hardware to software is a benefit for records management in the cloud as it provides more cost effective options. There are additional cost saving areas such as lower implementation costs and reduced operating costs. There is an overall reduced cost on the hosting of records from a Pay-per-use model in the cloud due to these benefits.

#### **6.4.2 Less pressure on ICT to provide increased storage capacity**

Cloud computing has the *Scalability and flexibility* benefit, (see **Chapter 3 Section 3.3.2**), which allows users to rapidly scale up or down resources based on their needs. Due to this scalability, there is less pressure on organisations' staff to forecast their storage requirements. Cloud computing provides effective resource monitoring to allow for an organisation's fluctuating storage requirement needs.

#### **6.4.3 Service access in various locations**

Cloud computing provides a *Greater mobility* benefit (see **Chapter 3 Section 3.3.7**). This allows for records to be accessed in various geographic locations from mobile devices.

#### **6.4.4 Collaborative opportunities with various geographically located individuals**

This benefit also draws from the *Greater mobility* benefit (see **Chapter 3 Section 3.3.7**). Where due to cloud computing's ability to provide access to records from

any location through the internet, it also allows for users to collaborate on documentation together despite being separated by distance.

#### **6.4.5 Potential for improved automation such as record keeping as part of business processes**

As identified in **Chapter 3, Section 3.3.8** cloud computing is able to provide *Improved power, automation and support management*. As a benefit for records management, this automation can allow for the automatic scaling of storage space required, based on the user's need.

#### **6.4.6 Increased time for more work due to reduced server maintenance time required.**

*Availability and reliability* (see **Chapter 3 Section 3.3.4**) as a benefit for records management allows for users to access their records at any time they require it and from any location.

### **6.5 Risks of records management in the cloud**

**Chapter 4** identified the ten risks and challenges associated with cloud computing. The Australasian Digital Recordkeeping Initiative (2010:9) identified the following risks with regard to record keeping and cloud computing:

- Identification of risks involved with using cloud computing service providers
- Assessing risks for different records
- Perform due diligence when selecting a service provider
- Contractual arrangement to manage risks
- Monitor arrangements with service providers

These are elaborated on below:

#### **6.5.1 Identification of risks with using cloud computing service providers**

According to the Australasian Digital Recordkeeping Initiative (2010:9-11), the maintenance and storage of records with a cloud service provider has numerous risks, such as:

- Legal or standard compliance, with record-creating jurisdiction, where the provider may fail to comply.
- Records may fall under the jurisdiction or other requirements of the hosted country.
- The unauthorised access of stored records may have other associated risks, such as deletion of records.
- The loss of access to records; and
- The value of records as evidence may be damaged (see **Chapter 4** for detail on cloud computing's risks and challenges).

Digital records stored in the cloud are affected by the same risks as records stored in other locations. However, cloud computing does contain additional risks such as:

- Individuals in other locations taking control, or claiming ownership of the records
- Loss of record access due to provider going out of business, or changing ownership
- Records being charged for return, or not returned upon request
- Provider upgrading their IT infrastructure which may cause compatibility issues with client, or record loss upon its return
- Poor backup and restore facilities due to provider cutting costs
- Record disposal by service provider without clients' permission

(Australasian Digital Recordkeeping Initiative 2010:10).

These risks are due to the unique characteristics of cloud computing, such as *Resource pooling* and *Broad network access* (see **Chapter 2 Section 2.4**). This is where the consumer may not be aware of the physical location of their stored records (unless stipulated). Furthermore, due to cloud computing's broad access, through multiple platforms from any location, there may be risks of unauthorised access. This can draw into question the viability of cloud computing for records management. It should be noted that even if a company used a non-cloud based provider for records management, there would always be risks to records hosted offsite. For example, an offsite-hosting service can still be affected by a disaster or



network issues (see **Chapter 4 Section 4.3**). However, when records are hosted externally, in the cloud, it becomes the cloud service provider's responsibility to ensure that the client's stored data is secure. It is the client's responsibility to ensure that the provider is able to protect this stored data (Convery 2010:13-14).

### **6.5.2 Assessing risks for different records**

The levels of risk of utilising a cloud provider for records storage is dependent on the assigned sensitivity, or importance of the records that an organisation wishes to store. If these records are too sensitive, then the organisation may decide not to utilise cloud storage for records.

For example:

- Records required for legal proceedings such organisations may be unable to prove that records have not been tampered with
- Special, secretive or confidential documents
- Records containing important information pertaining to individuals
- Commercially valuable records.

(Australasian Digital Recordkeeping Initiative 2010:11)

Legal compliance and auditability (see **Chapter 4 Section 4.3.2.3**) need to be carefully considered when utilising cloud computing for records storage. This is because organisations need to comply with the laws of their own country and the cloud-hosted data must comply with the laws of the country where the data is stored.

### **6.5.3 Preform due diligence when selecting a service provider**

The Australasian Digital Recordkeeping Initiative (2010:12) advises organisations that are selecting a cloud service provider to perform due diligence. This includes checking reference sites. They need to ask service providers about issues such as:

- Additional costs
- Privacy contracts
- External auditing

- Service disruption
  - Back up procedures
  - Restoration procedures
- Access restrictions

As mentioned earlier, AS ISO 15489 provides best practices for both paper and electronic records and the management thereof (Adam 2007:24). This standard touches on issues relating to records management process and controls, such as records retention (ISO 2001:11).

These issues must be discussed with the cloud service provider beforehand. Any additional concerns must be clarified and stipulated in a service level agreement (SLA). Concerns may be, for example, how data can be restored in the event of an incident (see **Chapter 4 Section 4.3.5 Incident response, notification and remediation**) or issues relating to *Availability and reliability* of services in the event of service disruptions (see **Chapter 3 Section 3.3.4** and **Chapter 4 Section 4.3.10**). How a cloud service provider deals with these issues will help determine whether or not they are a viable option for records storage for an organisation.

#### **6.5.4 Contractual arrangement to manage risks**

Contractual arrangements with cloud service providers must establish certain conditions. These conditions include:

- Record ownership remains with the organisation.
- Records are returned, as well as any metadata associated with the records, to the organisation upon request.
- The organisation is responsible for the management of records.
- Recordkeeping meets the organisations requirements.
- Privacy issues relating to records
- Stored records are used only by applications stipulated in the contract.
- Records are not shown to third parties without permission.
- Destruction of records are only done with the organisation's permission.
- Records are not transferred to a third party, without the organisation's permission.

On conclusion of the contract, all records are returned to the organisation in an accessible format and remnants are removed permanently from the providers' systems (Australasian Digital Recordkeeping Initiative 2010:12-13).

A contractual agreement must be drawn up to mitigate these concerns and should take into account the rights and responsibilities as identified by Gartner (2010) (see **Chapter 4 Section 4.3.9.1 Cloud Computing rights and responsibilities**). If a cloud service provider is unwilling to discuss these issues with prospective clients, then an alternative cloud provider may be a more viable option.

### **6.5.5 Monitor arrangements with service providers**

SLAs are a challenge for clients looking to utilise cloud computing for the storage of their data (see **Chapter 4 Section 4.3.2.2**). SLAs should be established between the cloud service provider and the organisation looking to utilise them for records storage. The SLA should contain performance provisions to ensure that the service provider maintains the information management and recordkeeping objectives over time. This SLA should also include that the service provider informs the organisation of any changes related to data arrangements, with regard to:

- Changes of storage location
- Recovery and back up procedures
- Security controls (Australasian Digital Recordkeeping Initiative 2010:14)

These risks, as well as the risks identified in **Chapter 4**, coincide with the risks identified by McKemmish (2013:20), who identified risks of records in the cloud to include:

- **Privacy:** This includes issue related to information privacy and confidentiality (see **Chapter 4, Section 4.3.2.1b**), where information hosted by a cloud service provider could be hosted offshore. This opens that information up to the jurisdictional laws of that country. For example, the USA and the Patriot Act.
- **Security:** Which includes a wide array of concerns from surface attacks, to unauthorised access (see **Chapter 4, Section 4.3.3**).

- **Authenticity:** This coincides with the characteristics identified by ISO 15489 (see **Chapter 6 Section 6.3.2.1**).
- **Integrity** This coincides with the characteristics identified by ISO 15489 (see **Chapter 6 Section 6.3.2.1**).
- **Accessibility:** This risk is concerned with accessibility of records; can they be accessed, who can access them and are they always accessible? (see **Chapter 4, Section 4.3.3.1 b**) and **Sections 4.3.10**).
- **Digital continuity:** This risk is concerned with integrity, availability and confidentiality (see **Chapter 4, Section 4.3.3.7**).
- **Lack of transparency of the cloud service:** This risk pertains to the cloud service provider and certain aspects of its operations, such as data hosting location, security services etc. (see **Chapter 4 Section 4.3.3.4** and **4.3.3.5**).

In addition to the risks mentioned in this chapter, records management in the cloud will also draw on the associated risks of cloud computing, such as those identified in **Chapter 4**. Many of these risks overlap as identified by McKemmish (2013:20). However, cloud computing does provide an excellent improvement on traditional records management, as it brings with it all of its unique benefits identified in **Chapter 3**.

## 6.6 Summary

This chapter identified that Australian organisations, which store records in the cloud, are subject to laws such as the *Electronic Transactions Act* 1999 (Australia 2011:14-15). Organisations such as Company X need to ensure that if they select a cloud service provider, they must ensure that they and the provider are compliant with this act. Organisations should also comply with International Standards. These Standards include: AS ISO 15489; AS 5044; ISO 16175.

Cloud computing brings specific benefits (see **Chapter 3**) which have a positive influence on its viability for records management. However, in addition to the risks of cloud computing identified in **Chapter 4**, care should be taken in the following areas:

- Identifying risks involved with using cloud computing service providers

- Assessing risks for different records
- Performing due diligence when selecting a service provider
- Forming contractual arrangement to manage risks
- Monitoring arrangements with service providers

No record keeping initiatives are without risk. Thus, cloud computing as an avenue is the same. Its viability can be debated one way or the other. However, it is down to each individual organisation to decide whether or not cloud computing is a viable option for records management. As each organisation is different, what suits one may not suit another. Stuart & Bromage (2010:223) reinforce this by stating that,

*Although the cloud does carry risks it is not a threat in itself, what is risky for one organisation may be acceptable for another organisation.*

In the **Chapter 7**, the research methodology for the research and more specifically the case study will be explained.

## Chapter 7 Research methodology

### 7.1 Introduction

According to Leedy & Ormrod (2013:2),

Research is a systematic process of collecting, analysing, and interpreting information (data) in order to increase our understanding of a phenomenon about which we are interested or concerned.

Research methodology must support research in attaining its goals and objectives set out by the research questions (Rodrigues 2013:205). This research was done in three stages.

- 1) Stage 1 was the literature analysis to provide a theoretical basis of understanding, as well as to answer the following research questions:
  - What are the potential benefits of cloud computing?
  - What are the challenges and risks associated with cloud computing?
  - To what extent is cloud computing a viable option for records management?
  - How can cloud computing be used to foster innovation within an organisation?

These have been reported in **Chapters 2-6**.

- 2) Stage 2 comprised the analysis of the case study results of a specific company, Company X, in order to answer the research question.
  - To what extent is cloud computing a viable option for records management?

The analysis is presented in **Chapter 8**.

- 3) Stage 3 comprised the conclusions, recommendations, final discussions and suggestions of areas of future research. This was done for all research questions addressed in stages one and two. This is presented in **Chapter 9**.

The focus of this chapter is on stage two. The aim of this chapter is twofold:

- Firstly, to explain how the analysis of the case study was conducted.
- Secondly, to outline the research methodology used by Company X, when the case study was originally conducted in 2012.

## **7.2 Research type**

Before an explanation of the research methodology, it is important to establish the type of research that was conducted. This was applied research, which is used to solve real, practical and specific world problems (Connaway & Powell 2010:2; Hancock & Algozzine 2006:5). In the case of this research, problems such as records management issues were examined, and the extent to which cloud computing can be a viable solution to these problems was explored. This study utilised an applied research approach in its analysis of a case study's results, in order to answer the research question:

- To what extent is cloud computing a viable option for records management?

## **7.3 Research philosophy**

The research philosophy of this study follows a pragmatic philosophy. Pragmatism follows the belief that the most important factor in research philosophy is the research question. A pragmatic philosophy is concerned with one approach, such as a qualitative approach, which may be better suited to answer a specific research question (Saunders, Lewis & Thornhill 2007:110). In this research, a qualitative approach was applied to the results of a case study findings, analyses, and the analysis of the reported research from the literature.

## **7.4 Research methodology**

This research utilised a qualitative approach, undertaken in its natural setting (Mouton 1996:168), in this case, Company X offices. A qualitative approach was used to gather data in order to learn more about, and understand a situation, rather than trying to explain, or even predict the phenomena in question. (Bhattacharjee 2012:115; Creswell 2002:14-15; Connaway & Powell 2010:80;

Mouton 1996:168). The situation in this research is Company X's case study results and cloud computing's viability.

In the case of this research, the researcher was working with more than one data source. These sources were the results from a case study, as well as a literature analysis reported on in previous chapters.

## **7.5 Research design**

In its most basic sense, the research design is the logical progression that connects the empirical data to the study's research questions and to its conclusions (Yin 2003:20). For the analysis of the literature, a descriptive design was used.

The investigation of the case study results is explorative in nature and seeks to develop ideas for further study (Yin 2003:120). The explorative design was appropriate for this research because in explorative case studies, the data collection and fieldwork may be conducted before the research definition and even the research questions are formulated (Tellis 1997). Company X conducted the case study in 2012. Subsequently, the researcher formulated the research problem, research questions and specific objectives pertaining to the research reported on in this dissertation. The research design was then developed with the focus on the analysis of the case study results.

Yin (2003:21-27) identifies five components of a research design, which are important and relevant to this study. These are discussed below with relation to the research at Company X:

**1. A study's questions:** These questions help identify what research strategy should be used, questions in terms of who, what, where, how and why (Saunders *et al.* 2007:139). This research was aimed at answering questions of how and what, such as:

- What are the potential benefits of cloud computing?
- What are the challenges and risks associated with cloud computing?



- To what extent is cloud computing a viable option for records management?
- How can cloud computing be used to foster innovation within an organisation?

**2. A study's propositions:** If there are any propositions in the study, then it directs the researcher's attention towards an area that should be examined within the study's scope. This study's proposition came from the research question:

- To what extent is cloud computing a viable option for records management?

This led to the following objectives or areas in the study:

- Determine cloud computing's potential benefits, risks and challenges
- Determine cloud computing's viability for records management
- Identify ways in which cloud computing can help promote innovation and innovative thinking within an organisation.

**3. Unit of analysis:** This component is connected with determining the nature of the case, such as, what is the actual case? (Tellis 1997; Yin 2003:22). In this research, the unit of analysis was Company X's case study findings.

**4. Logical linking of the data to the propositions:** A common approach here in logical linking of data is a pattern matching technique (Yin 2003:27). The analysis for this case study's findings used an analytical technique, known as explanation building. This is a special type of pattern matching process, with a goal to analyse the case study data through constructing an explanation about the case (Yin 2003:120). This is done through the stipulation of casual links between the phenomena being examined. The case study was used to help determine cloud computing's viability for records management at Company X. The case study results were examined and themes were created and revised. Thereafter, the results were re-examined from a new perspective. This was done to gradually

build up and refine the explanation (Yin 2003:122). In this case, the results contributed in answering the question on the viability of cloud computing.

- 5. Criteria for implementing the findings:** These last two components of research design are the least developed in case study research (Tellis 1997; Yin 2003:27). Unfortunately, according to Yin (2003) there is no accurate or standardised method for implementing the criteria for findings. In this research, the case study's analysis was compared against the literature analysis, done in **Chapters 3, 4, 5 and 6** in order to answer the research question on viability.

## **7.6 Research analysis**

In qualitative research, the emphasis is not on explaining or predicting phenomena but, rather on understanding them (Bhattacharjee 2012:113). Corbin & Strauss (2008:31) have stated that:

No researcher should become so obsessed with following a set of coding procedures that the fluid and dynamic nature of qualitative analysis is lost. The analytic process, like any thinking process, should be relaxed, flexible, and driven by insight gained through interaction with data rather than being overly structured and based only on procedures.

This means that although there are techniques and analytical processes to help guide the analysis of research, the researcher must be able to extrapolate from the research based on their own interaction with the data and not be constrained by rigid methods, which may impact and deter from the thought process. For this research, there was a qualitative approach to analysis with more than one research tool being used, that is the literature analysis of the reported research as well as the analysis of the case study results.

## **7.7 Justification for case study selection**

The mining environment is a hazardous and remote environment where clients may be situated in remote locations, with limited access to the Internet. Company

X is a mining software development company, which provides specialised services relating to consulting, mining shaft designs and mining software development. These tasks require Company X to be able to access and store their relevant records and project data wherever a client may be. Company X was experiencing various issues, such as file duplication and multiple versions of files, with their current internal storage system. Company X constructed a case study to access its internal server layout and the documentation practices of departments. The case study provided an analysis and interpretation of the results as well as a recommendation for a new server layout. This dissertation examined the results of these findings.

Case study research can use either a single or multiple case studies (Yin 2003:14). This research investigated a single case study's results for analysis. This case study was selected to help determine cloud computing's viability (for Company X) because at the time Company X was beginning the process of a server reorganisation in order to improve their documentation practices.

The case study conducted by Company X was selected due to the following factors:

**Specialised operating environment:** Company X operates with a specialised field, which deals with issues such as:

- Limited connectivity
- Remote locations of clients
- Everywhere accessible data
- Costs
- Security of stored data

These issues provide an environment where cloud computing adoption could be targeted towards.

**Consideration of cloud computing:** It is due to these issues, as well as the results from the case study that led to the consideration of cloud computing for

Company X. It is based on the findings from the questionnaire (see **Annexure A**), more specifically the questions from:

- Section A question 4,
- Section B question 13,14,16,17,18,19,21
- Section C question 22,23
- Section D question 24,25
- Section E question 32,33
- Section F question 34,35,36,37

Due to Company X considering cloud computing they allowed access to their case study for analysis for the purpose of this research.

**Various issues currently being experienced by current documentation practices:** Company X's departments were operating independently with regard to their documentation practices. The questionnaire was used to ascertain what these practices were in each of the departments.

This provided the researcher with an in depth understanding of issues that individual departments were experiencing. The viability of cloud computing was assessed by comparing these findings against the potential benefits, risks and challenges associated with cloud computing. These were identified and discussed in **Chapter 3** and **Chapter 4**. *The ten potential benefits of cloud computing* that were identified are:

1. Cost efficiency
2. Scalability and flexibility
3. Modernisation of business processes
4. Availability and reliability
5. Rapid developments and deployments
6. Business continuity and disaster recovery
7. Greater mobility
8. Improved power, automation and support management
9. Improved security
10. Green IT/ Green computing

*The ten risks and challenges associated with cloud computing discussed were:*

1. Compliance
2. Legality and auditability
3. Security
4. Everywhere accessible data
5. Incident Response, Notification and Remediation
6. Virtualisation
7. Governance and enterprise risk management
8. Interoperability, portability and data lock-in
9. Viability
10. Availability and reliability

The case study's results have been analysed to provide a practical perspective of the specific issues identified by the company. This will help indicate the viability of cloud computing for records management, specifically for a mining software development company.

### **7.8 Case study research methodology**

According to Hancock & Algozzine (2006:9-10), a case study is representative of a type of qualitative research. It involves the use of in-depth analysis and the description of a singular system, or unit, where the researcher aims to reach an in-depth understanding of the situation under analysis. For this research, the singular system was Company X. The research for this dissertation focussed on the analysis of the case study results only. However, the methodology utilised during the execution of the case study is given to provide an understanding of how the case study was conducted.

A qualitative case study is an in-depth, holistic description and analysis of a situation, such as an organisation, process, social unit, program or person (Merriam 2009:X). The organisation in this case study is Company X, a mining software development company in Australia. The case study on Company X was constructed using a qualitative approach, where data was gathered through a questionnaire, which was completed by the relevant departmental heads (see

**Annexure A).** The gathered data from the questionnaire was organised into common themes, where links between the gathered data were noted. Once the data was analysed common themes were drawn out which led to the identification of problem areas. The problem areas identified from the questionnaire were originally used to help reorganise the organisation's server layout and enhance the document management standard that was in use. The reorganisation of the server layout did not fall within the scope of this dissertation.

### **7.9 Case study research design**

With Company X's case study, being qualitative in nature, the aim was to gain an in-depth and descriptive understanding of the documentation practices within the company (Hancock & Algozzine 2006:9-10).

The section below discusses the population and questionnaire used in the research for the creation of Company X's case study, as well as how the results of the questionnaire were used.

### **7.10 Case study population and questionnaire**

The case study's data was collected in the form of a questionnaire in 2012. The case study drew on a targeted population within the organisation. The organisation (Company X) selected specific departments and the heads of these departments to answer the questionnaire. This was done to provide greater support and a fuller understanding of the departments' functioning. These departmental heads were the key users within the individual departments. They also had further interaction with other departments and information shared amongst each other, including data collection procedures and methods.

The population sample used in the case study of Company X's was divided into seven departments, of which five<sup>2</sup> were analysed for the purpose of Company X's study, namely the:

---

<sup>2</sup> The Finance and Human Resources (HR) departments were consulted but not analysed. The reason for this was due to confidentiality issues and at the request from Company X.

- **Consulting Department:** responsible for mining related projects and consulting services
- **Marketing Department:** responsible for public branding and marketing of products
- **Project Management:** responsible for software projects and development
- **Business Development:** responsible for client relations and new business
- **Training and Technical Writing:** responsible for technical documentation for software products.

### 7.10.1 Questionnaire

The questionnaire was divided into six sections, or themes, which were used for analysis:

- Section A: Work tasks
- Section B: Record types
- Section C: Issues
- Section D: Storage location
- Section E: Shared usage
- Section F: Solutions proposed by departments.

The findings of each of these themes will be analysed in **Chapter 8**.

The questions involved were a mixture of both open-ended and close-ended questions (see **Annexure A**). The questionnaires were completed in writing by the relevant departmental heads. Common issues experienced by them were identified, based on the sorting and cross referencing of their responses. Issues such as categorisation, server downtime and duplication of records were identified and the new server layout was then designed for Company X. The responses for the questionnaire have been analysed in **Chapter 8** for the purpose of addressing the research problem and research questions covered by this dissertation. The design of the new server layout does not form part of this research problem and is therefore not discussed in this dissertation.

As stated in **Chapter 1**, the purpose of this study has been to investigate the viability, benefits and challenges of cloud computing. This was done in order to provide information to determining whether or not cloud computing is viable as an alternative to traditional records management options. This was done through analysing the results of a case study that was conducted on an organisation's documentation practices and server layout. In addition, this research aimed to reveal how cloud computing could be used to promote innovation within an organisational setting.

### **7.11 Case study validity and reliability**

When conducting research, it is important to establish validity. Validity and reliability are discussed in relation to the case study being analysed for this research. Validity applies when the concepts' definition accurately matches what is observed in practice or reality (Babbie 2008:160, Du Plooy 2009: 70,135).

With regard to the validity of the case study for this dissertation, this case study and its results are considered valid as the study was done as a self-improvement tool aimed at improving the internal functioning of the organisation.

#### **7.11.1 Construct validity**

The case study of Company X was used as a form of validity known as construct validity. Construct validity is used for constructing the correct operational measures for the concepts that are being studied. This can be done in three ways, according to Yin (2003:36)

- First is through utilising multiple sources of evidence during data collection.
- Second is to establish a chain of evidence during data collection.
- Third is to have the case study draft reviewed by key informants.

Company X utilised the third way for establishing validity. The case study utilised a questionnaire to gather data. The Vice President of Company X, to ensure its validity, reviewed this case study, as well as the questionnaire. This was considered an appropriate method to ensure validity in this dissertation, as the case study was to improve Company X's internal documentation practices.



### 7.11.2 Reliability

Reliability refers to the internal consistency of measurement, which heralds the same result at different periods of time (Du Plooy 2009:131). This study analysed the data that was gathered through questionnaire used by Company X. The questionnaire was used as a form of intercoder reliability testing. Intercoder reliability testing is the reviewing of the questionnaire by an external party to determine whether bias, or misrepresentation would occur (Du Plooy 2009:133-134). In this case, the Vice President of Company X, who was not being analysed, reviewed the questionnaire and approved it. The questionnaire is included in **Annexure A**.

### 7.12 Ethical issues

This section outlines the ethical considerations taken with regard to the case study of Company X. According to Mouton (1996:42) ethics in research are focused on the preservation of the interest and the rights of those participating in the research. These rights are informed consent, privacy and confidentiality.

This coincides with the principles of research provided by Unisa (2012:9), Mack, Woodsong, Macqueen, Guest & Namey (2005:9), which are

- **Autonomy:** respecting individual rights, autonomy and dignity of those involved in the research.
- **Beneficence:** which is to maximise the benefits of the research to the research participants.
- **Nonmaleficence:** which is to minimise the risks (social and physiological) to those involved in the research.
- **Justice:** to ensure that the benefits and risks are distributed fairly to those involved in the research.

The case study conducted by Company X adhered to these issues in the following ways:

The questionnaire was presented to departmental heads, with regard to ascertaining their entire department's documentation practices, not at the

individuals themselves, thus ensuring individual confidentiality and privacy (autonomy) of the departmental members.

The issue of informed consent was discussed beforehand with each individual departmental head, informing them of:

- The purpose of the research
- What the research would entail
- What was expected of the participants
- Confidentiality of their departmental members

This was done to ensure nonmaleficence by informing the participants of the details of the study and ensuring their wellbeing.

Individuals were given a copy of the completed case study to ensure that they were treated fairly and their responses to the questionnaire were not incorrect.

Company X's vice president granted approval for the case study to be used for the purpose of this research, on the grounds that the company name, any specific company details and details relating to the individuals involved in the case study, would be omitted from this dissertation, ensuring both the company as well as the individuals' privacy.

### **7.13 Case study results analysis**

The case study results analysis has been done through the creation of a matrix of categories or themes. These are:

- Work tasks
- Record types
- Issues
- Storage location
- Shared usage
- Solutions proposed by departments

The results obtained have been sorted into these themes. Once these common themes were identified, the case study results were re-examined from this new perspective to determine cloud computing's viability. This was done through cross-referencing the results of the analysis against the potential benefits and the risks and challenges associated with cloud computing.

#### **7.14 Summary**

This chapter provided a review of the research methodology used in this dissertation, including the research type, research philosophy, methodology, design and analysis. This chapter also outlined the research methodology that was used in the case study conducted by Company X, including the research design, tools for gathering data, the population sample, how the data was analysed and the applicable ethical considerations.

In **Chapter 8**, the analysis of the case study results is presented.

## Chapter 8 Case study analysis and interpretation of research findings

### 8.1 Introduction

This chapter reports on the analysis of the case study findings in order to help answer the research question:

- To what extent is cloud computing a viable option for records management?
- How can cloud computing be used to foster innovation within an organisation?

These questions have been answered with regard to Company X only. The analysis of these findings is compared to the reported research conducted in **Chapters 3,4** and **6** in order to determine cloud computing's viability for records management for Company X. The case study findings are also compared to the reported research in **Chapter 5**, in order to determine how cloud computing can be used to foster innovation within an organisation.

### 8.2 Case study findings analysis

The case study was conducted on Company X. The population sample was seven departments, of which only five were analysed.

These were the:

- **Consulting Department:** responsible for mining related projects and consulting services.
- **Marketing Department:** responsible for public branding and marketing of products.
- **Project Management Department:** responsible for Software projects and development.
- **Business Development Department:** responsible for client relations and new business.
- **Training and Technical Writing Department:** responsible for technical documentation for software products.

Company X used the questionnaire to identify:

- Which individuals create documentation?
- Which individuals work on documentation?
- Which individuals access documentation?
- How this documentation is used?
- Types of documentation used?
- Current information management procedures
- Types of documentation used per department?
- Where is this documentation stored?
- Documentation formats

### 8.2.1 Common themes identified

The case study findings were gathered from a questionnaire. These related findings have been categorised together in **Table 8.1**. The themes have been used by the researcher to identify the benefits, risks and challenges Company X could be affected by, or gain, if adopting cloud computing for their records management needs.

**Table 8.1 Common themes identified**

Common themes identified	
<b>Work tasks</b>	This theme groups together what tasks (work) are performed by each department (see <b>Section 8.2.1.1</b> for more detail).
<b>Record types</b>	This theme is a combination of data sources and data types (see <b>Section 8.2.1.2</b> for more detail).
<b>Issues</b>	The issues experienced by each department are grouped together under this theme (see <b>Section 8.2.1.3</b> for more detail).
<b>Storage location</b>	This theme is comprised of storage locations that the departments utilise (see <b>Section 8.2.1.4</b> for more detail).
<b>Shared usage</b>	This theme combines the sharing and usage of data files (see <b>Section 8.2.1.5</b> for more detail).
<b>Solutions proposed by departments</b>	This theme groups together any solutions proposed by the departments (see <b>Section 8.2.1.6</b> for more detail).

### 8.2.1.1 Work tasks

In this theme the tasks (work) performed by each department are grouped together, for example: resource management, project management, marketing material creation etc. (see **Table 8.2 Work tasks**)

**Table 8.2 Work tasks**

Departments	Work tasks
<b>Marketing Department</b>	The department's tasks range from collateral development (Marketing material e.g. flyers) to the creation of templates and contact lists.
<b>Business Development Department</b>	Tasks range from the creation of quotes, to licences maintenance for software, sales material generation, support and developing marketing channels.
<b>Consulting Department</b>	Work tasks include the forecasting of consulting work, quotes, contracts, purchase orders, invoicing, transfers, and actual project work.
<b>Project Management Department</b>	The department handles resource management, financials, contracting, project initiation, issue management, documentation, project management, quality control, relationship management, reporting, risk, organisation and administration.
<b>Training and Technical Writing Department</b>	The department creates and updates training documentation.

These are re-categorised into the following common elements under the theme *Work tasks*:

- Documentation creation
- Documentation editing
- Multimedia creation
- Sharing of documentation

### 8.2.1.2 Record types

This theme is a combination of data sources and data types, for example, project data, documents, multimedia such as videos and promotional material, etc. Also included are the sources from which the data files are received, for example, internal departments, clients, internet sources etc. (see **Table 8.3 Record types**).

**Table 8.3 Record types**

Departments	Types of records	Sources of information
<b>Marketing Department</b>	All record types are self-generated material e.g. media releases.	Information is received externally from offices in other countries.
<b>Business Development Department</b>	The department receives product information, marketing material (e.g. video clips).	Information is given by the Consulting Department, the Project Management Department, Perth office and Canada office.
<b>Consulting Department</b>	Project data files are utilised and generated depending on the work that must be completed.	Information is generated internally and from external stakeholders. Previous projects and templates are also utilised.
<b>Project Management Department</b>	Project data files are generated and previous files are utilised.	Information is received internally and from external stakeholders, also through previous projects and templates.
<b>Training and Technical Writing Department</b>	Technical write-ups and training documents are self-generated.	Information sent from external clients. Additional information gained through internet research.

These are re-categorised into the following common elements under the theme Record types:

- Documents
- Project files
- Multimedia
- Externally received information
- Internally received information

### **8.2.1.3 Issues**

Issues experienced by each department are grouped together, for example: server outages, poor categorisation of documents, hard drive failure, etc. (see **Table 8.4 Issues experienced**).

**Table 8.4: Issues experienced**

Departments	Issues experienced
<b>Marketing Department</b>	<ul style="list-style-type: none"> <li>• There is a lack of consistency of documentation formats and versions.</li> <li>• There is a lack of a centralised storage location for graphic files, which causes duplication and delays, as work is often redone unnecessarily.</li> <li>• Documentation is difficult to locate as there is no logical storage procedure and documents are often stored in the incorrect locations on the server.</li> <li>• Files are worked on the PC and not off the server. These files are only backed up to the server when completed on a monthly basis.</li> <li>• Backups are done monthly due to the server being inaccessible at times which causes work disruptions.</li> </ul>
<b>Business Development Department</b>	<ul style="list-style-type: none"> <li>• Material from the <b>Marketing Department</b> needs rebranding, lack of knowledge of their work causes delays.</li> <li>• Need for greater client visibility, all their relevant information in a centralised place.</li> <li>• There is file duplication; a better file naming system is required to reduce this.</li> <li>• A better method for locating files is needed.</li> <li>• Information is in uncategorised text and is stored in emails.</li> <li>• A constant internet connection is required for work.</li> </ul>
<b>Consulting Department</b>	<ul style="list-style-type: none"> <li>• There is massive duplication of project data and conflicting versions of files.</li> <li>• There is no set storage structure for naming of files.</li> <li>• A life cycle management for files from the Marketing Department is required as there is material that needs to be transferred to the marketing department.</li> <li>• Shared policy documentation needs to be reviewed/stored in a centralised location.</li> <li>• There is an incomplete training database which needs to be linked with <b>Business Development Department's</b> Salesforce solution.</li> <li>• Information is stored in emails and PCs, not on the server.</li> <li>• The department head stored information on PC with no back up and the hard drive failed causing massive data loss.</li> </ul>
<b>Project Management Department</b>	<ul style="list-style-type: none"> <li>• Team members need the ability to update time sheets based on hours/ per project</li> <li>• Duplication is an issue due to poor searching capabilities on the server.</li> <li>• A structured storage location on the server with a correct filing system is required. The current one is not being followed in other departments.</li> <li>• A lack of communication and non-standardised SLA has led to issues on projects.</li> <li>• All project information must be retained for legal compliance.</li> </ul>
<b>Training and Technical Writing Department</b>	<ul style="list-style-type: none"> <li>• A centralised storage location is required on the server that can be accessed by all.</li> <li>• A standard is needed to limit the creation of multiple documents and versions which is causing a duplication of work.</li> <li>• Files are being stored based on their content.</li> </ul>

These are re-categorised into the following common elements under the theme Issues. These are:



- Lack of consistency of documentation formats
- Multiple versions of documentation
- Lack of centralised storage locations
- Delays in work caused by searching for documentation
- Duplication of work
- Various storage locations
- Documentation stored in incorrect locations in wrong departments
- Poor search facility to locate documentation on the server
  - Visibility of client information and records
- Documentation worked on local PC and backed up infrequently (monthly)
- Documentation backed up to server only when completed in final version
- Server can be unavailable (offline)
- No consistent document categorisation standard
  - Each department and each user names files differently
- Uncategorized documentation remain stored in their original received emails.
- Project files are massive and compressed to save space on the server.
- Constant internet connection is required for work.
- Information loss due to PC failure
- Documentation needs to be updated daily on server.
- Lack of communication and knowledge about other departments' documents causes issues and duplication of work.
- Documentation needs to be retained (project documents) for legal compliance.

#### **8.2.1.4 Storage location**

This theme addresses the issue of storage locations that the departments utilise, for example, local hard drives, internal servers, etc. (see **Table 8.5 Storage location**).

**Table 8.5 Storage location**

Departments	Storage location
<b>Marketing Department</b>	<ul style="list-style-type: none"> <li>Information is stored in a shared folder on the server.</li> <li>Files are stored alphabetically and based on type of work; numbers are given to indicate versions of documents. Completed files are given a prefix of "A" to move files to the top of the folder once completed.</li> <li>Frequently accessed files are stored on a PC not on server.</li> </ul>
<b>Business Development Department</b>	<ul style="list-style-type: none"> <li>Certain product information and marketing material is shared via Dropbox to select individuals in the Perth Office; this is due to large size of files.</li> <li>Files are stored locally and backed up to server. There is no categorisation system for documents.</li> <li>Files are stored in emails in original received formats.</li> </ul>
<b>Consulting Department</b>	<ul style="list-style-type: none"> <li>Files are stored in various shared folders on the server.</li> <li>Files are named using an "in progress" prefix and filed by client on server with Finance department, categorisation is based on project status.</li> <li>The "transfers" files stored in shared server directories are in temporary locations.</li> <li>Project files are shared projects with other offices.</li> <li>Server project data is +-900 GBs when compressed to save space. Project data is backed up by an external supplier.</li> <li>Project data is copied to PC and edited (live projects). When completed it is backed up to the server.</li> <li>Information is managed and stored in emails and on individual PCs.</li> <li>Files are categorised based on a date and previously implemented filing system; project information is saved on the server.</li> </ul>
<b>Project Management Department</b>	<ul style="list-style-type: none"> <li>Project records are stored on an ftp website; records are archived and retained following project closure.</li> <li>Documentation follows the document naming convention stipulated by Company X and is categorised based on Company X document management standard.</li> </ul>
<b>Training and Technical Writing Department</b>	<ul style="list-style-type: none"> <li>Files are stored in centralised folder on server when completed; incomplete files are stored on a PC.</li> <li>Files are stored logically.</li> </ul>

These are re-categorised into the following common elements under the theme Storage location:

- Documentation stored locally on laptops

- Backed-up infrequently or monthly
- Backed-up when documents are completed only
- Various storage locations on server
- Each department utilises its own categorisation method.
- Company X Document Management Standard
- Cloud based storage
- Files stored in temporary folders on server
- Project data is backed up to an FTP server offsite.

### 8.2.1.5 Shared usage

This theme combines the sharing usage of data files, for example: internal departments, clients, international offices etc. (see **Table 8.6 Shared usage**)

**Table 8.6 Shared usage**

Departments	Shared usage
<b>Marketing Department</b>	<ul style="list-style-type: none"> <li>• Documentation is shared on request to all departments.</li> <li>• Templates and images are shared to all departments freely.</li> </ul>
<b>Business Development Department</b>	<ul style="list-style-type: none"> <li>• Documentation is shared on request to all departments.</li> </ul>
<b>Consulting Department</b>	<ul style="list-style-type: none"> <li>• Documentation is shared with all departments. However, select documents are shared with the Finance Department only.</li> <li>• Select documentation are also shared with <b>Training and Technical Writing Department.</b></li> </ul>
<b>Project Management Department</b>	<ul style="list-style-type: none"> <li>• Documentation is shared with all departments.</li> </ul>
<b>Training and Technical Writing Department</b>	<ul style="list-style-type: none"> <li>• Documentation is used by all departments and shared to all departments.</li> </ul>

These are re-categorised into the following common elements under the theme Shared usage:

- Shared to all departments
- Shared with select departments.

### 8.2.1.6 Solutions proposed by departments

This theme highlights any solutions proposed by the departments (see **Table 8.7 Solutions proposed**).

**Table 8.7 Solutions proposed**

Departments	Solutions proposed
<b>Marketing Department</b>	<ul style="list-style-type: none"> <li>• Offline file synchronisation to the server would help to reduce duplication and ensure latest files are available.</li> </ul>
<b>Business Development Department</b>	<ul style="list-style-type: none"> <li>• The department will be utilising Salesforce to increase visibility of client information. This will provide a centralised storage location of information.</li> </ul>
<b>Consulting Department</b>	<ul style="list-style-type: none"> <li>• A Switch to Excel-based timesheets and invoicing system.</li> <li>• Move away from email-based management of information/documents.</li> <li>• A design manager who handles versions and backups of files.</li> <li>• A standardised terms and conditions document stored in a central location.</li> <li>• A centralised overview of client information to allow faster creation of invoicing and allowing people in departments to view reports for the client.</li> <li>• Consultants in department would benefit from forecasts being made readily available to them as well as to management (including financial positions, models, market updates and pricing lists).</li> </ul>
<b>Project Management Department</b>	<ul style="list-style-type: none"> <li>• None given</li> </ul>
<b>Training and Technical Writing Department</b>	<ul style="list-style-type: none"> <li>• The department has created an inventory file system of all training material for ease of access.</li> </ul>

These are re-categorised into the following common elements under the theme Solutions proposed by departments:

- Offline file synchronisation
- Centralised storage locations on server
- Dedicated storage locations on server
- Salesforce (currently in process of being acquired).

These common themes and elements are tabulated graphically (see **Table 8.8**) and cross-referenced with each department, highlighting the common elements experienced by them all. This is done to compare against the potential benefits and the risks and challenges associated with cloud computing so that the viability of cloud computing can be determined.

**Table 8.8 Case study findings analysis**

Case study findings analysis					
Common themes and elements shared by departments	Marketing department	Training and Technical Writing department	Business Development Department	Consulting department	Project Management
<b>Work Tasks</b>					
• Documentation creation	✓	✓	✓	✓	✓
• Documentation editing	✓	✓	✓	✓	✓
• Multimedia creation	✓		✓		✓
• Sharing of documentation	✓	✓	✓	✓	✓
<b>Record types</b>					
• Documents	✓	✓	✓	✓	✓
• Project files				✓	✓
• Multimedia	✓		✓		
• Externally received information	✓	✓	✓	✓	✓
• Internally received information	✓	✓	✓	✓	✓
<b>Issues</b>					
• Lack of consistency of documentation formats	✓				
• Multiple versions of documentation	✓	✓	✓	✓	✓
• Lack of centralised storage locations	✓	✓			
• Poor search facility to locate documentation on the server	✓		✓		✓
• Documentation worked on local PC and backed up (monthly)	✓			✓	

Issues (continued)	Marketing department	Training and Technical Writing department	Business Development Department	Consulting department	Project Management
• Documentation backed up to server only in completed final version.	✓			✓	
• Server can be unavailable (offline).	✓				
• No consistent document categorisation standard.	✓	✓	✓	✓	✓
• Uncategorized documents stored in original received emails.			✓	✓	
• Massive project files are compressed to save space on the server.				✓	
• Constant internet connection is required for work.			✓		
• Information loss due to PC failure.				✓	
• Documentation need to be updated daily on server.					✓
• Lack of communication/ knowledge about other departments documentation causes issues and duplication of work.					✓
• Project documentation need to be retained for legal compliance.					✓
<b>Storage location</b>					
• Documentation stored locally on laptops.	✓	✓	✓	✓	✓
• Various storage locations.	✓	✓			
• Each department uses own categorisation for documentation.	✓	✓	✓	✓	✓
• Company X Document Management Standard.					✓
• Files stored in temporary folders on server .				✓	
• Project data is backed up to an FTP server offsite.					✓
<b>Shared usage</b>					
• Shared to all departments.	✓	✓		✓	✓
• Shared with select departments	✓		✓	✓	
<b>Solutions proposed by departments</b>					
• Offline file synchronisation.	✓				
• Centralised storage locations on server.	✓	✓	✓	✓	✓
• Dedicated storage locations on server.	✓	✓	✓	✓	✓
• Cloud based storage.			✓		
• Salesforce (currently in process being acquired).			✓		

## 8.2.2 Cloud computing’s viability based on case study findings analysis

These common themes and elements are now compared against the *Potential benefits of cloud computing* (see **Chapter 3**), as well as, *the risks and challenges associated with cloud computing* (see **Chapter 4**). This is done in order to determine if there will be factors, which impact on the viability of cloud computing for Company X. The *Potential benefits of cloud computing* are also compared against the *benefits of records management in the cloud* (see **Chapter 6**) in order to determine any overlap with regard to viability for Company X. This is also done under the subheading entitled: “*The risks and challenges associated with cloud computing and the Risks of records management in the cloud* (see **Chapter 6**).

### 8.2.2.1 Potential benefits vs. viability

In **Table 8.9**, the potential benefits of cloud computing have been compared against the case study analysis findings. These potential benefits have also been cross-referenced with the benefits of records management in the cloud.

**Table 8.9: Tasks and elements met by cloud computing’s potential benefits**

Ten Potential Benefits of Cloud Computing	Tasks and elements						
	Will gain benefit	Work Tasks	Record types	Issues	Storage location	Shared usage	Solutions proposed by departments
1. Cost efficiency	✓	✓	✓	✓	✓	✓	✓
2. Scalability and flexibility	✓	✓	✓	✓	✓	✓	✓
3. Modernization of business processes	✓			✓			
4. Availability and reliability	✓	✓	✓	✓	✓	✓	
5. Rapid developments and deployments							
6. Business continuity and disaster recovery	✓	✓		✓	✓		
7. Greater mobility	✓						
8. Improved power, automation and support management							
9. Improved security	✓	✓	✓	✓	✓	✓	
10. Green IT/ Green computing	✓ *	✓	✓		✓		

\*Indirect benefit gained through utilising cloud computing

In **Chapter 6** the benefits of the cloud for records management were identified, they included:

- Reduced costs
- Less pressure on ICT to provide increased storage capacity
- Service access in various locations
- Collaborative opportunities with various geographically located individuals
- Potential for improved automation, such as record keeping, as part of business processes
- Increased time for more work due to reduced server maintenance time required

In **Table 8.10**, these are compared against the *Potential benefits of cloud computing* for overlap of the same benefit, in order to help determine cloud computing's viability for records management for Company X.



**Table 8.10 Benefits of the cloud for records management vs. Potential benefits of cloud computing**

Ten Potential Benefits of Cloud Computing	Benefits of records management in the cloud					
	Reduced costs	Less pressure on ICT to provide increased storage capacity	Service access in various locations	Collaborative opportunities with various geographically located individuals	Potential for improved automation such as, record keeping as part of business processes	Increased time for more work due to reduced server maintenance time required
1. Cost efficiency	✓					
2. Scalability and flexibility		✓				
3. Modernization of business processes						
4. Availability and reliability						✓
5. Rapid developments and deployments						
6. Business continuity and disaster recovery						
7. Greater mobility			✓	✓		
8. Improved power, automation and support management					✓	
9. Improved security						
10. Green IT/ green computing						

These benefits are explained with regard to how they impact on Company X:

- **Cost efficiency** – There will always be a need for cost efficiency for an organisation, as organisations need to turn a profit in order to remain functioning. *Cost efficiency*, with regard to Company X and viability of cloud computing, would be connected with all tasks and elements: Storage location, document creation, sharing of documents etc. would be addressed through cloud computing. A lower cost of hosting records would draw upon this benefit.
- **Scalability and Flexibility** – Due to increasing growth of business and the need to retain all project data for compliance issues, Company X must expand its storage requirements.
- **Modernisation of business processes** – Business Development Department is acquiring Salesforce, a customer relationship management service (Salesforce 2013), for its specific needs.
- **Availability and reliability** – Certain departments require constant Internet connection and server access to be able to access records at any time, when work may be required. All tasks and elements would utilise this benefit as they all create, share and receive records.
- **Rapid developments and deployments** – Company X has not indicated any pretested or specific software needed for the work.
- **Business continuity and disaster recovery** – The Consulting department had a hard drive failure causing data to be lost. Cloud computing could have prevented this due to its backups and continuity capabilities. All tasks and elements would utilise this benefit as they require constant access to their records to continue work.
- **Greater mobility** – Company X deals with the mining environment and as such has customers in remote locations. The ability to continue work and access their records remotely from various locations is important.
- **Improved power, automation and support management** was not indicated as a requirement for Company X.

- **Improved security** – This is always a benefit to organisations because records need to be secure to prevent any malicious activity and loss of data.
- **Green IT/ Green computing** – This was not a direct requirement mentioned by Company X. However, Company X would no longer need to print documents when traveling to areas due to cloud computing. This would be an indirect benefit for Company X by reducing their carbon footprint.

Eight out of ten potential benefits for cloud computing could benefit Company X (see **Table 8.9**). Certain potential benefits may be assigned higher value than others, which may impact on the viability question for Company X. However, the value would have to be determined by Company X. For example, *Cost efficiency* may outweigh the *Scalability and Flexibility* potential benefit, as the need to expand resources when needed may not be as important as reducing costs.

#### **8.2.2.2 Risks and challenges vs. viability**

In **Table 8.11** the risks and challenges associated with cloud computing are similarly compared against the case study analysis findings related to the potential benefits. This was done to determine which risks and challenges would directly impact on Company X, if they were to utilise a cloud-based system for records management. These risks and challenges are also compared against the risks of records management in the cloud.

**Table 8.11 Tasks and elements effected by risks and challenges associated with cloud computing**

Ten Risks & challenges associated with Cloud Computing	Tasks and elements						
	Will suffer risk/ challenge	Work Tasks	Record types	Issues	Storage location	Shared usage	Solutions proposed by departments
1. Compliance	✓	✓	✓	✓	✓		
2. Legality and auditability	✓	✓	✓	✓	✓		
3. Security	✓	✓	✓	✓	✓	✓	
4. Everywhere accessible data	✓				✓		
5. Incident response, notification and remediation	✓	✓	✓	✓	✓	✓	
6. Virtualisation							
7. Governance and enterprise risk management	✓			✓			
8. Interoperability, portability and data lock-in	✓	✓	✓	✓	✓	✓	
9. Viability	✓	✓	✓	✓	✓	✓	
10. Availability and reliability	✓	✓	✓	✓	✓		

There are also risks of records management in the cloud, which were identified in **Chapter 6**. These risks were:

- Identification of risks involved with using cloud computing service providers
- Assessing risks for different records

- Preform due diligence when selecting a service provider
- Contractual arrangement to manage risks
- Monitor arrangements with service providers

These risks are also compared against the risks and challenges associated with cloud computing in **Table 8.12** to determine any overlap with the same risks and challenges.

**Table 8.12 Risks of records management in the cloud vs. risks and challenges associated with cloud computing**

Ten Risks & challenges associated with Cloud Computing	Risks of records management in the cloud				
	Identification of risks involved with using cloud computing service providers	Assessing risks for different records	Preform due diligence when selecting a service provider	Contractual arrangement to manage risks	Monitor arrangements with service providers
1. Compliance	✓			✓	
2. Legality and auditability	✓	✓			
3. Security				✓	✓
4. Everywhere accessible data					
5. Incident response, notification and remediation			✓		✓
6. Virtualisation					
7. Governance and enterprise risk management				✓	
8. Interoperability, portability and data lock-in	✓			✓	✓
9. Viability					
10. Availability and reliability			✓		

These risks and challenges are explained with regard to Company X:

- **Compliance:** Company X requires its project data to be kept for legal compliance issues. This retention would need to be discussed with the cloud service provider.
- **Legality and auditability:** As stated in **Table 8.8**, Company X requires project data to be kept for legal compliance. The loss of such data could lead to legal consequences. With regard to the Human Resources and Finance department, these departments were not analysed due to company stipulations. However, if they were to move to a cloud-based server, there may be additional legal issues affecting viability, such as hosting location issues (see **Chapter 4 Section 4.3.2.1**).
- **Security:** Company X would require its data to be secure to prevent any malicious activity, or data tampering.
- **Everywhere accessible data:** This is a factor for Company X, as the institution does utilise mobile devices, such as cellular phones and laptops, to access documents and files for work with clients.
- **Incident Response, Notification and Remediation:** Company X requires its documents to be available at all times. If the server is unavailable, then work will be affected. This was a factor which has resulted in departments keeping local copies of files, which has led to duplication and lack of space on the server.
- **Virtualisation:** This is not a risk for Company X as the cloud services would be used for document storage and not for running specific cloud based software.
- **Governance and enterprise risk management:** This is a risk for Company X where due to legal reasons project data must be retained. A loss of governance with the cloud service provider may impact on this and impact on legal compliance (see **Chapter 4 Section 4.3.7**).
- **Interoperability, portability and data lock-in:** This is a risk for Company X. They cannot afford to lose access to their project data, stored documents and records if they migrate to a different cloud service provider.

- **Viability:** This may be a risk factor for Company X, due to its large storage requirements and the risk of hidden variable costs, which could impact on cloud computing *Cost Efficiency*.
- **Availability and reliability:** This is a risk for Company X. Consideration must be made for the environment in which the Company operates, which requires access to their records in remote locations. Lack of access to these records may hinder work.

There are nine out of ten of the risks and challenges associated with cloud computing which could affect Company X (see **Table 8.11**). However, certain risks and challenges may be of a higher concern for Company X. Deciding which risks would be of greater concern would be Company X's decision.

### **8.2.3 Cloud computing and innovation**

In **Chapter 5**, the cloud business enablers driving innovation were identified. These findings are compared against the ten potential benefits of cloud computing identified in **Chapter 3**, in order to determine cloud computing's ability to promote innovation. **Table 8.13** shows where these benefits overlap.

**Table 8.13: Cloud business enablers driving innovation vs. ten potential benefits of cloud computing**

Cloud Business Enablers (Berman <i>et al.</i> 2012:3)	Cost efficiency	Scalability and Flexibility	Modernization of business processes	Availability and reliability	Rapid developments and deployments	Business continuity and disaster recovery	Greater mobility	Improved power, automation and support management	Improved security	Green IT/ Green computing
1. Cost flexibility	✓									
2. Business scalability		✓								
3. Market adaptability			✓							
4. Masked complexity	✓									
5. Content driven variability			✓							
6. Ecosystem connectivity					✓					

These enablers are explained as:

- *Cost flexibility* such as cost savings and cloud computing’s pay-per-use structure (see **Chapter 3 Section 3.3.1**) overlaps with *Cost efficiency*. This allows for more capital to be used in operations as opposed to traditional IT costs.
- *Business scalability* such as easy resource scalability (see **Chapter 3 Section 3.3.2**) overlaps with *Scalability and flexibility*. This enabler allows organisations to expand their resource requirements rapidly.
- *Market adaptability* such as the ability to adjust rapidly, based on customer needs, (see **Chapter 3 Section 3.3.3**) overlaps with *Modernisation of business processes*. This creates a competitive advantage allowing organisations to adjust to changing markets.
- *Masked complexity*: Hiding complexities from customers such as not needing to involve them in upgrade details and requirements (see **Chapter**



**3 Section 3.3.1)** overlaps with *Cost efficiency*. As an enabler, this allows the customer to be free from being involved with any changes that may occur within the organisations.

- *Content-driven variability*: The ability to provide custom customer tailored products and services, enabling the targeting of more markets (see **Chapter 3 Section 3.3.3**), overlaps with *Modernisation of business processes*.
- *Ecosystem connectivity*: Promoting collaboration between users, which improved productivity and helps drive innovation (see **Chapter 3 Section 3.3.5**), overlaps with *Rapid development and deployment* (Berman *et al.* 2012:31; Lala 2012:10).

Based on these findings, the conclusion is drawn that cloud computing can support innovation within Company X through the potential benefits it provides if it is successfully adopted.

### **8.3 Summary**

The potential benefits, risks and challenges associated with cloud computing were matched against the case study findings analysis. From this comparison, it was found that there were equal potential benefits, risks and challenges determining the viability of utilising cloud computing for records management.

Although there are potential benefits equal to risks and challenges, this company must consider whether these potential benefits outweigh the risks (Stuart & Bromage 2010:223). However, it can be noted that within Company X, the Business Development Department was utilising a cloud-based service (Dropbox) for the temporary sharing of large documents and multimedia with another international office, not for the long-term storage of documents. Company X needs to be aware of the issues associated with this, with regard to the example given in **Chapter 4, section 4.3.3.1a**. The example showed the authentication issue, which compromised over 25 million Dropbox accounts, allowing access to any account without the correct password.

Based on the results found, the *potential benefits of cloud computing* would solve a majority of the issues identified at Company X (see **Table 8.9**). These would make cloud computing a viable option for records management. However, there are risks and challenges that would still need to be addressed. These must be discussed with the cloud service provider selected by Company X. These risks and challenges relate to:

- Legality and auditability
- Incident response, notification and remediation
- Interoperability, portability and data lock-in
- Availability and reliability.

Based on the findings presented in this chapter, cloud computing is a viable option for Company X. This recommendation is based on the potential benefits of cloud computing, as long as the selected cloud service provider deals with the identified risks.

The potential benefits of cloud computing were also compared against the reported literature in **Chapter 5**, the cloud business enablers driving innovation. All the enablers were found to overlap with potential benefits identified in **Chapter 3**. This indicates that cloud computing can promote innovation within Company X, if it is successfully adopted and gains the potential benefits of cloud computing.

In **Chapter 9** the final conclusions and summary of findings for the research questions are given as well as a recommendation for cloud computing's viability for other companies, similar to Company X.

## Chapter 9 Final conclusions and recommendations for further research

### 9.1 Introduction

In this dissertation, the research was concerned with answering the research problem statement:

*With the increase in growth of cloud computing, organisations must be aware of the potential benefits and challenges of adopting the technology of cloud computing. Organisations must be able to access its viability as an alternative for traditional management of records. Further questions arise on how cloud computing can be used to foster innovation within an organisation.*

This was done by answering the research questions. Those questions were:

- What are the potential benefits of cloud computing?
- What are the challenges and risks associated with cloud computing?
- To what extent is cloud computing a viable option for records management?
- How can cloud computing be used to foster innovation within an organisation?

Each of these questions have been addressed where the final findings and conclusions are summarised in **Sections 9.2 to 9.5**.

The following definition of cloud computing was created in **Chapter 2**, in order to better understand cloud computing:

*Cloud computing is a multi-tenancy system of (hard and soft) virtualised resources with utility properties. These rapid, on-the-go adjustable, pooled resources are used as an alternative to onsite storage and applications and provide virtual computing services, wherever an Internet connection is present (adapted from Armbrust, Fox, Griffith, Joseph and Katz 2009:3, Buyya, Yeo, Venugopal, Broberg, & Brandic 2009:5, Mell & Grance 2011:2; Vaquero Rodero-Merino, Caceres, and Lindner 2009:1).*

In the context of this research, all recommendations and findings are done in

relation to the case study and apply to Company X and similar organisations. Similar organisations refer to Australian private companies in the mining and software development sector.

## 9.2 Potential benefits of cloud computing

The first research question focused on cloud computing's positive aspects.

- What are the potential benefits of cloud computing?

This question was answered through a literature analysis to create the *Ten potential benefits of cloud computing*. These potential benefits are:

### 1. Cost efficiency

*Cost efficiency* is one of the most promising potential benefits of cloud computing. Convery (2010:63,65) provided the practical examples from Melrose Resources plc. and Guardian News & Media (GNM) that provided evidence indicating the cost saving capabilities of cloud computing in relation to software, hardware and training (see **Chapter 3, Section 3.3.1**).

With regard to records management, cloud computing's pay-per-use system allows users to upgrade their storage based on their needs, as and when more space is required.

### 2. Scalability and flexibility:

*Scalability and flexibility* feeds into cost efficiency. This allows users to forgo forecasting their resource needs and adjust resources only when it is required. The on-demand flexibility allows cost savings. However, the resources must be monitored to ensure that the costs do not reach exorbitant levels and that the cloud service provider can meet the users' needs (see **Chapter 3, Section 3.3.2**). Monitoring resources is essential for organisations that wish to utilise the cloud for records management, as more resources are required over time, causing costs to rise. This in turn can affect the cloud's perceived viability in the long term.

### **3. Modernisation of business processes:**

*Modernisation of business processes* allows for integrated cloud services to address individual organisational needs. This new customisable cloud service can impact on efficiency and productivity (see **Chapter 3, Section 3.3.3**).

### **4. Availability and reliability:**

*Availability and reliability* is an excellent potential benefit, as it provides cloud users availability of cloud services, 99.9% of the time. If outages occur, then users are automatically redirected to alternative servers, allowing for work to continue (see **Chapter 3, Section 3.3.4**). When outages do occur, the client does not control the restart of the services. Therefore, users must consider whether the cloud service providers are able to supply services during outages. Often if the cloud service provider cannot meet the stipulations of the Service Level Agreements (SLA's), then the customer may only be compensated in free service time (Convery 2010:11). These outages can draw into question the viability of cloud computing especially for data storage and records management.

### **5. Rapid developments and deployments:**

*Rapid development and deployment* for cloud computing allows for savings in time as well as effective resource provisioning. Due to the fact that there is no long-term commitment to the service, the client can cancel services that do not meet their unique needs and try an alternative service provider. Furthermore, because these services are pretested and configured they are instantly available to the client (see **Chapter 3, Section 3.3.5**).

### **6. Business continuity and disaster recovery:**

*Business continuity and disaster recovery* is achieved through the automatic replication of data to a decentralised storage system on multiple servers in various locations. This provides clients with business continuity as well as the prevention of the loss of data when and if disasters occur (see **Chapter 3, Section 3.3.6**). These are positive examples of the viability of cloud services for data storage and records management.

### **7. Greater mobility:**

*Greater mobility* is an excellent benefit of cloud computing for records management, as it allows workers that may travel and operate in various locations, such as on dispersed mine sites, to continue working and access their data through various devices over the internet (see **Chapter 3, Section 3.3.7**). This can help reduce copies of records.

### **8. Improved power, automation and support management:**

*Improved power, automation and support management* identify cloud computing's potential to handle larger workloads through its increased power and calculation ability provided by its near limitless resources and processing power. Furthermore, its improved level of automation helps reduce maintenance and speed up resource procurement (see **Chapter 3, Section 3.3.8**).

### **9. Improved security:**

As cloud computing service providers have the capacity to attribute greater resources, they are able to provide greater security for their clients. Security is of great concern for records management. Cloud computing's ability to provide greater levels of security is one of its most enticing benefits (see **Chapter 3, Section 3.3.9**).

### **10. Green IT/ green computing:**

With more and more organisations "Going Green", there is a greater focus on enterprises to lower their carbon footprint. Cloud computing is able to provide this benefit by saving on space and energy consumption, through the use of shared hardware infrastructure between multiple clients (see **Chapter 3, Section 3.3.10**).

The *ten potential benefits of cloud computing* were compared against the results of the case study findings (**Chapter 8 Section 8.2.2**), in order to help determine if cloud computing would solve issues experienced by Company X.

The findings indicated that Company X would benefit, as cloud computing will solve the majority of their issues. Eight out of the ten potential benefits for cloud computing are applicable to Company X. These are:

- **Cost efficiency** – All of Company X's tasks and elements such as storage location, document creation, sharing of documents etc. would all be addressed through cloud computing and a lower cost of hosting records would draw upon this benefit.
- **Scalability and flexibility** – Company X must expand its storage requirements as required due to increasing growth of business. All project data must be retained for compliance issues, drawing upon this potential benefit.
- **Modernisation of business processes** – The Business Development Department was already in the process of acquiring customer relationship management services (Salesforce 2013) for its specific needs.
- **Availability and reliability** – Certain departments within Company X require a constant Internet connection and server access, in order to access records. Cloud computing would be able to provide this benefit at all times when work may be required.
- **Rapid developments and deployments** – Company X would not utilise this benefit as they have not indicated any pretested or specific software that they may require.
- **Business continuity and disaster recovery** – A department in Company X had a hard drive failure, which led to data being lost. Cloud computing could have prevented this due to its backups and continuity capabilities.
- **Greater mobility** – Company X deals with the mining environment and as such has customers in remote locations, where the ability to continue work and have access to their records from various locations is important. This benefit would be important to Company X.

- **Improved power, automation and support management** – This was not indicated as a requirement for Company X.
- **Improved security** – This is always a benefit to organisations as records must be secure to prevent any malicious activity and loss of information. Company X would gain this benefit.
- **Green IT/ green computing** – Company X would no longer need to print documents, when traveling to areas with low connectivity, due to cloud computing’s capabilities. This would be an indirect benefit for Company X in reducing their carbon footprint.

The analysis of the literature provided sufficient evidence in answering this research question. With regard to Company X and similar software development companies in the mining industry, these potential benefits of cloud computing provide a positive view on cloud computing’s viability for their records management needs. From a potential benefit perspective, cloud computing is a viable option for records management for Company X.

For similar software development companies in the mining industry, these potential benefits must be considered by those individual organisations as each benefit may have higher value than another. For example, *Cost Efficiency* may outweigh the *Scalability and Flexibility* as a benefit. The need to expand resources when needed may not be as important as reducing costs.

### **9.3 Challenges and risks associated with cloud computing**

The second research question focused on cloud computing’s negative aspects and was formulated thus:

- What are the challenges and risks associated with cloud computing?

This question was answered through a literature analysis to identify the ten most common risks and challenges associated with cloud computing. The ten risks and challenges were identified as:



### **1. Compliance:**

*Compliance* is a big challenge for cloud computing, as organisations may wish to avoid doing business with an organisation that does not comply with international standards and legal requirements. It remains for each organisation to investigate what standards affect them and whether they do comply with these standards when utilising cloud computing (see **Chapter 4, Section 4.3.1**).

### **2. Legality and auditability:**

*Legality and auditability* is one of the largest challenges for cloud computing. An organisation must legally comply with acts and regulations, which are in effect in their home country. With cloud computing this can present a problem because data can now be hosted in another country and in various geographical locations where their relevant jurisdictions need to be known and adhered to. This creates further legal implications that must be considered. Another implication of cloud computing is its multi-tenant system, where if a drive is seized for legal matters, it may prevent other organisations from accessing their data stored on the same drive (see **Chapter 4, Section 4.3.2**). This can impede daily business as records may no longer be accessible, drawing into question cloud computing's viability.

### **3. Security**

*Security* is most likely the largest risk for cloud computing. A cloud service provider must ensure that a client's stored data is secure. It must be noted that it remains the client's responsibility to ensure that the service provider is able to provide this security. For legal reasons, the stored data must remain authentic, secure, confidential and reliable.

Challenges, such as surface attacks (viruses, DDOS attacks and Trojans etc.) are not new to IT and data security, but due to cloud computing data being stored on multi-tenant systems there is a greater risk from concentrated attacks value (see **Chapter 4, Section 4.3.3**). With regard to records management, *Security* draws cloud computing's viability into question, as the cloud data centres are more likely to be targeted.

#### **4. Everywhere accessible data**

*Everywhere accessible data* is a great risk for organisations utilising cloud computing. Organisations should incorporate its use ahead of the expansion of mobile device capacities and usage, rather than being forced into it. Through adopting the usage of mobile devices, security protocols can be developed in advance to deal with incidents, rather than being caught off guard (see **Chapter 4, Section 4.3.4**). The issue of cloud computing's viability for records management is drawn into question in a recent survey, conducted by the company Harmon.ie (2013). The survey conducted on mobile business users, found that 41% of mobile users admitted that they ignored company policies and stored and shared corporate documents on unapproved cloud services.

#### **5. Incident response, notification and remediation**

There are risks for cloud computing in how an incident (event) is dealt with, the speed at which it is handled, as well as what the damage may be if it is handled incorrectly. For example, if a server crashes, the client must be contacted and informed that an alternate server will be made available to ensure that their data can still be accessed. Delays in notification or incident response could cause a delay in work for the client, or even lead to data loss (see **Chapter 4, Section 4.3.5**). In order to determine cloud computing's viability, organisations must be fully aware of how their cloud service providers respond to incidents.

#### **6. Virtualisation:**

*Virtualisation* presents a particular risk for records management, as hypervisor security and cross VM exploitation can allow stored information on other VMs to be accessed. Unfortunately, this is not virtualisation's largest risk but rather security and privacy within a VM is. The hypervisor is used to create isolation between the VMs on the server. Unfortunately, if the hypervisor is no longer secure then all VMs are at risk (Bouayad *et al.* 2012: 29; Himmel 2012:21,26) (see **Chapter 4, Section 4.3.6**).

## 7. Governance and enterprise risk management

*Governance and enterprise risk management* is linked to *Legality and auditability*. A loss of governance can compromise an organisation's ability to comply with regulatory and legislative procedures. The organisation's capacity to show integrity, reliability and authenticity of information that they are storing in the cloud must be demonstrated (see **Chapter 4, Section 4.3.7**).

## 8. Interoperability, portability and data lock-in

*Interoperability* is concerned with all the components of cloud computing having the ability to exchange with different, as well as new components from alternate providers while still maintaining its ability to function. *Portability* is the ability of the applications' components to be moved and recycled in another location. However, in the absence of interoperability, portability may lead to data lock-in with a cloud service provider. *Data lock-in* occurs when the cloud service provider has an interest in retaining customers by being locked into their products. Data must be returned to a client in a usable format, if the client no longer wishes to do business with that service provider (see **Chapter 4, Section 4.3.8**). If data is locked into a vendor, then cloud computing is not viable for records management.

## 9. Viability

*Viability* has a few sub-risks, which are identified as:

**Hidden variable costs:** unknown costs

**Bugs in distributed systems:** the elimination on large-scale distributed systems.

**Shared reputation and accountability:** multi-tenant issues share blame among shared IP addresses on the same system.

Additional factors, which can affect the viability of cloud computing for records management, are determining what the rights and responsibilities are of the cloud service provider and what they are for the client. These rights and responsibilities must be discussed with a cloud service provider before implementation (see **Chapter 4, Section 4.3.9**).

## **10. Availability and reliability:**

*Availability and reliability* of service is a core benefit of cloud computing. However, it has its own risks. For example, service level commitments which are required for critical business processes, are often not included in the actual service given by the cloud service provider.

Another issue for reliability is with regard to a cloud service provider ceasing operations and going out of business. There is no regulated process for returning the information to its clients and contingency planning is required for these instances (Convery 2010:14).

Once the *risks and challenges associated with cloud computing* were identified it was compared against the results of the case study findings (**Chapter 8 Section 8.2.2**). The findings indicated to what risks Company X would be affected with regard to their issues.

It was discovered that nine out of ten risks and challenges would affect Company X. They are explained as follows:

- **Compliance:** Company X requires its project data to be kept for legal compliance issues.
- **Legality and auditability:** As stated above Company X requires project data to be kept for legal compliance. The loss of such data could lead to legal consequences. Company X must be held accountable if inspected.
- **Security:** Company X would require its data to be secure to prevent any malicious activity or data tampering.
- **Everywhere accessible data:** This is a factor for Company X, as the institution does utilise mobile devices such as cellular phones and laptops for work with clients to access documents and files.

- **Incident response, notification and remediation:** Company X requires its documents to be available at all times. If the server is inaccessible, the ability to work will be affected.
- **Virtualisation:** This is not a risk for Company X as the cloud services would be used for document storage and not for running specific cloud based software.
- **Governance and enterprise risk management:** This is a risk for Company X where due to legal reasons project data must be retained. A loss of control over data may impact legal compliance.
- **Interoperability, portability and data lock-in:** This is a risk for Company X. They cannot afford to lose access to their project data, stored documents and records if they migrate to a different cloud service provider.
- **Viability:** This may be a risk factor for Company X, as it has large storage requirements and there is a risk of hidden variable costs which could impact on cloud computing *Cost efficiency*.
- **Availability and reliability:** This is a risk for Company X. Consideration must be made for the environment in which Company X operates, which requires access to their records in remote locations. Lack of access to records may hinder work.

Cloud computing has many risks and challenges. However, if careful attention is paid to these, then their risk factor can be minimised. It must be noted that the mining industry may be impacted in specific ways. These include:

- The theft of sensitive information (e.g. geological block models, which shows minable ore information and all geological features)
- A halt to production caused by inaccessibility of records, necessary for compliance, with industry specific procedures

- Risks of legality, auditability and compliance, where geographically specific standards and laws of the mining industry must be considered

The analysis of the literature provided sufficient evidence in answering this research question. With regard to Company X, and similar organisations, these risks and challenges do provide a negative view on cloud computing's viability for their records management needs. From a negative perspective, cloud computing appears fraught with risk and challenges, which could affect Company X's ability to work. However, if these risks are discussed with a cloud service provider before implementation, they may be mitigated. If these risks and challenges can be mitigated with cloud computing, Company X and similar organisations in the mining industry can viably use cloud computing for records management.

As for other organisations, the viability would depend on the level of concern which each individual organisation places on each individual risk. *Compliance* could be regarded as more of a concern than the possibility of server down time due to *Availability and reliability*.

#### **9.4 Viability of cloud computing for records management**

The third research question focused on cloud computing's viability aspect and was formulated as:

- To what extent is cloud computing a viable option for records management?

This question was answered through **Chapters 3 to 8**, which dealt with the analysis of literature and case study's findings.

In **Chapter 6**, it was determined by the researcher that there are risks and benefits associated with utilising cloud computing for records management. These were compared against the potential benefits as well as the risks and challenges associated with cloud computing from **Chapters 3 and 4** in order to determine cloud computing's viability for records management. This comparison was done in **Chapter 8**.

The benefits of the cloud for records management were identified and discussed in

**Chapter 6:**

- Reduced costs
- Less pressure on ICT to provide increased storage capacity
- Service access in various locations
- Collaborative opportunities with various geographically located individuals
- Potential for improved automation such as record keeping as part of business processes
- Increased time for more work due to reduced server maintenance time required

These were cross-referenced with the *potential benefits of cloud computing* and were found to all correspond with the potential benefits of cloud computing, identified in the literature analysis. With regard to Company X, this indicates the viability for cloud computing and records management. Reinforcing the previous findings from the case study findings analysis, it indicated that Company X would gain eight out of the ten potential benefits of cloud computing.

Cross-referencing was done also for the risks of records management (**Chapter 6**). The results that were identified in the literature analysis correspond with the risks and challenges associated with cloud computing. These were:

- Identification of risks involved with using cloud computing service providers
- Assessing risks for different records
- Perform due diligence when selecting a service provider
- Contractual arrangement to manage risks
- Monitor arrangements with service providers

The literature analysis in **Chapter 6** also found there are laws which must be addressed which impact on cloud computing's viability. Australian organisations, which want to store records in the cloud, are subject to laws such as the *Electronic Transactions Act 1999* (Australia 2011:14-15) so that when selecting a cloud service provider, the organisation needs to be sure that the provider is compliant

with this act. Organisations should also comply with international standards, being AS ISO 15489; AS 5044; ISO 16175.

The analysis in **Chapter 8** found that a large number of issues experienced by Company X could be solved by the potential benefits of adopting cloud computing. Unfortunately, there are still a large number of risks and challenges for cloud computing. These could be dealt with if they are discussed with a cloud service provider before its adoption. Company X must discuss the rights and responsibilities of the user and the cloud service provider beforehand. A service level agreement must be drawn up to address the risks and challenges that have been identified. If this is done, then cloud computing does appear to be a viable option for records management for a mining software development company such as Company X.

For other organisations in the mining industry in Australia, these laws identified must be examined to determine if they impact the organisation. The type of information an organisation stores can affect cloud computing's viability for records management, for example, the *Electronic Transactions Act 1999*, which deals with electronic transactions (Australian Government. n.d) and stipulations with regard to stored electronic information. This act can affect companies depending on what type of information they are storing in the cloud.

The benefits, risks and challenges of records management (**Chapter 6**) correspond with the potential benefits (**Chapter 3**) as well as the risks and challenges associated with cloud computing (**Chapter 4**). This indicates that cloud computing is still a viable option for records management for other organisations in the mining industry. Risks however, need to be discussed beforehand with the cloud service provider. Whether or not an organisation is willing to accept those risks, depends on what that organisation would consider as viable risks for themselves.

## **9.5 Cloud computing and innovation**

The fourth research question focused on cloud computing and innovation and was:



- How can cloud computing be used to foster innovation within an organisation?

This question was answered through a literature analysis of features that drive innovation within an organisation in **Chapter 5** and compared against the potential benefits of cloud computing in **Chapter 8**.

This was achieved by the analysis of the Cloud Enablement Framework, which discussed what business enablers help drive innovation within an industry. The framework has the ability to provide new, more productive, reactive and innovative methods of conducting business. As organisations are now beginning to realise the cloud's power to create new business models, as well as to promote sustainable competitive advantages, they will begin to utilise cloud capabilities to drive business success and value, whether they are optimisers, innovators or disruptors (Berman *et al.* 2012:34).

These enablers have been explained in relation to their overlapping benefits identified in **Chapter 3**, with regard to promoting innovation within Company X, these being:

- **Cost flexibility**
- **Business scalability**
- **Market adaptability**
- **Masked complexity**
- **Content-driven variability**
- **Eco-system connectivity**

An alternative perspective was also analysed, which was provided by a discussion of a research paper by Willcocks *et al.* (2013: 184) (see **Chapter 5, Section 5.3.3**). Willcocks *et al.* (2013) identified the factors driving and preventing cloud computing's adoption in relation to its innovative practices. The scholars further concluded that cloud computing as an innovation provides organisational units with the ability to alter their pre-existing business services, through the collaboration and innovation beyond the enterprise. The unique features of cloud

computing provide business innovation opportunities which can adjust the risk profile of these business innovations. This allows for new business processes and their service levels to be tested and expanded, or disbanded, if they are unsuccessful. Based on these findings, the conclusion was drawn that cloud computing can support innovation within Company X if successfully adopted.

Cloud computing has features and challenges which require attention to encourage its adoption for innovative purposes (Willcocks *et al.* 2013:184). For other organisations, the findings agree that if cloud computing is successfully adopted and gains the potential benefits, then it should promote innovation within that organisation.

## **9.6 Suggestions for further research**

This research was conducted on the analysis of a single case study's results and pertains to a specific field, the mining software development field. Although the potential benefits, risks and challenges associated with cloud computing are generalised, they are tailored towards questioning the viability of cloud computing for records management for the Company X, and similar organisations.

Additional research would be needed to create a more specific answer on the viability of cloud computing to other organisations. Such topics include:

- Laws pertaining to other geographically hosted data
- In-depth investigation into the hosting of stored data relating to personal information and electronic transactions
- In-depth investigation into ISO standards for compliance pertaining to the specific organisation
- Mitigation of risks and challenges of cloud computing
- Successful adoption of cloud computing

## **9.7 Recommendations on the use of cloud computing for records management**

With regard to Company X, cloud computing is a viable option for records management. Cloud computing will solve a majority of issues that Company X has

experienced. However, it must be considered that these are potential benefits and may only be offered under certain conditions by all cloud service providers.

The potential benefits as well as all the risks and challenges need to be discussed with cloud service providers before committing to their services. Not addressing these risks and challenges will affect the effectiveness and viability of cloud computing for Company X for their records management. Company X must be aware of where their data will be hosted (geographically) for legal purposes. They should also be aware of the rights and responsibilities for both them and the cloud service provider. A service level agreement must be drawn up before cloud adoption to ensure clarity on these issues. Furthermore, a cloud service provider that adhered to international standards such as ISO 15489 is recommended as this standard outlines best practices for records management. Another consideration is the hosting of personal information for other organisations in the mining industry. These same risks and challenges would need to be discussed with the cloud service provider before committing to their services.

## **9.8 Value of study in closing**

This study successfully answers the research problem through the identification of potential benefits, risks and challenges associated with cloud computing, the viability of cloud computing for records management as well as how cloud computing could be used to promote innovation within organisations.

Although there are negative aspects regarding the risks and challenges associated with cloud computing, these could be mitigated through communication with the cloud service provider. With adequate communication, the potential benefits provided by cloud computing may lead it to be considered as a viable option for records management within the mining software development sector in Australia.

## References

- Adam, A. 2007. *Implementing Electronic Document and Record Management Systems*. Boca Raton: Auerbach Publications.
- Aleem, A. & Sprott, CR. 2013. Let me in the cloud: analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime* 20(1):6-24. Available at: <<http://dx.doi.org/10.1108/13590791311287337>> [Accessed 02 April 2013].
- Almadallah, M. 2014, *Cloud Computing: Challenges and Risk Management Framework*, North Carolina Agricultural and Technical State University.
- Amazon. 2012. Amazon Elastic Compute Cloud (Amazon EC2). [Online] Available at: <<http://aws.amazon.com/ec2/>> [Accessed 18 November 2012].
- Armbrust, M. Fox, A. Griffith, R. Joseph, AD. & Katz, R. 2009. Above the Clouds: A Berkeley View of Cloud Computing. *UC Berkeley Reliable Adaptive Distributed Systems Laboratory White Paper*, [Online]. Available at: <<http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf>> [Accessed 25 September 2012].
- Armistead, CG. Bowman, C. & Newton, J. 1994. Managers' perceptions of the importance of supply, overhead and operating costs. *International Journal of Operations & Production Management* 15(3):16-28. Available at: <<http://0-dx.doi.org.oasis.unisa.ac.za/10.1108/01443579510080526>> [Accessed on 13 August 2013].
- Asghary Karahroudy, A. 2011. *Security Analysis and Framework of Cloud Computing with Parity-Based Partially Distributed File System*, East Carolina University.
- Askhoj, J., Sugimoto, S. & Nagamori, M., 2011. Preserving records in the cloud. *Records Management Journal*, 21(3), pp.175–187. Available at: <http://www.emeraldinsight.com/10.1108/09565691111186858> [Accessed October 18, 2013].
- Australia. 2011. Electronic Transaction Act 1999. (Act No.162 of 1999). Available at: <<https://www.comlaw.gov.au/Details/C2011C00445>> [Accessed 14 October 2015].

- Australia. 2014. Privacy Act 1988. (Act No.119 of 1998). Available at: <<https://www.comlaw.gov.au/Details/C2015C00451/fe8d4b53-f971-417d-ac45-c27e6ccda569>> [Accessed 14 October 2015].
- Australasian Digital Recordkeeping Initiative. 2010. Advice on managing the recordkeeping risks associated with cloud computing. [Online] Available at: <[http://www.adri.govt.nz/products/ADRI\\_statement\\_re\\_cloud\\_computing\\_v1-0\\_July\\_2010.doc](http://www.adri.govt.nz/products/ADRI_statement_re_cloud_computing_v1-0_July_2010.doc)> [Accessed on 12 June 2013].
- Australian Government. n.d. E-commerce. [Online] Available at: <<http://www.ag.gov.au/RightsAndProtections/ECommerce/Pages/default.aspx>> [accessed 19 October 2014].
- Australian Taxation Office. 2012. Record keeping for small businesses. [Online] Available at: <<https://www.ato.gov.au/General/Other-languages/In-detail/Information-in-other-languages/Record-keeping-for-small-businesses/>> [Accessed 21 October 2015].
- Avanade, 2013. Is enterprise social collaboration living up to its promise? [Online] Available at: <<http://www.avanade.com/~media/documents/resources/social-collaboration-global-study.pdf>> [Accessed 09 November 2013].
- Babbie, E. 2008. *The Basics of Social Research*. 4th Edition. Belmont: Thompson Wadsworth.
- Baroudi, C. 2009. *Green IT For Dummies®*, IBM Limited Edition. Indianapolis: Wiley Publishing.
- BBC. 2013. China hit by 'biggest ever' cyber-attack. *BBC News*, [online] 27 August. Available at: <<http://www.bbc.co.uk/news/technology-23851041>> [Accessed 18 October 2013].
- Berman, S.J., Kesterson-Townes, L., Marshall, A. & Srivathsa, R. 2012. How cloud computing enables process and business model innovation. *Strategy & Leadership* 40(4):27-35. Available at: <<http://www.emeraldinsight.com/journals.htm?articleid=17041621&show=abstract>> [Accessed 18 August 2012].
- Bhattacharjee, A. 2012. Social science research: principles, methods, and practices. 2nd ed. Available at:

- [http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa\\_textbooks](http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks) [Accessed 12 August 2013].
- Biggs, S. & Vidalis, S. 2009. 'Cloud Computing: The Impact on Digital Forensic Investigations' in IEEE (Institute of Electrical and Electronics Engineers). *International Conference for Internet Technology and Secured Transactions (ICITST)*. London, England. 9-12 Nov. 2009. New York: Curran Associates.
- Brodkin, J. 2008. Loss of customer data spurs closure of online storage service 'The Linkup'. *Network World*, [online] 11 August 2008. Available at: <<http://www.networkworld.com/news/2008/081108-linkup-failure.html>> [Accessed 2 November 2013].
- Bouayad, A. Blilat, A. El Houda Mejhed, N. & El Ghazi, M. 2012. 'Cloud computing: Security challenges' in IEEE (Institute of Electrical and Electronics Engineers) 2012 *Colloquium in Information Science and Technology (CIST)*, Fez, Morocco, 22-24 October. New York: Curran Associates.
- Buckley, C. 2013. The cloud: Mitigating risks as you relinquish control. *TechRepublic* [online] 26 September. Available at: <<http://www.techrepublic.com/blog/tech-decision-maker/the-cloud-mitigating-risks-as-you-relinquish-control/>> [Accessed 09 November 2013].
- Buyya, R., Yeo, CS., Venugopal, S., Broberg, J. & Brandic, I. 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems* (25):599-616. Available at: <<http://dx.doi.org/10.1016/j.future.2008.12.001>> [Accessed on 24 September 2012].
- Cambridge Business English Dictionary Online. 2014. Cambridge University Press, UK. Available at: <<http://dictionary.cambridge.org>> [Accessed 5 March 2014].
- Carroll, M., Van der Merwe, A. & Kotzé, P. 2011. 'Secure Cloud Computing Benefits, Risks and Controls' in IEEE (Institute of Electrical and Electronics Engineers) *Information Security For South Africa*, Johannesburg, South Africa 15-17 August. New York: Curran Associates.

- Cervone, HF. 2010. An overview of virtual and cloud computing. *OCLC Systems & Services* 26(3):162-165. Available at: <<http://dx.doi.org/10.1108/10650751011073607>> [Accessed 23 March 2012].
- Chan, T. 2009. Full interview: At&t's Joe Weinman. Green Telecom Live [Online]. Available at: <<http://www.greentelecomlive.com/2009/03/16/full-interview-att%E2%80%99s-joe-weinman/>> [Accessed 02 October 2012].
- Chaput, SR. & Ringwood, K. 2010. Cloud Compliance: A Framework for Using Cloud Computing in a Regulated World, in *Cloud Computing Principles, Systems and Applications*, edited by N Antonopoulos & L Gillam. London: Springer. Ch.14.
- Cloud Security Alliance. 2011. Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0. [Online] Available at <<https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>> [Accessed 22 April 2013].
- Cloud Security Alliance, 2013. About. [Online] Available at: <<https://cloudsecurityalliance.org/about/>> [Accessed 13 August 2013].
- Connaway, LS. & Powell, RR. 2010. *Basic research methods for librarians*. 5<sup>th</sup> edition. Santa Barbara: Libraries Unlimited.
- Convery, N. 2010. Guidance for outsourcing information storage to the cloud. [Online]. Available at: <[http://www.archives.org.uk/images/documents/Cloud\\_Computing\\_Toolkit-2.pdf](http://www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf)> [Accessed on 28 December 2012].
- Corbin, J. & Strauss, A. 2008. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 3<sup>rd</sup> Edition. Thousand Oaks: Sage.
- Corsello, J. 2012. Maximizing talent management through the cloud: New technologies offer opportunities to develop skills and careers. *Human Resource Management International Digest* 20(4):27-30. Available at: <<http://dx.doi.org/10.1108/09670731211233339>> [Accessed 18 August 2012].
- Creswell, JW. 2002. *Research design: qualitative and quantitative approaches*. Second Edition Thousand Oaks: Sage Publications.
- CSA. 2011. Cloud Security Alliance Announces Key Initiative in Development of

- Cloud Security Standards in Partnership with ISO/IEC. [Online] Available at: <<https://cloudsecurityalliance.org/csa-news/key-initiative-in-development-of-cloud-security-standards-in-partnership-with-isoiec/>> [Accessed 04 October 2012].
- Delic, K. & Riley J. 2010. Enterprise Knowledge Clouds: Applications and Solutions, in *Handbook of Cloud Computing*, edited by B. Furkht, & A. Escalente. New York: Springer.
- Deloitte Touche Tohmatsu. 2009. The Next Wave of Green IT, IT's role in the future of enterprise sustainability. [Online] Available at: <[http://www.deloitte.com/assets/dcom-unitedkingdom/local%20assets/documents/uk\\_c\\_green\\_it\\_emea.pdf](http://www.deloitte.com/assets/dcom-unitedkingdom/local%20assets/documents/uk_c_green_it_emea.pdf)> [accessed 13 August 2013].
- Dignan, L. 2008. Amazon explains its S3 outage. [Online] Available at: <<http://www.zdnet.com/blog/btl/amazon-explains-its-s3-outage/8010>> [Accessed 19 September 2013].
- Dhar, S. 2012. From outsourcing to Cloud computing: evolution of IT services. *Management Research Review* 35(8):664-675. Available at: <http://dx.doi.org/10.1108/01409171211247677> [Accessed 02 April 2013].
- Donoghue, A. 2009. Lightning zaps Amazon cloud. [Online.] Available at: <[http://news.cnet.com/8301-1001\\_3-10263425-92.html](http://news.cnet.com/8301-1001_3-10263425-92.html)> [Accessed 19 September 2013].
- Du Plooy, GM. 2009. *Communication Research: techniques, methods and applications*. Second Edition. Kenwyn: Juta.
- Ferdowsi, A. 2011. Yesterday's Authentication Bug. *The Dropbox Blog*, [Blog] June 20, Available at: <<https://blog.dropbox.com/2011/06/yesterdays-authentication-bug/>> [Accessed 8 February 2014].
- Foo, F. 2012. US Patriot Act fears over data storage unfounded: lawyer. *The Australian* [Online] Available at: <<http://www.theaustralian.com.au/australian-it/us-patriot-act-fears-over-data-storage-unfounded-lawyer/story-e6frgakx-1226336465455>> [Accessed 24 October 2012].
- Gagliardi, F. & Muscella, S. 2010. Cloud Computing – Data Confidentiality and Interoperability Challenges, in *Cloud Computing Principles, Systems and Applications*, edited by N Antonopoulos & L Gillam. London:



Springer.Ch.15.

Gartner, 2010. *Gartner Global IT Council for Cloud Services Outlines Rights and Responsibilities for Cloud Computing Services*. [press release] 12 July 2010, Available at: <<http://www.gartner.com/newsroom/id/1398913>>. [Accessed 05 January 2014].

Gartner, 2013. *Gartner Says At Least 60 Percent of Information Workers Will Interact With Content Applications via a Mobile Device by 2015*. [press release] 26 June 2013, Available at: <<http://www.gartner.com/newsroom/id/2529315>> [Accessed 09 November 2013].

Gellman, R. 2009. Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. [Online] Available at <[http://www.worldprivacyforum.org/pdf/WPF\\_Cloud\\_Privacy\\_Report.pdf](http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf)> [Accessed 09 May 2013].

Hancock, DR & Algozzine, B. 2006. *Doing Case Study Research: A Practical Guide For Beginning Researchers*. New York: Teachers College Press.

Harmon.ie. 2013. New Survey Reveals! Mobile 'Rogue IT' Costing US Organizations Almost \$2B. *Harmon.ie blog*, [blog] 12 September. Available at: <<http://harmon.ie/blog/new-survey-reveals-mobile-rogue-it-costing-us-organizations-almost-2b>> [Accessed 09 November 2013].

Harmon, RR., Demirkan, H. & Raffo, D. 2012. Roadmapping the next wave of sustainable IT. *Foresight* 14(2):121-138. Available at <<http://dx.doi.org/10.1108/14636681211222401>> [Accessed 18 August 2012].

Heiser, J. & Nicolett, M. 2008. *Assessing the Security Risks of Cloud Computing*. Gartner. [Online]. Available at: <<http://cloud.ctrls.in/files/assessing-the-security-risks.pdf>> [Accessed on 27 September 2012].

Hickey, AR. 2010. Cloud Computing Services Market To Near \$150 Billion In 2014. [Online] Available at: <<http://www.crn.com/news/managed-services/225700984/cloud-computing-services-market-to-near-150-billion-in-2014.htm>> [Accessed 22 May 2013].

Higgins, JM. 1995. Innovation: The core competence. *Strategy & Leadership* 23(6):32-36. Available at: <[Cameron Bassett](http://0-</a></p></div><div data-bbox=)

- dx.doi.org.oasis.unisa.ac.za/10.1108/eb054532> [Accessed 25 May 2014].
- Hilton, S. 2010. *Cloud Computing Is No Fad*. Information Week SMB, Forbes [Online] Available at: <<http://www.forbes.com/2010/07/12/cloud-computing-growth-entrepreneurs-technology-informationweeksmb.html>> [Accessed 25 August 2012].
- Himmel, MA. 2012. *Qualitative Analysis of Cloud Computing Risks and Framework for the Rationalization and Mitigation of Cloud Risks*. Pace University.
- Hurley, C. 2004. What, If Anything, Is Records Management? *Records Management Association of Australasia Conference. Canberra, Australia 12-15 September 2004*. Available from: <http://www.infotech.monash.edu.au/research/groups/rcrg/publications/ch-what.pdf>.
- ICO. n.d. The Guide to Data Protection. [Online] Available at: <[http://www.ico.org.uk/for\\_organisations/data\\_protection/~/\\_media/documents/library/Data\\_Protection/Practical\\_application/the\\_guide\\_to\\_data\\_protection.pdf](http://www.ico.org.uk/for_organisations/data_protection/~/_media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf)> [Accessed 11 November 2013].
- ICO. 2012. Monetary penalty notices. [Online] Available at: <<http://www.ico.org.uk/enforcement/fines>> [Accessed 05 January 2014].
- ISO. 2001. ISO/TR 15489-1:2001. [Online] Available at: <[http://www.iso.org/iso/catalogue\\_detail?csnumber=31908](http://www.iso.org/iso/catalogue_detail?csnumber=31908)> [Accessed 09 April 2013].
- ISO. 2009. ISO/TR 15801:2009. [Online] Available at: <[http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=50499](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50499)> [Accessed 21 November 2012].
- ISO. 2011. ISO/TR 23081-3:2011. [Online] Available at: <[http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=57121](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57121)> [Accessed 21 November 2012].
- ISO 2005. ISO/IEC 27002:2005. [Online] Available at: <[http://www.iso.org/iso/home/store/catalogue\\_ics/catalogue\\_detail\\_ics.htm?csnumber=50297](http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50297)> [Accessed 21 November 2012].

- ISO n.d. Benefits of International Standards. [Online] Available at: <<http://www.iso.org/iso/home/standards/benefitsofstandards.htm>> [Accessed 27 June 2013].
- Jadeja, Y. & Modi, K. 2012. 'Cloud computing - concepts, architecture and challenges' in IEEE (Institute of Electrical and Electronics Engineers). *International Conference on Computing, Electronics and Electrical Technologies*. Nagercoil, Tamil Nadu, India, 21-22 March. New York: Curran Associates.
- Kandira, M. 2013. *A strategic framework for cloud computing security and compliances requirements to enable cloud services adoption*. (Unpublished Masters Dissertation). University of South Africa.
- Kisten, B 2013. *Information security risk management in cloud computing*. (Unpublished Masters Dissertation). University of South Africa.
- Lala, R. 2012. The Power of Cloud: Driving Business Model Innovation. [Online] Available at: <[http://www.eiseverywhere.com/file\\_uploads/0c4722a03eb565b93f948df0e71d38c8\\_Cloud\\_enabled\\_Business\\_Transformation.pdf](http://www.eiseverywhere.com/file_uploads/0c4722a03eb565b93f948df0e71d38c8_Cloud_enabled_Business_Transformation.pdf)> [Accessed 6 June 2014].
- Laudon, KC. & Laudon, JP. 2011. *Management Information Systems: Managing the Digital Firm*. 12<sup>th</sup> Edition. New Jersey: Prentice Hall.
- Leedy, PD & Ormrod, JE. 2013. *Practical research: planning and design*. 10th ed. Boston: Pearson.
- Lin, A. & Chen, N. 2012. Cloud computing as an innovation: Perception, attitude, and adoption. *International Journal of Information Management*, 32(2012), pp.533–540. Available at: <http://dx.doi.org/10.1016/j.ijinfomgt.2012.04.001>.
- Ludwig, S. 2011. Dropbox bug drops passwords, underscoring the cloud's risks. *Venturebeat*. [Online] 21 June 2011. Available at: <<http://venturebeat.com/2011/06/21/dropbox-files-left-unprotected-for-four-hours-due-to-software-bug/>> [Accessed on 1 November 2013].
- Mack, N., Woodsong, C., MacQueen, K.M., Guest, G. & Namey, E. 2005. *Qualitative research methods: a data collector's field guide*. Durham, NC: Family Health International.

- Macvittie, L. 2009. Control, choice, and cost: The Conflict in the Cloud. [Online] Available at: <https://devcentral.f5.com/articles/control-choice-and-cost-the-conflict-in-the-cloud#.UndTWZE2-f0> [Accessed 2 November 2013].
- Mahmood, Z. 2011. Cloud Computing for Enterprise Architectures: Concepts, Principles and Approaches, in Z Mahmood & R Hill *Cloud Computing for Enterprise Architectures*. London: Springer. Ch.1.
- Marshall, M. 2012. Dropbox has become ‘problem child’ of cloud security. *Venturebeat*. [Online] 1 August 2012. Available at: <http://venturebeat.com/2012/08/01/dropbox-has-become-problem-child-of-cloud-security/>.> [Accessed on 1 November 2013].
- Marston, S., Bandyopadhyay, S., Zhang, J. & Ghalsasi, A. 2011. Cloud computing — The business perspective. *Decision Support Systems*, 51(1), pp.176–189. Available at: <http://www.sciencedirect.com/science/article/pii/S0167923610002393> [Accessed July 9, 2014].
- McKemmish, S. 2013. ‘Recordkeeping and Archiving in the Cloud. Is There a Silver Lining?’ in The Future Of Information Sciences, 4th International Conference *The Future of Information Sciences: INFUTURE2013 – Information Governance*, Zagreb, 6-8 November 2013. Croatia: University of Zagreb.
- Mell, P. & Grance, T. 2011. *The NIST Definition of Cloud Computing* [online] Gaithersburg: National Institute of Standards and Technology. Available at: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> [Accessed 05 April 2013].
- Merriam, SB. 2009. *Qualitative Research A Guide to Design and Implementation*. San Francisco. John Wiley & Sons.
- Microsoft. 2013. Active Directory Domain Services. [Online] Available at: <http://technet.microsoft.com/en-us/windowsserver/dd448614.aspx> [Accessed 5 January 2014].
- MineRP (Australia). 2012. Document Management Standard. [corporate document] Brisbane: MineRP (Australia).
- Mohan, R. 2011. Storms in the Cloud: Lessons from the Amazon Cloud Outage. *Security Week*, [online] 6 June 2011. Available at: <

- <http://www.securityweek.com/storms-cloud-lessons-amazon-cloud-outage> [Accessed 15 February 2014].
- Mollah, MB., Islam, RK. & Islam SS. 2012. Next Generation of Computing through Cloud Computing Technology, in IEEE (Institute of Electrical and Electronics Engineers) *25th IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)*, Montreal, Canada, 29 April - 02 May. New York: Curran Associates.
- Mouton, J. 1996. *Understanding social research*. Pretoria: Van Schaik.
- National Archives of Australia. 2010. AGLS Metadata Standard. [Online] Available at: <<http://www.agls.gov.au/pdf/AGLS%20Metadata%20Standard%20Part%202%20Usage%20Guide.PDF>> [Accessed 13 June 2013].
- National Archives of Australia. 2013a. A Checklist for Records Management and the Cloud. [Online] Available at: <<http://www.naa.gov.au/records-management/publications/cloud-checklist.aspx>> [Accessed 12 June 2013].
- National Archives of Australia. 2013b. Australian and international standards. [Online] Available at: <<http://www.naa.gov.au/records-management/strategic-information/standards/ASISOstandards.aspx>> [Accessed 12 June 2013].
- National Archives of Australia. 2013c. Legislation that affects how your agency manages its records. [Online] Available at: <<http://www.naa.gov.au/records-management/strategic-information/standards/recordslegislation.aspx>> [Accessed 18 June 2013]
- National Archives of Australia. 2013d. Records management and the cloud. [Online] Available at: <<http://www.naa.gov.au/records-management/agency/secure-and-store/rm-and-the-cloud/index.aspx>> [Accessed 12 June 2013].
- National Archives of Australia. 2013e. What is records management? [Online] Available at: <<http://www.naa.gov.au/records-management/getting-started/records-management/index.aspx>> [Accessed 13 October 2015]
- NeCTAR, 2011. Research Cloud. [Online] Available at: <[http://www.nectar.org.au/sites/default/files/CloudBrochure\\_3.pdf](http://www.nectar.org.au/sites/default/files/CloudBrochure_3.pdf)> [Accessed 27 May 2013].
- Office of the Australian Information Commissioner. n.d. The Privacy Act.

- [Online] Available at: <<http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act>> [Accessed 18 June 2013].
- Onwubiko, C. 2010. Security Issues to Cloud Computing. In Antonopoulos, N. & Gillam, L. 2010. *Cloud Computing Principles, Systems and Applications*. London: Springer. Ch.16
- Opala, OJ. 2012. *An Analysis Of Security, Cost-Effectiveness and IT Compliance Factors Influencing Cloud Adoption By IT Managers*. PHD. Capella University.
- Oxford Dictionaries. 2013. Oxford University Press, UK. Available at: <<http://oxforddictionaries.com>> [Accessed 27 May 2013].
- Quddusi, S.U.H., 2014. Document management and cloud computing. *The TQM Journal*, 26(2), pp.102–108. Available at: <http://dx.doi.org/10.1108/TQM-06-2012-0038>. [Accessed January 18, 2015].
- Queensland Government. 2013a. Risks of cloud computing. [Online] Available at: <<http://www.business.qld.gov.au/business/running/technology-for-business/cloud-computing-business/cloud-computing-risks>> [Accessed 18 June 2013].
- Queensland Government. 2013b. Privacy laws. [Online] Available at: <<http://www.business.qld.gov.au/business/starting/legal-obligations/protecting-privacy-information/privacy-laws>> [Accessed 18 June 2013].
- Rabai, L.B.A., Jouini, M., Aissa, A.B., Mili, A. 2013. A cybersecurity model in cloud computing environments. *Journal of King Saud University - Computer and Information Sciences*, 25(1):pp.63–75. Available at: <http://www.sciencedirect.com/science/article/pii/S131915781200033X> [Accessed September 15, 2015].
- Ramgovind, S. 2010. *What are the information security considerations in cloud computing*. (Unpublished Masters Dissertation). University of South Africa.
- Read, J. & Glinn, ML. 2011. *Records Management*. 9<sup>th</sup> Edition. Mason: South-Western Cengage Learning.
- Reed, B. 2005. Records, in *Archives: Recordkeeping in Society*, edited by S. McKemmish, M. Piggott, B. Reed & F. Upward. Wagga Wagga: Centre for Information Studies.

- Reed, J. 2011. Following Incidents into the Cloud. *SANS Reading Room*. [Online] Available at: <<http://www.sans.org/reading-room/whitepapers/incident/incidents-cloud-33619>> [Accessed March 5 2014].
- Rimal, BP., Choi, E. and Lumb, I. 2010. Taxonomy, Survey, and Issues of Cloud Computing Ecosystems, in *Cloud Computing Principles, Systems and Applications*, edited by N Antonopoulos & L Gillam. London: Springer. Ch.2.
- Rittinghouse, JW. & Ransome, JF. 2010. *Cloud Computing Implementation, Management, and Security*. Boca Raton: CRC Press.
- Rodrigues, ADS. 2013. An archival collecting framework for the records generated by South Africa's Portuguese community-based organisations in Gauteng. PHD, University of South Africa.
- Rogers, EM. 2003. *Diffusion of Innovations*. 5th Edition. New York. Free Press.
- Ross, VW. 2010. *Factors influencing the adoption of cloud computing by decision making managers*. Capella University.
- Salesforce. 2013. What is CRM?. [Online] Available at: <<http://www.salesforce.com/eu/crm/what-is-crm.jsp>> Accessed 12 August 2013].
- Saunders, M, Lewis, P, & Thornhill, A. 2007. *Research methods for business students*. 4th ed. Harlow: Pearson.
- Sims, J.E. 2012, *Information security in the age of cloud computing*, The University of Mississippi.
- Soliman, F. 2012. Role of Cloud Systems as a Global Innovation Crucible, in IEEE (Institute of Electrical and Electronics Engineers) *IEEE Symposium on E-Learning, E-Management and E-Services (IS3e)*, Kuala Lumpur, Malaysia, 21-24 October. New York: Curran Associates.
- Sosinsky, B. 2011. *Cloud Computing Bible*. Indianapolis: Wiley Publishing.
- Staneovska-Slabeva, K., Wozniak, T. & Ristol, S. 2010. *Grid and Cloud Computing: A Business Perspective on Technology and Applications*. Heidelberg: Springer.
- State Records of Southern Australia. 2011. Australian Standard AS ISO 15489 - Records Management. [Online] Available at:

- <[http://www.archives.sa.gov.au/files/management\\_ARM\\_ISO15489.pdf](http://www.archives.sa.gov.au/files/management_ARM_ISO15489.pdf)>  
[Accessed 18 April 2013].
- Stuart, K. & Bromage, D. 2010. Current state of play: records management and the cloud, *Records Management Journal* 20(2):217-225. Available at: <<http://dx.doi.org/10.1108/09565691011064340>> [Accessed 23 March 2012].
- Suo, S. 2013, *Cloud implementation in organizations: Critical success factors, challenges, and impacts on the IT function*, The Pennsylvania State University.
- Sun, D., Chang, C., Sun., L. & Wang, X., 2011. Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments. *Procedia Engineering*, 15, pp.2852–2856. Available at: <http://www.sciencedirect.com/science/article/pii/S1877705811020388> [Accessed November 13, 2014].
- Tellis, W. 1997. Introduction to Case Study. *The Qualitative Report, Volume 3* (2). [Online] July 1997. Available at: <http://www.nova.edu/ssss/QR/QR3-2/tellis1.html>. Accessed 01 February 2015.
- Thomas, PY. 2010. Cloud computing: A potential paradigm for practising the scholarship of teaching and learning. *The Electronic Library* 29(2):214-224. Available at: <<http://dx.doi.org/10.1108/02640471111125177>> [Accessed 23 March 2012].
- Trope, J. 2013. *Adoption of cloud computing by South African firms: an institutional theory and diffusion of innovation theory perspective*. (Unpublished Masters Dissertation). Johannesburg: University of the Witwatersrand.
- Underwood, J. & Isikdag, U. 2011. Merging technologies for BIM 2.0. *Construction Innovation: Information, Process, Management* 11(3):252-258. Available at: <<http://dx.doi.org/10.1108/14714171111148990>> [Accessed 25 August 2012].
- Unisa 2012. Policy on research ethics. Available at: <[http://www.unisa.ac.za/contents/colleges/col\\_agriculture\\_enviro\\_n\\_sciences/docs/ResearchEthicsPolicyJan2013.pdf](http://www.unisa.ac.za/contents/colleges/col_agriculture_enviro_n_sciences/docs/ResearchEthicsPolicyJan2013.pdf)> [Accessed: 28 February 2013]
- United States of America. 2001. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism



- Act of 2001 (USA PATRIOT ACT) (Public Law 107–56, Oct. 26, 2001). Available at: GPO Access, <<http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>> [Accessed 21 November 2012].
- Vaquero, LM., Rodero-Merino, L., Caceres, J. & Lindner, M. 2009. A break in the clouds: Towards a cloud definition. *SIGCO M M Computer Communications Review* (39):50-55. Available at: <<http://www.research.ibm.com/haifa/projects/systech/reservoir/public/CloudDefinitionPaper.pdf>> [Accessed on 24 September 2012].
- Velte, AT. Velte, T.J. & Elsenpeter, R. 2010. *Cloud Computing: A Practical Approach*. New York: McGraw-Hill.
- Willcocks, LP. Venters, W. & Whitleym EA. 2013. Cloud sourcing and innovation: slow train coming? A composite research study. *Strategic Outsourcing: An International Journal* 16(2):184-202. Available at: <<http://0-dx.doi.org.oasis.unisa.ac.za/10.1108/SO-04-2013-0004>> Accessed on 8 March 2014].
- Yin, RK. 2003. *Case Study Research Design and Methods*. 3<sup>rd</sup> Edition. Thousand Oaks: Sage.
- Zhang, K. 2012, *Security in cloud computing: New challenges and solutions*, Indiana University.

## **Annexure A: Company X Documentation practices questionnaire**

## **Company X Documentation practices questionnaire**

The following questionnaire is designed to survey the departments at Company X with regard to their current documentation practices in view of Company X's consideration of adopting cloud computing for their future storage requirements.

This is a departmental survey for the following departments:

- Consulting
- Marketing
- Project management
- Business development
- Training & Technical writing

### **Personal details**

**Name:**

**Department:**

**Date:**

### **Questionnaire**

*Your responses to these questions will provide data relating to the types of information that you use to perform your work task, the types of documentation that your department generates, as well as your records management practices. It will also provide data that will enable the mapping of information flows within the organization and between the organization and external environment. Thank you for your cooperation!*

## Section A: Work Tasks

This section of the questionnaire deals with tasks (work) that are performed by the department.

1. Please mention the tasks that your department performs as well as the information that is required to perform these tasks. *For example, Promotional material generation: Requires graphics and product information.*

TASK	INFORMATION REQUIRED
Task 1:	
Task 2:	
Task 3:	
Task 4:	
Task 5:	
Task 6:	
Task 7:	
Task 8:	



6. If you could recommend an improvement to this information in relation to its content what would it be?

7. If you could recommend an improvement to this information in relation to its format what would it be?

8. Is there any information required to help your department function more effectively?

9. What type of information would make the greatest impact on your department's tasks?

10. What sources/resources does your department utilise, in order to find the information, they require? *For example, internet, publication, client given information etc.*

11. Would more timely information impact on your department's ability to make more effective decisions? *(Please tick relevant boxes)*

Yes

No

12. How does your department stay current about events happening in your industry?

## Section B: Record Types

This section of the questionnaire deals with documentation in the department.

13. Who in your department creates documentation? *E.g. only you, consultants, developers etc.*

14. What kinds of documentation do they create? *(Please tick relevant boxes)*

.doc/docx

.xls

.pdf

other

Marketing

software files

material

15. What role does the user of these types of documentation have? *e.g. engineer, software developer*

16. Who reviews/finalizes documentation in your department?

17. Who edits documentation in your department?



18. Who uses documentation in your department?

19. Who approves the publication/distribution of documentation?

20. Who sets guidelines and policies for managing documentation? (e.g. *Access restrictions*)

21. Who manages documentation in your department?

### **Section C: Issues**

This section of the questionnaire deals with issues that have been experienced by the department.

22. How well do you manage your documentation once you obtain it?

23. If applicable, give an example of past mismanagement of documentation.

## Section D: Storage location

This section of the questionnaire deals with where documentation is stored by the department.

24. Where do you store documentation on the server? (please specify locations)

Document Type	Location on server

25. Is your documentation saved directly to the server or is the majority of your documentation based on your hard drive? (*Please tick relevant boxes*)

Server       Hard drive

26. Is your documentation created in one format and later changed to another? (*Please tick relevant boxes*)

Yes       No

27. How do you categorize documentation?

28. What categorization preference do you use for documentation?

29. Is there a categorization preference based on importance of documentation? (*Please tick relevant boxes*)

Yes       No

30. IF "Yes" who decides the Level of importance?

31. Is this categorization system being used by others in your department? *(Please tick relevant boxes)*

Yes       No

### **Section E: Shared usage**

This section of the questionnaire addresses the sharing of documentaion.

32. Could the information you have access to be valuable to other departments? *(Please tick relevant boxes)*

Yes       No

33. With which departments do you share information? *(Please tick relevant boxes)*

Finance      &       Training      &       Consulting  
HR                      Tech Writing  
 Marketing       Business       Project  
   Development      Management

### **Section F: Solutions proposed by departments**

This section of the questionnaire deals with any solutions proposed by the department.

34. What opportunities do you see for improving the effectiveness and productivity of your department's tasks through the use of information resources and technologies? *For example, cloud computing*

35. Do you understand what cloud computing is? *(Please tick relevant boxes)*

Yes

No

36. Do you currently utilise any cloud based storage? *(Please tick relevant boxes)*

Yes

No

37. How might new technology assist your department in its tasks? *For example, cloud computing can enable always available information despite a user's location.*

## **Annexure B: Company X overview**

Company X is a mining software development company in Australia, which provides specialised services relating to consulting, mining shaft designs and mining software development.

These tasks require Company X to be able to access and store their relevant records and project data wherever a client may be. Company X was experiencing various issues, such as file duplication and multiple versions of files, with their current internal storage system. Company X constructed a case study to access its internal server layout and the documentation practices of departments.

Company X operates with a specialised field, which deals with issues such as:

- Limited connectivity
- Remote locations of clients
- Everywhere accessible data
- Costs
- Security of stored data