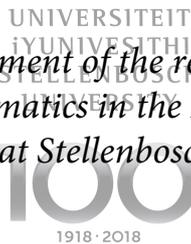


**Adoption of SaaS-based ERP by SMEs in an
emerging market economy:
Giving up control over mission critical business
software**

**by
Philippus Bernardus de Wet**



*Thesis presented in fulfilment of the requirements for the degree of
Master of Socio-Informatics in the Faculty of Arts and Social
Sciences at Stellenbosch University*



Supervisor: Dr. Andrew Boake
Supervisor: Prof. Bruce Watson

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date:

Copyright © 2018 Stellenbosch University

All rights reserved

Abstract

Small and Medium Enterprises (SMEs) are playing a key contribution to a healthy economic environment. Traditional Enterprise Resource Planning (ERP) systems are generally too expensive for SMEs. Fortunately for technological enhancements, cloud computing makes it possible for companies to rent ERP on a subscription or a pay-per-use model. Due to cash flow, capital and human resource constraints, the public cloud is an ideal solution for SMEs. The business application as well as the server infrastructure is owned and maintained by cloud service providers. Previous studies have found that by losing direct control over systems is one of the main disadvantages of Software-as-a-Service (SaaS-based) ERP.

By adopting SaaS-based ERP, organisations fear that they will lose control over the security and privacy of their data making their systems vulnerable to data breaches. In addition, loss of control over system performance and uptime might also cause rejection of SaaS. The purpose of this qualitative research study is to explore the adoption of SaaS-based ERP by SMEs in an emerging economy like South Africa, when not only control, but also trust is placed in the hands of third-party providers to manage, protect and support the heart of a business, i.e. its mission critical business system. An analysis is required of the adopter categorisation where local SMEs currently find themselves in and an understanding of SMEs willingness to outsource their IT, data and business software.

This study has found that on the basis of Roger's diffusion of innovations (DOI) theory, if any of the SME participants would want to adopt a SaaS application, they would fall in the "late majority" adoption category. With 53% of the business applications used in this research study is of a SaaS type, it can be said that the peak of the innovativeness curve has been reached for SMEs partaking in this study. Overall, it has been found that SaaS-based ERP performed better than conventional ERP by achieving a 32% higher ranking in functionality and a 27% higher ranking in provider support.

While planned downtime outside business hours has no effect on the adoption of SaaS-based ERP by SMEs in this study, planned downtime within office hours, unplanned downtime and severe cloud outages does have an effect. Most SMEs wouldn't reject SaaS-based ERP; they would rather prefer to switch cloud providers.

It turns out that most SMEs in this study are risk averse and will reject a system previously hacked. It has been found that a major security breach would have an impact on SaaS-based ERP adoption. Such an event would cause most participants to switch to an alternative provider; half of which would migrate back to an on-premise ERP application. Vendor lock-in

will complicate such a transition process. It has also been found that the local SMEs don't take full responsibility for protecting their systems against security breaches.

Trust is considered to be the third most important cloud adoption factor and that the majority of these SMEs are comfortable with handing control over to cloud providers. Brand, reputation and a comprehensive Service Level Agreement (SLA) impacts trusting relationships and provides peace of mind to SaaS tenants. It appears that changes and challenges related to control cause a shift in trust, from personal relationships in the traditional sense to a system that's secure and stable with little downtime.

All the SaaS-based ERP tenants are located in or close to main cities. By focusing on SME operating in remote towns with a poor technological infrastructure, further research will add more value by focussing on last mile connectivity, broadband technology and connection latency challenges.

Opsomming

Klein en medium ondernemings (KMO's) speel 'n belangrike rol tot 'n gesonde ekonomiese omgewing. Meeste van hierdie organisasies kan nie tradisionele ondernemingshulpbronbeplanning (OHB) stelsels bekostig nie. Gelukkig maak tegnologiese verbeterings in wolkverwerking dit moontlik om OHB en ander soortgelyke besigheidstelsels te huur op 'n subskripsie of 'n betaal-soos-jy-gebruik basis. Die stelsel, sowel as die bediener infrastruktuur, is die eiendom van wolkdiensverskaffers en word deur hulle onderhou. Weens beperkte kontantvloei, kapitaal en menslike hulpbronne is wolkverwerking 'n ideale opsie vir KMO's. Vorige studies het bevind dat een van die vernaamste nadele van Sagnetware-as-'n-Diens (SanD-gebaseerde) OHB-stelsel is om direkte beheer oor stelsels te verloor.

Deur die aanneming van SanD-gebaseerde OHB-stelsel, vrees organisasies dat hulle beheer oor die sekuriteit en privaatheid van hul data sal verloor, wat sodoende hul stelsels kwesbaar maak vir data-oortredings. Daarbenewens kan die verlies van beheer oor stelselprestasie en beskikbaarheid ook beteken dat SanD-gebaseerde OHB-stelsels moontlik verwerp mag word. Die doel van hierdie kwalitatiewe navorsingstudie is om ondersoek in te stel oor die aanneming van SanD-gebaseerde OHB-stelsels deur KMO's in 'n opkomende ekonomiese mark soos Suid-Afrika. Spesifiek wanneer beide beheer en vertroue in die hande van derdeparty-diensverskaffers geplaas word om die hart van 'n besigheid te bestuur, beskerm en te ondersteun. Deur te bepaal waar plaaslike KMO's hulself tans bevind, moet 'n ontleding gedoen word in terme van die aannemingskategorie. Dit is ook noodsaaklik om begrip te hê van KMO's se bereidwilligheid om hul IT-, data- en besigheids-sagnetware uit te kontrakkeer.

Indien enige van die KMO-deelnemers 'n SanD-toepassing wil aanneem, het hierdie studie bevind dat op grond van Roger se diffusie van innovasies teorie, hulle in die "laat meerderheid" aannemingskategorie sal val. Aangesien 53% van die sagnetware wat vir besigheidsdoeleindes in hierdie navorsingsstudie gebruik word van 'n SanD-tiepe is, kan daar afgelei word dat die KMO's wat aan hierdie studie deelgeneem het, die piek van die innoveringskurwe bereik het. Oor die algemeen is gevind dat SanD-gebaseerde OHB-stelsels beter presteer as konvensionele OHB-stelsels aangesien KMO's in hierdie studie hul 32% hoër gegradeer het in terme van funksionaliteit en 27% hoër vir verskafferondersteuning.

Terwyl beplande stelsel aftyd buite besigheidsure geen invloed op die aanneming van SanD-gebaseerde OHB-stelsels deur KMO's in hierdie studie het nie, het beplande aftyd binne kantoorure, onbeplande aftyd en ernstige wolkonderbrekings, wel 'n effek. Die meeste KMO's sal nie 'n SanD-gebaseerde OHB-stelsel verwerp nie; hulle sal wel eerder verkies om van wolkverskaffers te verander.

Dit blyk dat die meerderheid van die KMO's in hierdie studie riskant is en 'n stelsel waarop inbraak gemaak is, sal verwerp. Daar is bevind dat 'n groot sekuriteitsoortreding 'n negatiewe impak sal hê op die aanneming van SanD-gebaseerde OHB-stelsels. Indien so 'n gebeurtenis wel sou plaasvind, sal die meeste van die deelnemers oorsakel na 'n alternatiewe verskaffer; waarvan die helfte sal terugval na 'n tradisionele OHB-stelsel. Verskaffer afhanklikheid sal wel so 'n oorgangsproses bemoeilik. Daar is ook bevind dat die plaaslike KMO's nie volle verantwoordelikheid neem deur hul stelsels te beskerm teen sekuriteitsoortredings nie.

Vertroue word beskou as die derde belangrikste wolk-aannemingsfaktor en dit was bevind dat die meerderheid van die KMO's gemaklik is om beheer van hul OHB-stelsels oor te gee aan wolkverskaffers. Handelsmerke, reputasie en 'n omvattende diensvlakooreenkoms het 'n impak op vertrouensverhoudings en bied gemoedsrus aan SanD-huurders. Dit blyk dat

veranderinge en uitdagings met betrekking tot die oorgee van beheer 'n verskuiwing in vertroue veroorsaak, van persoonlike verhoudings in die tradisionele sin na 'n besigheidstelsel wat veilig en stabiel is met baie min afdyd.

Al die SanD-gebaseerde OHB-huurders is geleë in of naby hoofstede. Deur te fokus op KMO's wat in afgeleë dorpe wat oor 'n swak tegnologiese infrastruktuur beskik, sal verdere navorsing meer waarde toevoeg deur te fokus op die laaste myl-konneksie, breëbandtegnologie en latensie uitdagings.

Acknowledgements

Ek wil eerstens my ouers bedank vir hulle ondersteuning, liefde en omgee– julle het al die jare by my gestaan en in my geglo.

Waldu, my engel uit die hemel! Dankie dat jy saam met my die pad gestap het en jou ondersteuning deur moeilike tye. Lief jou baie.

Vir al my vriende en kollegas wat gereëld gevra het hoe dit gaan en hoe my tesis vorder, dankie vir julle belangstelling en ondersteuning.

To my company director, Stephen Howe. Thank you for assisting me through this journey and allowing me to take hours and full days off when I needed it.

A special thank you to my research supervisors Prof. Bruce Watson and Dr. Andrew Boake. Your insights, guidance, patience and time are greatly appreciated. I will miss our early morning breakfast sessions dearly.

To my Creator, thank you for being with me every step of the way.

List of abbreviations

ADSL	-	Asymmetric Digital Subscriber Line
ASP	-	Application Service Provider
BER	-	Bit Error Rate
BRICS	-	Association of: Brazil, Russia, India, China and South Africa
BYOD	-	Bring-your-own-device
CAPEX	-	Capital Expenses
CPT	-	Cape Town
CRM	-	Customer Relationship Management
DBA	-	Database Administrator
DBIR	-	Data Breach Investigations Report
DDoS	-	Distributed-Denial-of-Service
DES	-	Data Encryption Standard
DME	-	Developed Market Economy
DoS	-	Denial-of-Service
DSL	-	Digital Subscriber Line
EME	-	Emerging Market Economy
ERP	-	Enterprise Resource Planning
EU	-	European Union
GDP	-	Gross Domestic Product
HaaS	-	Hardware-as-a-Service
HR	-	Human Resource
HTTP	-	Hyper Text Transfer Protocol
HTTPS	-	Hyper Text Transfer Protocol Secure
JHB	-	Johannesburg
IaaS	-	Infrastructure-as-a-Service
IAS	-	International Accounting Standard (IAS)
ICASA	-	Independent Communications Authority of South Africa
IS	-	Information System
ISP	-	Internet Service Provider
IT	-	Information Technology
KMS	-	Klein en Medium Ondernemings

NAT	-	Network Address Translation
NIST	-	National Institute of Standards and Technology
OHB	-	Ondernemingshulpbronbeplanning
OPEX	-	Operational Expenses
OS	-	Operating System
PaaS	-	Platform-as-a-Service
PER	-	Packet Error Rate
POS	-	Point-Of-Sale
SaaS	-	Software-as-a-Service
SADC	-	Southern Africa Development Community
SDL	-	Security Development Lifecycle
SINR	-	Signal to Interference plus Noise Ratio
SLA	-	Service Level Agreement
SME	-	Small and Medium-sized Enterprise
SNR	-	Signal to Noise Ratio
SanD	-	Sagteware-as-'n-Diens
SOAP	-	Simple Object Access Protocol
SoD	-	Segregation of Duties
SSL	-	Secure Socket Layer
TSL	-	Transport Security Layer
UFB	-	Ultra-Fast Broadband
VDSL	-	Very-high-bitrate Digital Subscriber Line service
WWW	-	World Wide Web
XML	-	Extensible Markup Language

Contents

Part 1: Prologue	1
Chapter 1: Introduction	1
1.1 Introduction	1
1.2 Previous studies that address the problem	2
1.3 Limitations of previous studies.....	4
1.4 Relevance of the study	5
1.5 Purpose statement	6
1.6 Conclusion	6
Chapter 2: Literature review	7
2.1 Background	7
2.2 Key Concepts.....	7
2.2.1 SMEs in an Emerging Market Economy.....	7
2.2.2 Traditional Enterprise Resource Planning (ERP) systems.....	9
2.2.3 Cloud Computing	12
2.2.4 SaaS-based ERP.....	19
2.2.5 SaaS-based ERP adoption in an Emerging Economy.....	25
2.2.6 SaaS ERP risk: Loss of control over security	29
2.2.7 SaaS ERP risk: Loss of control over system availability.....	41
2.2.8 Provider support and trust.....	49
2.3 Conclusion	51
Chapter 3: Research Design Methodology	53
3.1 Research topic	53
3.2 Research aim and objectives.....	54
3.3 Research method.....	54
3.4 Research questions.....	55
3.5 Conclusion	56
PART 2: Analysis	57
Chapter 4: SaaS-based ERP Adoption.....	57
4.1 Introduction	57
4.2 Research participants in this study	57
4.2.1 SME Customers.....	57
4.2.2 Application providers.....	59
4.3 Adoption of SaaS and SaaS-based ERP by SMEs in emerging markets.....	60
4.3.1 Benefits, Challenges and risks of SaaS-based ERP vs. conventional ERP/accounting systems	60
4.3.1.1 Comparison of perceived and actual ERP benefits.....	60
4.3.1.2 Comparisons of ERP challenges and risks	61

4.3.2	Roger’s diffusion of innovation theory: Adopter category of local SMEs	65
4.3.2.1	The extent of ERP/Accounting systems being used	65
4.3.2.2	The extend of cloud computing file sharing and storage being used.....	71
4.3.2.3	The extend of SaaS business applications being used.....	71
4.3.2.4	Adopter category of SaaS solutions by local SMEs	74
4.4	Critical SaaS-based ERP adoption factors	75
4.4.1	Critical SaaS-based ERP Adoption factors identified by SMEs in EMEs	75
4.4.2	Critical adoption factors identified by cloud application providers in EMEs.....	78
4.4.3	Comparison of critical adoption factors between market economies	79
4.5	Conclusion	81
Chapter 5: Cloud Support.....		83
5.1	Introduction	83
5.2	The impact of support on SaaS-based ERP adoption.....	83
5.3	Provider support findings.....	86
5.3.1	Application provider support.....	86
5.3.2	Internet service provider support.....	87
5.3.3	Cloud business platform hosting provider support.....	88
5.4	Support issues and loss of business.....	89
5.5	Conclusion	90
Chapter 6: Cloud Availability.....		92
6.1	Introduction	92
6.2	The impact of cloud downtime on SaaS-based ERP adoption	92
6.3	Actual scheduled and unscheduled downtime	95
6.3.1	Scheduled downtime.....	95
6.3.2	Unscheduled downtime.....	96
6.3.3	Cloud application providers and downtime.....	98
6.4	Service Level Agreements and cloud uptime percentages	99
6.5	Business continuity plans	100
6.6	Cloud connectivity	100
6.6.1	Connectivity requirements.....	101
6.6.2	Connectivity challenges	101
6.6.3	Connectivity experiences	102
6.7	Conclusion	105
Chapter 7: Data Security and Data Privacy		107
7.1	Introduction	107
7.2	The impact of security breaches on SaaS-based ERP adoption.....	108
7.3	Internal and external security breaches	109
7.4	SaaS tenants and Conventional Customer findings.....	109

7.5	Cloud application provider findings	111
7.6	Data privacy	112
7.7	Conclusion	113
Chapter 8: Trust and change in business models		115
8.1	Introduction	115
8.2	Changes in a cloud provider's business model	115
8.3	Creating and maintaining trust in SaaS	118
8.4	Conclusion	119
PART 3: Epilogue		121
Chapter 9: Conclusions and Recommendations		121
9.1	Introduction	121
9.2	Summary of the study.....	121
9.2.1	Overview of the problem and methodology	121
9.2.2	Findings, trends and what it means in terms of literature.....	122
9.3	Limitations	124
9.4	Future works	124
9.5	Conclusion	125
Bibliography		126
Appendixes		135
Appendix A		135
Appendix B		135

List of figures

Figure 1: Top 10 Emerging Markets from 2012 to 2017 ((M-Brain (previously Global Intelligence Alliance), 2012)	8
Figure 2: Separation of responsibilities (“YungChou”, 2010)	15
Figure 3: Application types deployed on Public Cloud (Sfondrini, Motta and You, 2015)	20
Figure 4: ERP deployments by business size in 2012 (Castellina, 2012)	21
Figure 5: Adopter Categorisation on the Basis of Innovativeness (Rogers, 2003)	27
Figure 6: Threat actor categories over time. Source: (Verizon, 2017).....	33
Figure 7: Percentage of breaches per threat category over time. Source: (Verizon, 2017) ..	34
Figure 8: SMEs deployment model breakdown	58
Figure 9: SME locations within South Africa (MapCustomizer, 2018)	59
Figure 10: Number of years trading (SaaS).....	66
Figure 11: Previous system used: (SaaS)	66
Figure 12: Number of system users (SaaS)	67
Figure 13: Functionality rating (SaaS)	67
Figure 14: Number of years trading (Conventional)	68
Figure 15: Number of system users (Conventional)	70
Figure 16: System functionality rating (Conventional).....	70
Figure 17: Business applications by deployment model (SaaS group)	72
Figure 18: Business applications by deployment model (Conventional)	73
Figure 19: Adoption of SaaS-based business applications	74
Figure 20: Adopter categorisation of SMEs on the basis of innovativeness	75
Figure 21: Top adoption factors by number of votes	76
Figure 22: Top 3 adoption factors	76
Figure 23: Top adoption factors by deployment model	78
Figure 24: Top adoption factors of SME and provider participants in an EME	79
Figure 25: Top adoption factors comparison- SMEs and providers in an EME vs. DME	80
Figure 26: Results of SaaS-based ERP selection scenarios	85
Figure 27: Support rating scale - Conventional vs SaaS	86
Figure 28: Rating scale - ISPs.....	88
Figure 29: Rating scale - Cloud hosting provider	89
Figure 30: Scheduled downtime outside business hours.....	93
Figure 31: Scheduled downtime within office hours.....	93
Figure 32: Unscheduled downtime within business hours	94
Figure 33: Severe server outage	94
Figure 34: Bandwidth technology upgrades	103
Figure 35: Effect of an external security breach	108
Figure 36: Ten changes SaaS has on a provider's business model	116

List of Tables

Table 1: Thirteen factors for adopting SaaS-based ERP (Rodrigues et al., 2016)	4
Table 2: The five perceived attributes of innovations (Rogers, 2003)	5
Table 3: Cloud Characteristics (Mell and Grance, 2009)	13
Table 4: Basic cloud requirements (Forrest, 2009)	13
Table 5: Cloud delivery models	15
Table 6: SaaS service model main characteristics	16
Table 7: Cloud deployment models (Schubert and Adisa, 2011)	17
Table 8: Cloud computing influencing factors	19
Table 9: Benefits and Concerns of Cloud Computing (Schubert and Adisa, 2011)	19
Table 10: SaaS-based ERP influencing factors (Castellina, 2012)	22
Table 11: SaaS-based ERP hindering factors (Castellina, 2012)	22
Table 12: Main benefits of SaaS-based ERP	23
Table 13: Main challenges of SaaS-based ERP	25
Table 14: Number of security incidents (Castellina, 2012)	30
Table 15: Types of security breaches (Durowoju et al. 2011)	34
Table 16: Authentication and authorisation preventative measures (Erpcloudnews, 2011) ..	38
Table 17: Quality of Service factors	44
Table 18: Business continuity plan per event type (Erpcloudnews, 2012)	47
Table 19: Downtime factors (Erpcloudnews, 2010)	48
Table 20: Deployment model per Industry	58
Table 21: Cloud application provider background	60
Table 22: Business application usage (SaaS group)	72
Table 23: Business application usage (Conventional)	73
Table 24: Top three adoption factors per SME	76
Table 25: Top 3 adoption factors by group	77
Table 26: SaaS-based ERP selection scenarios	84
Table 27: Bandwidth technology upgrades per SME	102
Table 28: South Africans affected by data leaks	113

Part 1: Prologue

Chapter 1: Introduction

1.1 Introduction

This research study investigates how the adoption of cloud-based ERP by SMEs in emerging market economies is influenced by factors such as lack of control by putting security and data privacy, system uptime, system connectivity and trust in the hands of third-party service providers.

SMEs play a major role in creating a healthy economic environment contributing to a country's Gross Domestic Product (GDP) and job creation. Due to capital constraints they have a limited budget to spend, especially on IT. While traditional ERP systems are too expensive, fortunately for technological enhancements, cloud computing makes it possible for companies to rent ERP on a subscription or pay-as-you-go basis. Cash flow, limited capital and man power constraints makes the public cloud an ideal option for SMEs. The main disadvantages of ERP deployed on the public cloud, also referred to Software-as-a-Service (SaaS), is that an organisation is losing direct control of its system and therefore face some challenges such as data security, data privacy, system uptime, system performance and downtime.

How does giving up control of data security, data privacy, cloud availability and the dependency on internet connectivity affect the adoption of SaaS-based ERP for SMEs in an emerging economy? To answer this primary research question, supporting questions have been asked to investigate the influence of these challenges on the adoption of SaaS-based ERP from both local SaaS provider and SaaS tenant's perspectives as well as the bigger role that trust plays when these elements are in the hands of third-party providers.

This research paper consists of nine chapters and is grouped into three parts: the prologue, analysis and the epilogue. In the first two chapters of the prologue, the research was conducted through a literature review that investigated previous work on the subject. The research design methodology, which entails the research topic, aim, objectives, the research method and the primary and secondary research questions, is discussed in detail in chapter three. The analysis part of the thesis starts at chapter four, where eight SMEs and two cloud application providers were interviewed to determine the extent of the influence of these factors. Based on these findings, it's possible to determine on the basis of innovativeness into which adopter category South African SMEs find themselves. Benefits and challenges of SaaS-based ERP are then compared with that of conventional systems. Lastly, the critical adoption

factors are determined that SMEs and cloud application providers in EMEs consider the most important. Chapter five investigates provider support provided to the SMEs and its impact on cloud adoption. Support encompasses infrastructure, platform and application support. Chapter six investigates the effect of scheduled downtime, unscheduled downtime, loss of data during downtime, downtime penalties, business contingency plans and connectivity on the adoption of SaaS-based ERP.

A central theme to this thesis is that by giving up control of core systems running in the public cloud, security is placed in the hands of others. Data security and data privacy are discussed in chapter seven. It's the responsibility of application providers to build the necessary application security measures into their systems and of cloud business platform hosting providers to protect the servers the application is running on. SaaS tenants however also have a responsibility and need to ensure that security measures are in place and to educate their employees about the risks cloud ERP exposes them to. User authentication, authorisation, segregation of duties and audit trails are some of the topics discussed.

Giving up of control is a major deciding factor for certain companies when they want to move their ERP/accounting applications over to the cloud as this involves putting their trust in others. Chapter nine examines the changes made to a provider's business model when the cloud is introduced to their customers. Trust was an important adoption factor amongst SMEs in a Developed Market Economy (DME). This chapter will verify the role of trust amongst SMEs in an EME.

The final part of this thesis is the epilogue. On a high level, chapter nine will provide a summary of the research problem, research findings and trends, limitations of the study and the significance of the results. The chapter will conclude by proposing additional research where gaps exist.

1.2 Previous studies that address the problem

The cloud has been a topic of numerous research studies. SaaS and specifically SaaS-based ERP have not yet fully matured and are still relatively new to being adopted by emerging markets.

Core to this study is the loss of control and the impact it has relative to cloud downtime, connectivity, data security, data privacy, changes in provider business models, changes in support models and the role of trusting relationships.

In 2013, a research study focussed on the reluctance of South African SMEs to consider a SaaS-based ERP business model. It was found that five inhibitor themes have emerged which

had a negative impact on Cloud-ERP adoption. In an order from most significant, these themes were (1) System performance and availability risk, (2) Sunk cost and satisfaction with existing systems, (3) Loss of control and Vendor trust, (4) Data security risk and (5) Functionality fit and customisation limitations (Faasen, Seymour and Schuler, 2013). The same researchers found that (6) Improved IT Reliability and (7) Perceived cost reduction were an additional two driver themes which had a positive impact on the adoption. There has been a considerable change in the landscape of cloud systems and technologies since then.

A research dissertation by Sahin (2013) investigated security challenges of cloud ERP from a user perspective and found that (1) data security (availability, confidentiality, integrity and non-repudiation of the system), (2) authentication & authorisation, (3) threats towards the violation of the available services (such as network and physical security) and (4) compliance with country regulations and laws were the main security challenges. The study examined current security issues of traditional ERP versus cloud computing technology. It was concluded that some of the issues of traditional ERP could be mitigated through cloud ERP, therefore someone else is dealing with a complex ERP architecture, enhanced datacentres, security and control environments and network and application security enhancements. Cloud ERP might have solved certain traditional ERP issues, but it has also opened the door for new issues, refer to section 2.2.6.3.

A major concern of SaaS-based ERP is that in the public cloud, a multitenant environment, a security breach might cause other cloud tenants to see confidential data. Sahin (2013) indicates that cloud tenants aren't separated in the hardware level, instead they are separated at the virtual level and that SaaS ERP providers should ensure that company data between different tenants are separated.

Research done in Europe by Rodrigues et al. (2016), studied the adoption of SaaS-based ERP amongst European SMEs and identified thirteen factors of adoption as listed in table 1.

	Adoption Factor	Explanation
1	Cost	Lower total cost of ownership (TCO).
2	Trust in solution partner	A third-party organisation acting as provider partner, responsible for implementation of the ERP, professional services, industry expertise and consulting.
3	Availability	Data centres ensuring high system availability and data availability.
4	Implementation	Shorter time frame to implement system
5	Security	Concerns of security, data confidentiality of and jurisdictional boundaries.
6	Flexibility	Ease and cost of implementing enhancements to adapt the ERP system to the changes in the business (growth).

7	Data integrity	Importance of having centralised and integrated information and that the data is accurate and consistent.
8	Integration of cloud platforms	Integration of cloud platforms translating into interoperability of various systems provided as a service.
9	Ubiquity	Creating a flexible and mobile workforce through an independent access possibility via any device over the internet.
10	Compatibility	To be able to plug-and-play other software systems and specific devices/tools and use them without worrying about background compatibility.
11	Usability	The cloud system should at least perform on the same level as existing system. Easy to use and learn.
12	Analytics	The use of integrated analytics tools to provide real-time reports and key performance indicators (KPIs) to assist with decision making and planning.
13	Best practice	System that works accordingly with standard practices so that users can be efficient and effective. Refocusing on the activities that are valuable to customers by focusing on product/service differentiation and following standardised system processes.

Table 1: Thirteen factors for adopting SaaS-based ERP (Rodrigues et al., 2016)

The researchers found that cost was rated as the top adoption factor, followed by trust in the solution partner, availability, implementation and security in order of importance. European SaaS application providers were asked the same question and indicated that customers would view cost, availability and security as the top three adoption factors, followed by usability and implementation. What was interesting in this study is that providers didn't view trust as an adoption factor and that customers didn't view security as important as provider experts predicted. In one of the case studies it surfaced that security is more of a concern for IT specialists than for the actual users.

1.3 Limitations of previous studies

When new technology such as the cloud is made available, users will either adopt or reject it. Section 2.2.5.1 will be discussing the diffusion of innovation (DOI) theory in more detail, but an important footnote is that potential adopters evaluate an innovation based on the five characteristics listed in table 2.

The research done by Faasen, Seymour and Schuler (2013) found that there are similarities between the satisfaction with the existing system and the DOI construct "relative advantage". These researchers have indicated that further research on the use of the DOI theory for SaaS-

based ERP adoption might improve understanding as there might be possible relationships with the other DOI constructs.

	Characteristic	Explanation
1	Relative advantage	Is the innovation better than anticipated?
2	Compatibility	Is the innovation in line with the values and culture of the organisation and does it address the requirements of the potential adopters?
3	Complexity	Is the innovation difficult to grasp and use?
4	Trialability	If the innovation be tested at no cost, can testing be done within the time frame?
5	Observability	Are the results of the innovation visible to others?

Table 2: The five perceived attributes of innovations (Rogers, 2003)

Sahin (2013) required additional data for evaluating cloud ERP security issues and suggested that additional interviews should be conducted, or a cloud ERP product should be tested so that that the results can be evaluated to contribute to the subject through a case study.

The literature still shows that there is a lack of empirical research about SaaS-based ERP adoption factors. Rodrigues et al. (2016) work was explorative in nature. A quantitative research approach is required to validate and refine the thirteen adoption factors listed in the previous section.

1.4 Relevance of the study

This research study is specifically targeted at academic researchers in the information system (IS) domain, SMEs operating in emerging market economies, larger corporates considering adopting the public cloud who can learn from SMEs, ERP practitioners who can gain knowledge and provide recommendations and lastly, ERP providers who will receive insight into cloud challenges and changes in business models.

The diffusion of innovation theory for SaaS-based ERP will give academic researchers an idea of where in the adoption curve South Africa is and how the adoption rate is affected by certain challenges. SME business owners and decision makers will gain insight in cloud computing, deployment of ERP via the cloud and the benefits and challenges thereof. SMEs doing business in other market economies will also benefit from this study. If SMEs can take the risk and possibly flourish to do business on SaaS-based ERP, surely this will open the door for larger enterprises to adopt the public cloud.

Last not but least, the cloud has introduced major changes for ERP practitioners and providers of both traditional and cloud accounting/ERP software as new technologies had to be adopted and skills had to be development through steep technical learning curves. Some of the ground challenges will be highlighted. In addition, the cloud didn't only mandate changes in how traditional ERP was programmatically written and deployed, it also had an impact on a provider's business models, such as roles and responsibilities.

1.5 Purpose statement

The purpose of this qualitative study is to explore the adoption of SaaS-based ERP by SMEs in an emerging economy when control of mission critical financial systems is placed in the hands of cloud providers.

1.6 Conclusion

Chapter one of the prologue provided a background of this research study at a high level in terms of previous studies addressing SaaS-based ERP adoption, the limitations of those studies, the relevance of this study and ends with a purpose statement.

Given the purpose of this research as described above, it's required to explore the adoption of SaaS-based ERP by SMEs in an emerging economy when control of mission critical business systems is placed in the hands of cloud providers. Hence, this study needs to determine if SaaS ERP is an affordable, viable long-term sound solution which can be adopted by the majority of SMEs in an emerging market economy when not only control, but also trust, are placed in the hands of another who is responsible for managing, protecting and supporting the heart of your business.

Previous studies indicated that additional research is required, therefore we will pursue this understanding in the chapters to come by adding new knowledge for local SMEs, SMEs operating in other markets, cloud providers and academic researchers.

Although this chapter has given us a base on which to ground this research, existing knowledge of cloud computing is shared in the next chapter, the literature review which will be focussing on SMEs in EMEs, traditional on-premise and hosted ERP systems, the emergence of cloud computing, ERP deployed over the public cloud, SaaS-based ERP adoption and the risks and challenges involved.

Chapter 2: Literature review

2.1 Background

“We are entering an era when we no longer need to load dedicated software on our computers, but will interface through browsers and servers. That will be a major platform change” (Ryan, 2012).

Application Service Providers (ASPs) who are hosting a company’s IT infrastructure (hardware and software) didn’t only open the door to the private cloud, but was also a major influencer to the delivery of the public cloud. Cloud providers are responsible for configuring, maintaining and upgrading the physical and virtual servers a company’s data is running on as well as all the software installed on them. These external companies also have a duty to protect a company’s data and to ensure that the system is up and running.

The focus of this chapter is on key concepts: smaller enterprises in emerging economies, traditional ERP systems being installed on-premise and hosted at third party providers, the emergence of cloud computing, ERP and accounting systems delivered over the public cloud (SaaS-based ERP), SaaS ERP adoption and the risks involved. The chapter concludes with one of the main SaaS-based ERP disadvantages identified: organisations are losing direct control of their systems by putting their data privacy, data security, system availability, system performance and trust in the hands of others.

2.2 Key Concepts

2.2.1 SMEs in an Emerging Market Economy

The focus group in this study is on SMEs operating in emerging markets.

A country can fall into one of three markets: Developed, Emerging or in the Frontier market (Emerging Money, 2012). An Emerging Market Economy (EME) is defined as an “economy with low to middle per capita income” (Heakel, 2017). The research study concentrates specifically on South Africa which currently falls in one of the top ten EMEs, as Figure 1 indicates.

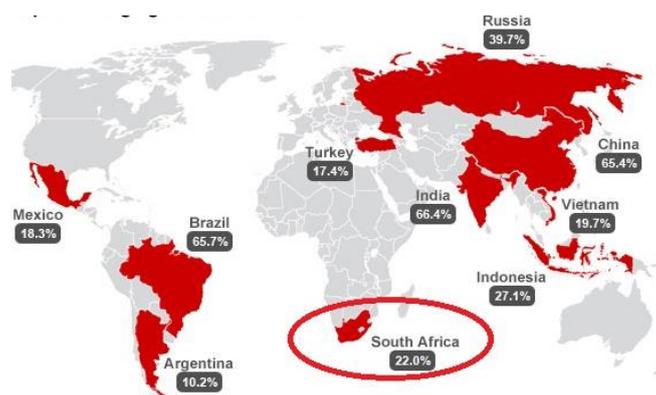


Figure 1: Top 10 Emerging Markets from 2012 to 2017 ((M-Brain (previously Global Intelligence Alliance), 2012)

Although rival ratings agencies Fitch and S&P downgraded the credit rating of South Africa's debt to junk status in 2017 (Cronje, 2018), the country's financial and banking systems are classified as one of the best in the world. In an independent rating by the inaugural Lafferty Bank Quality Ratings done in 2016, Capitec Bank was the top-ranked bank in the world (lol, 2016).

Another area where South Africa has excelled is its telecommunications infrastructure. The core of this thesis is cloud computing (section 2.2.3). To be able to connect to a computer system functioning in the cloud, section 2.2.3.1 explains that an internet connection is needed, hence a good reliable telecommunications infrastructure is a necessity. SouthAfrica.info (2012) reported that locally "there is an explosive growth in mobile telephony and broadband connectivity; with a network that's 99.9% digital and includes the latest in fixed-line, wireless and satellite communication, the country has the most developed telecoms network in Africa". Unfortunately, the high cost of internet data in South Africa remains a stumbling block for many SMEs. In March 2018 (lol, 2018) reported that the Independent Communications Authority of South Africa (Icasa) found that the price of data in South Africa is below average when compared to the Southern Africa Development Community (SADC). A survey conducted by research consultancy BDRC Continental agrees that South Africa's broadband cost do indeed rank below a number of countries in the emerging market economy (Lang, 2018). When Icasa compared data costs with the five BRICS nations, South Africa ranked the third most expensive (lol, 2018). However, when compared with the continent's six leading economies, BDRC Continental found that data in South Africa is indeed expensive and ranked South Africa's broadband data costs 97th out of 196 countries (Lang, 2018).

SMEs are a major economic force as they play a major role in creating a healthy economic environment contributing to a country's Gross Domestic Product (GDP) and job creation. According to Abor and Quartey (2010), 91% of formal business entities in South Africa are classified as SMEs, contributing between 52% and 57% to the GDP and provides about 61%

to employment. Survival challenges for these organisations include unstable labour markets and price sensitive consumers.

Tight budgets and fierce competition are major challenges. Operational costs must be minimised, and IT savings can contribute hugely. IT infrastructure, business software and costs related to the implementation, maintenance, support and licensing costs thereof can cost a company thousand, if not millions.

2.2.2 Traditional Enterprise Resource Planning (ERP) systems

Cloud-based ERP systems had its origin in traditional or conventional ERP systems. This section explains what ERP systems are, how they are implemented and how they are viewed by SMEs.

2.2.2.1 ERP Background

To operate efficiently a company should use a business system to facilitate the essential aspects of the business, such as the communication between participating parties, orchestrating of business processes, storing, viewing and editing essential data and providing insight into the business health.

Since the inception of ERP systems in the late 80's and early 90's, the term ERP is still unknown to many people. An ERP system can be defined as "integrated software packages, commonly known as business applications, designed to integrate and optimise the business processes and transactions in a firm, comprising different functional modules; accounting, procurement, sales, production, warehouse, etc., in order to improve firm performance" (Rodrigues et al., 2016). Company data is stored in a common central database. From this definition it's clear that the purpose of an ERP system is to support the core business processes of a company (Schubert and Adisa, 2011), and that information is integrated across the entire enterprise (both internally and externally) to flow seamlessly (Bhatia and Gupta, 2014).

Over the last 25 years information systems have matured a lot. Software houses started to build integrated business software solutions by combining isolated business applications into a unified offering. Various applications have been merged into what has become an integrated ERP system. These are usually grouped into "modules". Most ERP software providers have built the essential modules into their systems, including purchasing, stock control, sales, production planning, quality management, cost control, fixed assets accounting, human

resources, project management and finance as the core modules. In addition to maturing of ERP modules and functionality, traditional ERP systems have also matured in customisation and integration capabilities (Duan et al. 2012). ERP systems generally cater for a wide range of industries. Implementing IT application support into your company can proceed along two competing lines: 1) "Best of breed", which involves integration of diverse vendors' software, each of which has been selected to be the best in their field and 2) an integrated best practice approach, i.e. business best practices are implemented in the modules covering the business areas and are implemented into the company, using an integrated ERP package. Organisations are all unique. Preferably, the system should be adjusted to fit in with the organisation and not the other way around. Not all requirements can be met "out of the box", so customization is required to add or change the provided functionality and integration is required to enhance the provided functionality by integrating to other software.

In IT parlance, traditional ERP systems are referred to as on-premise ERP, or more specific: "traditional license on-premise" ERP (Kosasi et al. 2014). In this licensing model, IT costs aren't treated as an expense. Server hardware is classified as a fixed asset which is capitalised and depreciated over a period of time. The International Accounting Standard (IAS) classifies the ERP software and database purchased as an intangible asset provided that it meets the capitalization criteria under IAS 38 (Epstein and Jermakowicz, 2010).

Once the system has been implemented, it's there to stay at least for a couple of years. In a study done in 2011 by the Aberdeen group, it was found that of the organisations surveyed, 18% of them had an ERP system which was implemented less than two years ago, the bulk (41%) have an ERP system between two and seven years old, 34% between seven and fifteen years while only 7% had a system of fifteen years or older (Prouty, 2011).

2.2.2.2 Implementing traditional ERP

Two distinctions can be made within traditional ERP, On-Premise - and Hosted ERP (Duan et al. 2012).

In an on-premise ERP, the software is purchased via a license model and is installed onto end user computers and servers in-house. The SME is in control of the infrastructure and platform, handles all maintenance and absorbs the cost maintaining the server (Duan et al. 2012). Internal human resources or third parties are required to maintain the IT infrastructure and systems in place. Traditional ERP systems consequently require high capital cost investments with procuring their own infrastructure. An on-premise solution therefore puts the customer in control of their infrastructure and platform as they handle the maintenance needed on their server infrastructure and absorbs all the costs (Duan et al. 2012).

An alternative to on-premise is to have the licensed application hosted by a third party. In mid to late 1990's a new model emerged: the hosted solution (Beaman, 2004). A hosted solution can be defined as a technology service which is provided to an individual or group of organisations by a service provider that host the physical servers by running the service at another location through a direct network connection which may or may not run via the internet (Frapp, 2011). The third-party business providing the computer-based services is known as an Application Service Provider (ASP). This solution is in essence a private cloud model.

The hosted solution may be deployed in two different ways (Castellina, 2012):

- The application software and only the application software is installed on a physical server for the exclusive use of one customer, or
- In a virtual environment, dedicated to an organisation. The application is installed on a virtual server. One or more virtual servers are running on top of a physical server thereby sharing resources between multiple companies.

Except for the high capital costs when procuring a traditional ERP system, other main traditional ERP issues identified is the complexity of the system implementation, functionality, customisation and integration requirements (Al-Johani and Youssef, 2013). To optimise collaboration between systems as well as between systems and end users, integration has always been a major challenge. Trimi et al. (2005) identified change management, software licenses, consulting fees and in-house staff time as additional challenges to ERP projects.

2.2.2.3 SMEs view of traditional ERP

Due to the expensive nature of ERP systems, these systems can generally appeal to larger organisations (Spathis & Constantinides, 2004). SMEs neither have the budget for these capital expenses nor the human resources to maintain and support them.

An important aspect is that SMEs have relatively simple business processes, hence traditional ERP is an overkill. Most SMEs don't need to have a complex customisable ERP system in place and tend to rather make use of affordable, yet non-integrated solutions. In a study done by Gartner, about 44% of SMEs rely on a combination of disparate systems such as spreadsheet and basic accounting packages like QuickBooks to perform ERP processes and manage their business resulting in time-consuming and duplication of data entries (Joch, 2015).

To conclude, companies have become very reliant on ERP in managing their business processes. System challenges cripple many corporates who implemented ERP. In addition, due to their expense and complexity, ERPs have not generally been a feasible option for SMEs.

2.2.3 Cloud Computing

Cloud ERP evolved from traditional ERP. Cloud ERP is only one type of a cloud computing product delivered as a shared service to a pool of users via the internet.

2.2.3.1 Cloud Computing background

In today's information age, companies are expanding rapidly and work arrangements are more flexible. Having offices and branches in different locations isn't an uncommon business practice today. Globalisation created an environment for the establishment of multinational corporates. Certain companies are more flexible and can allow their employees to work from home or wherever they are. It's essential for these companies and employees to stay connected.

Since 1991 when the internet became publicly available (Bryant, 2011); the internet has played a major role on how people communicate, collaborate and conduct business. Bhatia and Gupta (2014) notes that it has a dramatic impact on how individuals access information as they are interconnected all over the world.

The term cloud computing has only featured in the late 2000s. In fact, Clarke (2010) states that the term was first used by Google's CEO in 2006. Cloud isn't really a new phenomenon as it actually incorporates elements of IT outsourcing (Schubert and Adisa, 2011). According to the National Institute of Standards and Technology (NIST), cloud computing is defined as "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" (Mell and Grance, 2009). These computing resources can be accessed in numerous ways, such as users connecting via the internet through a web browser or system-to-system web services. Ubiquitous access allows access from anywhere at any time.

Based on the definition above, NIST has identified five essential cloud characteristics in table 3.

Cloud characteristics:	
1	On-demand self-service: Without the intervention and assistance of a provider, a customer would be able to provision computing capabilities by themselves.
2	Broad network access: Access to the cloud is via the internet.
3	Resource pooling: Shared computing resources such as infrastructure, applications and services
4	Rapid elasticity: Services can easily be scaled up or down on-demand.
5	Measured service: Resources are controlled by the cloud provider through meters which are running in the background controlling the cloud services

Table 3: Cloud Characteristics (Mell and Grance, 2009)

Unlike the traditional on-premise computing model, cloud computing should be seen as the “delivery of computing as a service rather than a product” (Bhatia and Gupta, 2014). It seems like there is a slight disconnect in what true cloud really is as some software providers incorrectly advertise their products as a cloud offering. To be classified as a true cloud, McKinsey & Company listed three basic requirements which cloud offerings have to adhere to in table 4.

Requirements:	
1	The cloud’s infrastructure is highly abstracted from cloud users, for example the location of the data.
2	The application and infrastructure is rented, i.e. pay-per-use or subscription model.
3	Multi-tenancy

Table 4: Basic cloud requirements (Forrest, 2009)

Keeping these requirements in mind, major differences in cloud computing is that:

- Data can be located anywhere. To provide redundancy and in case of a failure or natural disasters, backups are usually kept in different locations. The physical location(s) might be unclear/unknown to users (Peng and Gala, 2014). Providers might also move data to different servers in other locations or even to another country for costing and technical reasons without informing their clients (Pearson, 2009). Users are usually not in control of where their data or any backups are being stored, however some providers such as Microsoft allows their customers to specify where their data can be stored. Cloud users would prefer their data to be stored in the same country due to regulatory requirements and jurisdictional boundaries. “Organisations can be restrained by local laws in countries where they operate which prevent certain info to be kept off-shore” (Schubert and Adisa, 2011).
- Change in the licensing model. There is no need for organisations to purchase computer hardware and software, instead they simply rent the software online

(Schubert and Adisa, 2011). A key requirement of true cloud is that users are billed on a pay-per-use basis (Forrest, 2009), or on a fixed subscription basis (Snider, 2013) which is usually revised annually. Forrest (2009) states that the subscription payment model is much more affordable to smaller companies as software expenditure is treated as normal operational expenses (OPEX) that typically require significantly lower upfront investments.

The first providers of cloud computing were Salesforce.com in 1999, followed by Amazon in 2002, Google in 2006 and Oracle in 2010 (Bhatia and Gupta, 2014). The following section will elaborate on the types of cloud services and how they are being deployed.

2.2.3.2 Cloud Delivery/Service Models

Computing resources are provided through delivery models, also known as cloud service models. This section will give a background of the various types of delivery models and then focus on how ERP is delivered via the cloud when shared by multiple SMEs.

According to NIST, there are three types of cloud services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) (Mell and Grance, 2009). Table 5 contains a summary of these models.

Delivery Model:		Description
1	IAAS Infrastructure as a Service	<p>IaaS refers to the provision of Infrastructure as a computing resource.</p> <p>Definition: “resources such as CPU cycles, memory, storage and network equipment is provided to a customer by an outsourcing provider. In this service model, it’s possible to share a server among multiple tenants. The service is typically billed on a utility computing basis” (Schubert and Adisa, 2011).</p> <p>Examples: Amazon’s Web Services and Secure Storage Service (S3), (Bhardwaj et al. 2010).</p> <p>Target market: Administrators. They are in control of the operating system and application software, but they not able to control the cloud infrastructure (Garcia, 2015, Duan et al. 2012).</p>
2	PAAS Platform as a Service	<p>PaaS is the provision of the platform infrastructure as a computing resource.</p> <p>Definition: “The provision of resources required to build applications and services to a customer by an outsourcing</p>

		<p>provider. Typical scenarios are application design, development, testing and deployment” (Schubert and Adisa, 2011).</p> <p>Examples: Google AppEngine, Salesforce.com’s force.com engine and Microsoft’s Azure platform services (Schubert and Adisa, 2011).</p> <p>Target market: Software developers. They have control over their deployed applications, but not the infrastructure components such as storage and processing (Garcia, 2015).</p>
3	SAAS Software as a Service	<p>SaaS is the provision of software applications as a computing resource.</p> <p>Definition: “The provision of an application which is hosted (off premise) by a provider as a service to customers who access it via the Internet” (Schubert and Adisa, 2011).</p> <p>Examples: Office 365, sharepoint online (Rodrigues et al. 2016), Google Apps, Salesforce (CRM), WebEx Web Office (Schubert and Adisa, 2011).</p> <p>Cloud ERP examples: NetSuite, Epicor, Acumatica, Ramco, Workday (Robb, 2016)</p> <p>Target market: End users or business (Duan et al. 2012). They only have control over the application which consists of a set of configuration options to personalise the application (Garcia, 2015).</p>

Table 5: Cloud delivery models

In figure 2, a traditional on-premise solution is compared with the three cloud service models.

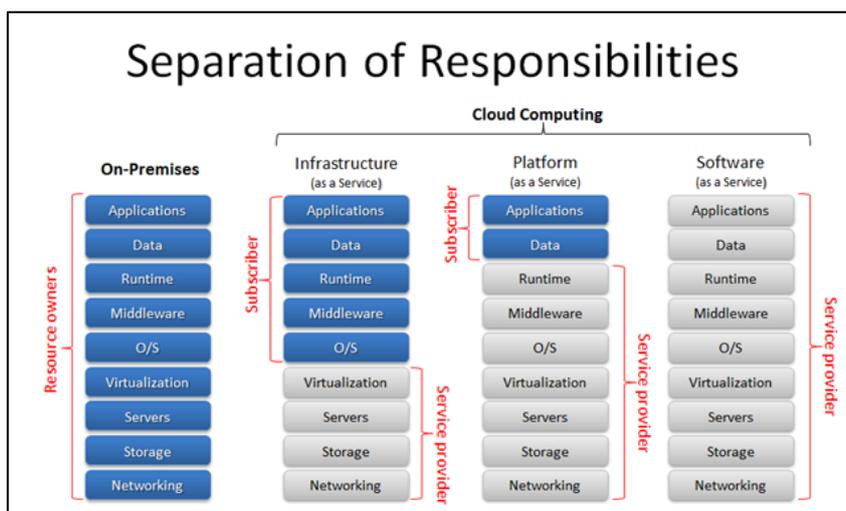


Figure 2: Separation of responsibilities (“YungChou”, 2010)

IaaS and PaaS require a combination of internal resources and outsourcing, while SaaS is fully managed by the cloud service provider(s). Because cloud ERP involves renting ERP

functionality and accessing it over the network, only SaaS is within the scope of this research study. The intricacies of the other models, although interesting, lie beyond our discussions.

SaaS and Multi-tenancy

A very important concept highlighted in the SaaS definition is multi-tenancy. Bhatia and Gupta (2014) listed multi-tenancy, SaaS and cloud computing as the three emerging technologies of the decade.

In contrast to ASP / the private cloud that requires single tenancy, discussed in section 2.2.2.2, SaaS is based on a multi-tenant model where the same application code is shared between SaaS-tenants, but each have their own private data spaces (Schubert and Adisa, 2011). The traditional computing model is based on a single-tenant model, where only one company or group of sister companies have access to the licensed software and their “private” database. However, Garcia (2015) noted that in a multi-tenancy model, a computer resource can be shared by one or more consumers (within the same organisation or from different organisations) and that these resources are in a form of storage, processing, memory and applications. According to Bhatia and Gupta (2014), “in Multi-tenancy software architecture, an organization’s data is served as a single instance by a hosted application that many customers use. This instance of an organization’s data is referred to as a tenant”. SaaS ERP clients are henceforth referred to as SaaS tenants.

Multi-tenancy is interesting from a data point of view and a major concern is that a SaaS tenant’s data might be shared with other parties. Multi-tenancy isolates data from others through isolation technology, virtualisation, clustering and segmentation (Garcia, 2015). Data privacy and data security will be discussed in section 2.2.6.

	SaaS Characteristic	Source
1	The software application is running in a cloud computing platform over the network - generally through web browser.	(Garcia, 2015)
2	Access through normal internet connection. Device: a computer, tablet or mobile device.	(Snider, 2013) (Mahara, 2013)
3	SaaS is based on the multitenant model allowing companies to share resources.	(Velte et al. 2010) (Forrest, 2009)
4	The software isn’t licensed or owned by the end user.	(Castellina, 2012)
5	Payments are usually made on a subscription basis.	(Snider, 2013)
6	SaaS is based on what you see is what you get, hence it doesn’t require much customisation or integration with other applications.	(Velte et al. 2010)

Table 6: SaaS service model main characteristics

Table 6 contains a summary of the SaaS service model's main characteristics from various sources.

The following section will explain the four ways in which cloud delivery models are deployed.

2.2.3.3 Cloud Deployment Models

Based on the previous section it can be concluded that cloud-based ERP systems can either be hosted or managed by (1) themselves; (2) the application provider, or (3) the cloud business platform hosting provider support. According to Schubert and Adisa (2011), the NIST definition for cloud computing describes the principle of exclusivity where the deployment model depends on the exclusiveness of the service model. If the cloud resides outside of the organisation and it's managed by a cloud service provider it's known as the external cloud and if the cloud resides within the organisation it's known as an internal cloud (Barnatt, 2010).

There are four cloud deployment models available. Schubert and Adisa (2011) defines the public, private, hybrid and community cloud in table 7.

Deployment models:		Definition
1	Public cloud	"The provision of a cloud computing environment that is based on a collection of virtual servers where multiple customers share physical hardware. In this outsourcing model the customer rents virtual servers on demand".
2	Private cloud	"The provision of a cloud computing environment that is based on a collection of physical servers that are exclusively run for one customer".
3	Hybrid cloud	"The provision of a cloud computing environment that comprises two or more clouds (public and/or private). In this outsourcing model the customer operates (on-premise) or rents (off premise) a base set of physical servers and adds virtual servers on demand".
4	Community cloud	"The provision of a cloud computing environment that is shared by several organizations and which is managed by either a participating organization or a third party".

Table 7: Cloud deployment models (Schubert and Adisa, 2011)

Due to the nature of SMEs, only the public cloud is within scope for this research as these organisations have limited internal resources, are less complex and in need of a cost-effective

ERP solution. The public cloud is based on the principle that it's available to everyone. Through multi-tenancy, anyone can pay a fee to join a cloud offering which is shared publicly.

A public cloud fulfils the requirements of a true cloud. According to Duan et al. (2012), the public cloud is labelled as SaaS in its true form as it addresses the three requirements of true cloud discussed earlier in section 2.2.3.1. It's important not to think that SaaS equals the cloud and the cloud equals SaaS (Gross and Veague, 2013). SaaS is only one element of cloud, cloud is more than that as can be seen from this section's discussions.

In the public deployment model, services are rented and shared by multiple tenants. No upfront capital is needed to acquire hardware and software licenses and because of this, Duan et al. (2012) indicates that capital expenses (CAPEX) are transferred to OPEX. Software licenses are replaced with pay-per-use or on a subscription basis, refer to section 2.2.3.1.

2.2.3.4 Cloud computing driving and hindering factors

To sell their products, cloud ERP providers need to persuade potential customer to rent the software. From various literature studies, six main reasons why SMEs should adopt cloud computing is summarised in table 8 below.

No	Factor	Comment	Source
1	Cost	Reduction in operational and capital cost.	(OECD, 2010) (Mattison and Raj, 2012)
2	Flexibility	Software that's user configurable.	(Mattison and Raj, 2012)
3	Scalability	Customers in the SaaS model can easily scale up or down depending on how much they require. Examples: <ul style="list-style-type: none"> • Only pay for capacity used • Number of users • Functionality used 	(Elragal and El Kommos, 2012) (Gross and Veague, 2013)
4	Improved system performance	Virtualization of data centre infrastructures.	(Koehler et al. 2010)
5	Mobility	Accessible by using any device and a simplistic design	(Mattison and Raj, 2012)
		High availability.	(Koehler et al. 2010)

		Workforce mobility and customer mobility.	(Prouty and Castellina, 2011)
6	Tools	The need for the right tools which plays a big part in the way work gets done in business.	(Fauschette, 2013)

Table 8: Cloud computing influencing factors

The biggest hindering factor why organisations wouldn't want to adopt cloud computing is loss of control and security. Elragal and El Kommos (2012) states that "unlike cloud, organisations have more control over in-house systems and hence they are considered as secure". This thesis wants to argue that this hindering factor is wrong. It is likely that that cloud providers are more focussed on security as they possess the necessary skills and knowledge not necessarily owed by the organisation itself.

2.2.3.5 Benefits and Concerns of Cloud Computing

Organisations who wish to pursue the cloud route need to be aware of the challenges and risks they might face. Table 9 contains a summary of cloud benefits and concerns.

	Benefits:	Concerns:
1	Decrease of capital cost: No high upfront cost: hardware and software license.	Permanent access. Internet down time.
2	Cost transparency: Pay-per-use or subscription models.	Control. Cloud provider's service going down.
3	Decrease of operational cost.	Location of data. Confidential information stored outside of the company.
4	Increased flexibility due to lower switching cost.	Integration of applications.
5	Guaranteed service level.	Vendor lock-in.

Table 9: Benefits and Concerns of Cloud Computing (Schubert and Adisa, 2011)

Section 2.2.4.3 will be discussing benefits and drawbacks specific to SaaS-based ERP in more detail.

2.2.4 SaaS-based ERP

While the previous section focussed on traditional ERP systems, cloud computing services, delivery models, deployment models and the benefits and concerns of cloud computing, this section will examine SaaS-based ERP software and service providers, SaaS-based ERP

benefits and challenges and lastly the impact of SaaS-based ERP on SMEs. Cloud ERP refers to ERP deployed through a private or hybrid model, while SaaS-based ERP on the other hand is ERP specifically running in a public deployment model which is hosted by the application service provider or the cloud business platform hosting provider.

2.2.4.1 SaaS-based ERP software and software providers

With on-premise ERP, everything is managed and controlled internally by the customer. Either their own internal IT department or a dedicated third party is responsible for maintaining the IT infrastructure supporting the business and ensuring that all software services are running and accessible. SaaS-based ERP can be defined as ERP “accessed through internet, where the application and data are under control of the service provider, with payment for the software services provided usually through subscriptions paid by user on a monthly basis” (Rodrigues et al. 2016).

While many types of enterprise applications have been moved into the cloud, ERP is one of the very last. Figure 3 illustrates a survey done in 2014 across eleven countries within Europe, Asia and North America revealed that Office suites and CRM were the most used applications migrated to the public cloud while ERP only accounted for ten percent (Sfondrini, Motta and You, 2015).

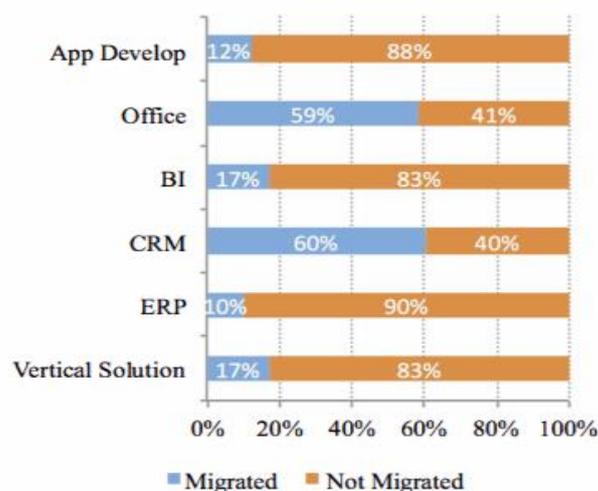


Figure 3: Application types deployed on Public Cloud (Sfondrini, Motta and You, 2015)

These figures are changing constantly as more SMEs are planning to move their ERP systems into the cloud as it's an affordable option for them. Bento et al. (2015) indicated that the growth of cloud-based ERP systems is expected to be greater than conventional ERP systems.

In a study done by Gartner, the top 5 ERP software providers in the late 2000s were SAP, followed by Oracle, Sage, Infor and Microsoft, with SAP and Oracle dominating the market by owning 40% of the market share in 2012 (Pang et al. 2013). Interesting enough, these providers were not the main pioneers of Cloud ERP. Instead, new small SaaS-based ERP systems were introduced rapidly by fast growing ERP vendors such as Workday, Workforce, Cornerstone OnDemand (CSOD) and NetSuite (Columbus, 2014). Traditional ERP software providers needed to tap back into the ERP market by either changing the core system to be able to run in the cloud or acquire one of these smaller providers' SaaS ERP software.

The roles of the traditional ERP vendor have changed significantly. Instead of only selling, implementing and supporting the ERP software, the service provider now also needs to act as a cloud service provider. In microeconomics and management, this shift is known as vertical integration (Schubert and Adisa, 2011). There is a whole change in the provider's business model impacting business models and SLAs, refer to section 2.2.7.3. Figure 4 shows that in 2012, 59% of SMEs were willing to consider on-premise ERP while 26% preferred SaaS-based ERP and the rest being hosted in the private cloud (Castellina, 2012).

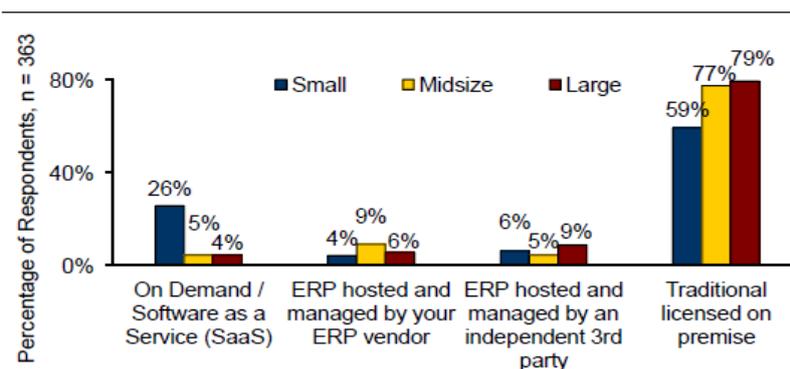


Figure 4: ERP deployments by business size in 2012 (Castellina, 2012)

2.2.4.2 SaaS-based ERP influencing and hindering factors

While section 2.2.3.4 looked at reasons why organisations should embrace or discard cloud computing, this section evaluates the top influencing and hindering factors of SaaS-based ERP. Members in a social network need to be encouraged with good reason why they should move their business systems into the cloud.

Table 10 explains the top five factors driving ERP to the cloud as identified in a study by Castellina (2012).

No	Ranking	%
1	Lower total cost of ownership	82
2	Low capital costs.	61
3	Easy and affordable upgrades.	56
4	Perceived ease of implementation.	44
5	Limited IT resources.	42
6	Seeking best fit solution. Vanilla ERP with modules that have already been integrated by the provider to design an integrated best-fit solution.	42

Table 10: SaaS-based ERP influencing factors (Castellina, 2012)

The top four hindering factors why organisations wouldn't want to adopt a SaaS-based ERP system are listed in table 11, with security and loss of control being the main reasons.

No	Ranking	%
1	Security concerns. Privacy (POPI Act) and data leaks.	39
2	In control of own upgrades. Multi-tenancy doesn't provide the luxury of choosing whether to upgrade or not.	22
3	Tailor design. Custom development is generally limited in public deployments.	21
4	Downtime risk. System and network infrastructure outages.	18

Table 11: SaaS-based ERP hindering factors (Castellina, 2012)

2.2.4.3 Benefits of SaaS-based ERP

Section 2.2.3.5 focused on cloud benefits and challenges. Table 12 is a summary of the main benefits specific to SaaS-based ERP collected from various literature sources.

No	Benefit	Reason	Source
1	Cost	Lower upfront & running cost	(Duan et al. 2012)
2	Focus on core competencies	Focus on the business and do what you're good at. Outsource IT rather than hire them in.	(Duan et al. 2012)
3	Support	Better IT support from external experts.	(Peng and Gala, 2014)
4	Technology	Access to more advanced computing / technology that you could not support yourself.	(Duan et al. 2012)

5	Reduced implementation time	Ease of deployment results in a system which is deployed faster.	(Fauschette, 2013)
6	Elasticity	Ability to use resources as needed.	(Duan et al. 2012)
7	Improved system availability, mobility and usability	System isn't restricted to specific locations, but access-anywhere nature. Cloud systems are more accessible than conventional systems.	(Duan et al. 2012)
8	Decentralisation	By not being restricted by specific locations, being accessible allows for decentralised system processing if integration isn't an option.	(Fauschette, 2013)
9	Performance	Faster response times and system speed won't be slowed down by increased data storage. Trade-off between network access and more powerful scalable back-ends.	(Peng and Gala, 2014)
10	Integration	Increase in cloud-based ERP products can simplify integration and eliminate data silos.	(Fauschette, 2013)
11	Upgrades	Faster updates across diverse geographical locations. Centralised upgrades supported by experts.	(Peng and Gala, 2014)
12	Flexibility / Agility	Flexible deployment providing for faster business decisions making and increased productivity.	(Fauschette, 2013)
13	Competitiveness	Access to the above SaaS-based ERP benefits allows new entrants or SMEs to play in the bigger leagues as they are being placed faster on the map.	Azarnik et al. 2012

Table 12: Main benefits of SaaS-based ERP

2.2.4.4 Challenges of SaaS-based ERP

The challenges of SaaS-based ERP that have been identified in previous literature sources are summarised below in table 13.

No	Challenge	Reason	Source
1	Control	Control of application and data in the hands of external providers.	(Enterprisetech, 2015)
2	Customization	Generally, public cloud solutions are highly configurable, but when one has a unique requirement which isn't a standard configuration, then one need one's own version, i.e. private cloud.	(Gross and Veague, 2013)

3	Integration	Traditionally, integration has many technical challenges at a price, this is even more difficult for cloud ERP as it has more distributed and moving parts.	(Peng and Gala, 2014)
4	Data security	Data in motion over company boundary, data at rest in shared data store, making vulnerability more common.	(Elragal and El Kommos, 2012)
		It's argued that that an in-house system is more secure as data is protected against hackers by being stored, locked and maintained on the company's premise.	(Elragal and El Kommos, 2012)
		Cloud providers that have a high staff turnover, are smaller in size and have weak data security in place are more likely to experience internal and external security breaches.	(Peng and Gala, 2014)
5	Performance	Reliability of the network.	(Woodie, 2015)
		Speed of the network, communication between client's computer and cloud-based service provider.	(Duan et al. 2012)
		Limitations on data transfer.	(Duan et al. 2012)
6	Availability	Access isn't local but over a network: Outage risks.	(Duan et al. 2012)
		Downtime of system not under your control. If internet or your ERP service provided is down – the service is down.	(Schubert and Adisa, 2011)
7	Regulatory compliance	Regulations were not designed by keeping cloud computing in mind, therefore SaaS-based ERP might find it difficult to always comply with international standards and regulations. Compliance generally requires additional data to be stored, accessed, retrieved and monitored which may require additional development if not available in the solution.	(Kim et al, 2009)
8	Governance	Governance is a discipline required when faced with a highly configurable solution. The stability can be compromised if design, testing and release processes aren't followed. SaaS ERP solutions usually have high end-user configurability and with that comes responsibility from both provider and customer.	(Mattison and Raj, 2012)

9	Transparency and data privacy	Shared data services causing data leaks in multi-tenancy environment.	(Garcia, 2015)
		Unclear location of data storage.	(Peng and Gala, 2014) (Garcia, 2015)
10	Vendor lock-in	Each provider does things in their own way. They use their own proprietary format to store data, making it difficult to either change to another provider or to integrate with other providers.	(Schubert and Adisa, 2011)
11	Trust	Trust is built over a long working relationship as well as responsiveness in difficulties.	(Gross and Veague, 2013)
		Providers have to build confidence through “consistent performance, verifiable results, service guarantees, transparency and contingency plans”.	

Table 13: Main challenges of SaaS-based ERP

From the literature findings above, it's clear that the benefits of using cloud outweigh its challenges. Although new challenges have surfaced in a cloud deployment model, this model has solved some of the traditional ERP challenges discussed previously.

2.2.4.5 Conclusion: SaaS-based ERP and SMEs

Previous research suggest that smaller companies are the first to utilise SaaS-based ERP (Al-Johani and Youssef, 2013, Sultan, 2011). SMEs have a limited cash flow, capital funds and human resources, which make SaaS ERP an ideal solution to invest in because it's affordable, the solution is agile in today's economic competitive environment.

According to Fauschette (2013), mid-size companies will follow suit, but these might rather opt for the private cloud or a hybrid cloud deployment giving them more control over their system, offering them higher levels of customisations and finally having more control over privacy and security issues. Last to follow are larger companies as they have already invested a lot of money in their existing systems and operate in more complex environments.

2.2.5 SaaS-based ERP adoption in an Emerging Economy

This section will be examining the adoption of SaaS-based ERP by SMEs in an emerging economy.

2.2.5.1 Diffusion of innovations theory

When new technologies or innovations are introduced to a population, it can either be accepted or rejected. Rogers designed a theory which is used as a theoretical framework for “Technology diffusion and adoption” (Sahin, 2006), and defines diffusion as “the process in which an innovation is communicated through certain channels over time among the members of a social system” (Rogers, 2003). The innovation is introduced to a small sample takes the risk of exploring and implementing it. If successful, it will be adopted by more entities over time and will ultimately have a positive impact on the adoption.

Rogers (2003) has also designed a 5-step Innovation-decision process whereby:

(1) Knowledge is generated

Section 2.2.3 gave a thorough background on cloud computing, its benefits and challenges and deployment models, while SaaS-based ERP was discussed in section 2.2.4.

(2) Persuasion of members

By having a better understanding of SaaS-based ERP, members will either have positive or negative feelings towards running their ERP system in the public cloud. In order for SMEs to adopt the software, cloud ERP providers need to persuade potential customer to rent the software. Section 2.2.3.4 and 2.2.4.2 discussed influencing and hindering factors of cloud computing and SaaS-based ERP.

(3) Decision to adopt or reject

By considering the SaaS-based ERP benefits, challenges, influencing and hindering factors, entities can choose to adopt the innovation or reject it. If a decision was made to adopt the innovation, the implementation stage follows.

(4) Implementation of the new technology

The innovation is put to practise. As soon as a new technology or innovation is released and adopted, users can be classified as either earlier adopters or later adopters.

Rogers (2003) identified five adoption categories, which fall in one of these two groups and defined adoption category as “the classifications of members of a social system on the basis of innovativeness”. Refer to figure 5.

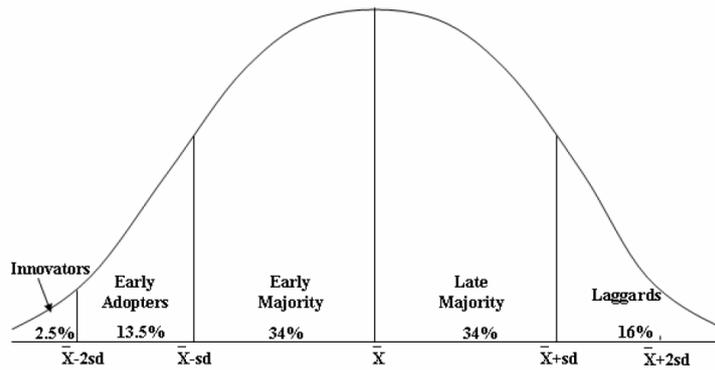


Figure 5: Adopter Categorisation on the Basis of Innovativeness (Rogers, 2003)

In a survey done by Gartner it was found that despite all the SaaS-based ERP challenges having an impact on the slow adoption rate in developed countries, there still is a major interest in SaaS-based ERP (Herstermann et al, 2010).

“Teething problems” might arise. According to Rogers (2003), reinvention can also happen at this stage as modifications to the innovation occur. SaaS Cloud computing has not fully matured yet. Cloud providers had to learn from mistakes they previously made as well as mistakes made by others. When Microsoft planned to release their Dynamics NAV 2013 and Dynamics GP 2013 to Windows Azure in the Microsoft elastic cloud, they didn’t want to make the same mistakes SAP did, who ended up pulling their SAP Business-By-Design cloud solution. Oracle’s combined Fusion applications also encountered a host of issues (Beal, 2012).

In the data analysis chapters, teething problems that South African SMEs experience, will be investigated.

(5) Confirmation

Confirmation occurs in practice and success leads to more adoption. Attitudes and support are crucial at this stage as it determines the choice to adopt or reject (Sahin, 2006). When a SME decides to adopt SaaS-based ERP, it will revise whether the decision was a good choice. If it doesn’t find satisfactory evidence, it will ultimately result in either rejection of the innovation or cause a delay in the adoption period until similar companies find evidence of proven value.

2.2.5.2 Adoption trends

An organisation’s annual revenue, region and industry will have a global impact on the adoption rate.

Adoption rate by annual revenue

The size of a company is a significant adoption factor. According to Mattison and Raj (2012), based on the size of annual revenue, the first movers who will adopt cloud ERP are smaller companies with a revenue below 750 million USD. Companies who are part of the second movers group have a revenue between 750 million USD and two billion USD. Larger enterprises with revenues above that fall in the later adopter group.

Adoption rate by region

A market economy segment is a significant factor. Mattison and Raj (2012) found that the first movers to adopt the cloud ERP were North America, Europe, Japan and Australia, which are developed market economies. Second movers would include countries like India, China and Brazil which are, like South Africa, emerging market economies. Territories part of the frontier economy market are mostly classified as later adopters.

Adoption rate by industry

Business industry and complexity is a significant factor. Another significant factor is industry sector. Mattison and Raj (2012) found that the first movers to adopt the cloud ERP are software companies, consulting services and light manufacturing. Second movers are typically retail companies who process high volume transactions and healthcare companies in possession of confidential patient data. Later adopters are industries with complex operations, such as manufacturing companies with custom development to fit their business.

Based on previous findings, South African SMEs will explore and possibly adopt SaaS-based ERP before mid-size and large enterprises would consider doing so. SaaS-based ERP would have been tested already by several SMEs in developed markets by the time it reaches early adopters in emerging markets. SaaS-based ERP is more likely to be adopted by SMEs that are less complex in nature.

Although cloud computing has been around for more than a decade with the emergence of cloud email and social networks such as Facebook, Instagram and LinkedIn; companies have only recently moved their core business systems into the cloud or are thinking about it. Even though EMEs are slower than the developed world in embracing technology, a couple of SMEs have locally already implemented SaaS-based ERP.

2.2.5.3 Planning for SaaS-based ERP adoption

Winston Churchill once said that “plans are of little importance, but planning is essential”. It’s advisable for companies who want to move their business software to the cloud, to consult an expert in performing a risk and readiness study. Accenture, a leading consulting firm, suggests incorporating governance and regulatory compliance, software integration, vendor lock-in, data security and privacy into a risk management study (Mattison and Raj, 2012). SMEs might not consider a risk and readiness study as important or might not have the time, money or human resources available to conduct such an assessment.

2.2.5.4 Conclusion

This research study is positioned as potentially fulfilling a number of steps in the innovation process. Specifically clearing up the necessary understanding of both the technology and its benefits and drawbacks, evaluating whether the technology can be confirmed as being successful (by asking adopters about their experience) and then encouraging further adoption by communicating this confirmation.

Even though the list of SaaS-based ERP challenges in section 2.2.4.4 is lengthy, some of those risks can be minimised by deploying different deployment models, such as a private or hybrid cloud giving enterprises more flexible options when it comes to control, customisation, integration and security. One of the main perceived challenges with SaaS-based ERP is loss of control which is covered in the next section.

2.2.6 SaaS ERP risk: Loss of control over security

In cloud ERP, the burden of data security, system availability and maintenance is transferred from the organisation to the cloud provider (Sahin, 2013). SaaS tenants can therefore focus on their core business while SaaS providers look after their systems. Giving up of control over security, data privacy, system uptime and support however is a major deciding factor for certain companies when they want to move their ERP/accounting applications over to the cloud as this involves putting their trust in others. Trust is therefore a critical factor in the decision to give up control.

Provider reputation can easily be harmed by high-profile media exposure such as the occurrence of data leaks. Quite a number of data breach horror stories have been reported

(Baker et al. 2011, p.6), including attacks on SaaS-based ERP. Both SaaS tenants and SaaS providers need to be proactive and protect the system from malicious attacks.

Data security and data privacy are significant concerns. It's therefore important that cloud providers have adequate protection measures in place. To that end, we will discuss the nature of the risks faced and the measures to be put in place.

2.2.6.1 Data security

“Data security relates to the practise of the protection of data against unauthorised access, disclosure and use” (Peng and Gala, 2014). Section 2.2.4.2 expressed that security concerns were perceived as the top hindering SaaS ERP adoption factor. In a LinkedIn survey in 2013, 54% of the respondents listed security as their top concern for migrating to the cloud (Nielsen, 2014).

Some argue that traditional systems with on-site data storage are more secure. According to Elragal and El Kommos (2012), by having control over one's data as it is stored onsite, it is protected against any malicious attacks. It's argued that with traditional ERP, multiple copies of important company data was stored on employee computers, laptops and storage devices risking disclosure to unauthorised people if the hardware is lost or stolen (Peng and Gala, 2014). Internal breaches are a probability as sensitive data might be downloaded from the system by internal staff and sold to competitors. Login credentials are shared without being aware of its risks. Yet, these scenarios can also happen in a cloud environment and organisations shouldn't take cloud security lightly. Linthicum (2015) reported of a cloud horror story where an enterprise customer data and credit card details were hacked by a file sharing provider. Failure in technology may also result in data breaches, however Peng and Gala (2014) pointed out that a review of the literature suggested that human resources are more prevalent than technology failure in causing security breaches.

Castellina (2012) evaluated the responses of a study done in 2009 which focussed on system downtime due to security and data-loss/data. Thirty-six organisations that used on-premise solutions and twenty-two organisations using cloud-based solutions were compared.

	Risk	Solution:	Number of incidents in twelve months
1	Downtime due to security	On-premise	11
		Cloud-based	6
2	Data loss/ Data Exposure	On-premise	11
		Cloud-based	6

Table 14: Number of security incidents (Castellina, 2012)

The findings summarised in table 14 indicate that on-site has significantly more incidents, making cloud-based systems more secure. Some of the reasons why SaaS security is considered better are that cloud providers are more thorough at responding to threats (e.g. keeping security patches up to date) and that they go through more vigorous security checks than in-house IT departments (Landy and Hakhinian, 2014).

2.2.6.2 Data privacy

It was previously pointed out that trust plays an important role when having limited control over a SaaS ERP system. SaaS providers need to guarantee the protection of keeping sensitive data confidential. Peng and Gala (2014) pointed out that poor data privacy is caused by poor security practices and defines data privacy as “the right of client companies to be sure that their confidential data kept by service providers is controlled and used properly, i.e. not to disclose to any unauthorised individuals/organisations”.

In a shared multi-tenant environment there are concerns that data leaks might occur across virtual barriers (Garcia, 2015). However, as cloud tools, processes and skills mature, these concerns should gradually fade away (Mattison and Raj, 2012). The public cloud needs to isolate SaaS tenants from each other. Isolation can be achieved by using private IP addresses which not only separates the infrastructure from the cloud services, but also partitions the cloud services from each other (Nolle, 2015). Amazon and Google use a more sophisticated public and private address mapping system. Amazon calls its approach "elastic IP addresses", while Google uses the project codename "Andromeda" to describe their approach.

In section 2.2.3.1, it was stated that one of the basic requirements of a cloud offering was that hardware management is highly abstracted from the cloud user and therefore the data can be physically located anywhere. Providers might move data to different servers, possibly to another geographic region or even to another country due to technical and costing reasons, without informing SaaS tenants (Pearson, 2009)- Should SaaS tenants be worried about the physical location of the data? Peng and Gala (2014) indicated that each country may apply data protection laws differently, increasing the possibility for data privacy to be jeopardized. These authors used the U.S Patriot Act as an example whereby no consent is required for the US government to access the data.

We currently live in the information/digital age. Information about oneself can be obtained quite easily as it is digitally available. It's the responsibility of each natural person and legal entity to protect a person's personal information. In South Africa, the Protection of Personal Information (POPI) Act, 2013, regulates the processing (e.g. collection, usage, storage) of personal

information which relates to an identifiable, living, natural or juristic person (South Africa Department of Justice and Constitutional Development, 2013). The purpose of the POPI act is “to ensure that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing another entity's personal information by holding them accountable should they abuse or compromise your personal information in any way” (WorkPool, 2016). The act therefore requires that SaaS tenants, SaaS providers and third parties should be responsible in protecting the personal information of other parties. The POPI Act 4 of 2013 also states that compliance demands us to identify what personal information is and to take reasonable measures in protecting the data (South Africa Department of Justice and Constitutional Development, 2013). Only the minimum required data should be captured and stored and data that's no longer required should be discarded. By being compliant, companies won't only avoid legal penalties and/or imprisonment, but will also minimise the amount and type of data that could be breached.

2.2.6.3 Security defences

To maintain the cloud services, cloud providers generally have better hardware and technology than SMEs which enable them to provide more efficient secure systems (Sahin, 2013).

Although cloud ERP has solved certain traditional ERP security issues, the cloud deployment model introduces a new landscape accompanied with new threats, such as browser-based threats, phishing attacks, botnets and ransomware. According to Zscaler (2013), traditional appliance-based security defences such as antivirus/DS signature updates, fixed perimeter controls, networks layer security, inbound security, end point control and operational security management aren't enough to protect business software in the cloud.

The traditional boundary has changed, new network and web security issues have been introduced by cloud ERP demanding a change in conventional security defences. Organisations need to be aware of every user, device and application accessing its corporate network (Zscaler, 2013). The new application landscape now combines components from both inside and outside of the corporate network which is accessed by a mixture of corporate devices, Bring-your-own-devices (BYODs) and external devices, over a variety of secure and insecure networks. We therefore can't rely solely on perimeter security, either physical or network security zones. Cloud requires a next generation security!

2.2.6.4 Security breaches

One of the main reasons why some companies are afraid to move to the cloud is because of data breaches.

Since 2008, the Verizon Data Breach Investigations Report (DBIR) has been released annually. The DBIR study isn't specifically SaaS-based ERP related, instead it examines information security incidents with the focus on security breaches, which is used as an indicative tool in this study. In 2016, 42 068 incidents were reported, which off 1 935 were real data breaches (Verizon, 2017). Only 4.6% of the incidents resulted in a data breach. The report defines an incident as "a security event that compromises the integrity, confidentiality or availability of an information asset", while a breach is defined as "an incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party" (Verizon, 2016). . The 2017 DBIR version found that the majority of security breaches were caused externally, followed by internal breaches (Verizon, 2017), illustrated in figure 6.

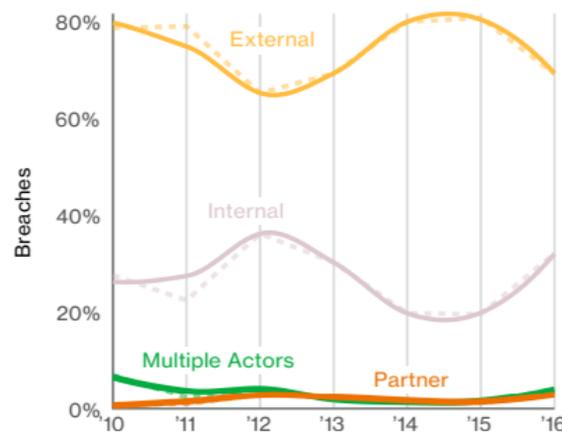


Figure 6: Threat actor categories over time. Source: (Verizon, 2017)

By comparing these results with the 2010 DBIR version, it's interesting to see that breaches caused by external actors have increased dramatically. In the 2010 DBIR report it was found that 70% of data breaches were caused externally, while 48% was internally and 11% caused by business partners (Baker et al. 2010).

Over the last couple of years there was a steep decline in server breaches, while there was an increase in breaches through user devices and people (Verizon, 2016). Financial gain in first place, followed by espionage, were the two main motives why external agents contributed to 93% of the breaches in the 2017 report (Verizon, 2017). Figure 7 illustrates that hacking, malware distribution and social engineering are the weapons of choice for attackers.

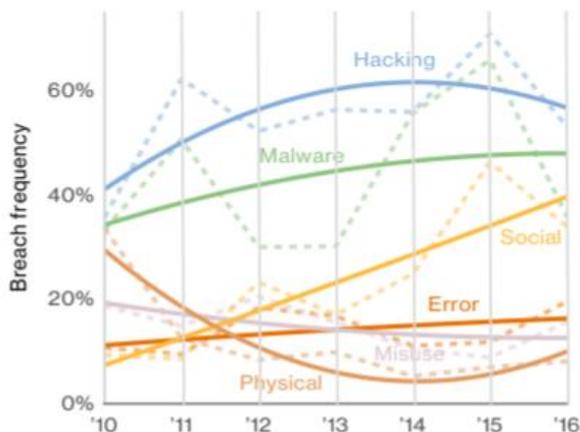


Figure 7: Percentage of breaches per threat category over time. Source: (Verizon, 2017)

It's clear the steep rate indicates that attackers are becoming more successful and well-organised. In table 15, the types of security breaches are grouped into three areas. Security breaches don't only risk the exposure and loss of sensitive data, it also disrupts business processes as a cloud downtime might probably be experienced as explained in section 2.2.7, resulting in loss of revenue and damaging both the SaaS tenant and SaaS provider's company image.

Area		Type of breach
1	Internal-based breaches	Incidents caused by staff
2	External-based breaches	Viruses or malicious software
		Hacking
		Worm
		Password sniffing
		Spoofing (IP, Web) attack
		Denial of service (DoS) attack
3	Platform-based breaches	Breaches caused by service providers
		Systems failure or data corruption

Table 15: Types of security breaches (Durowoju et al. 2011)

No industry, region or company is safe when it comes to a data breach. In 2016, it was found that financial organisations were mostly affected by breaches (24%), 15% involved healthcare, 12% the public sector, while retail and accommodation combined to account for 15% of the breaches (Verizon, 2017). It might take long before a company realises that a breach has occurred. Positive news is that detection times are getting better and that there is a slight decline in the number of breaches which stays open months or more, as the detection gap is closing little-by-little (Verizon, 2016). NetSuite, an American cloud computing company providing SaaS-based ERP, was hacked in 2012 over several months. McCarthy (2016)

reported that the hacker had changed demo account details which locked out a potential client and posted content of an offensive nature in a different company's test account costing the application provider \$189,000 to fix the accounts and restore its systems. SaaS-based ERP providers should be proactive and hire ethical hackers and third parties like auditors to review and test the security of their systems.

This section makes it clear that the ultimate goal of SaaS providers should be to detect incidents in a fast manner and to avoid data breaches when it comes to security.

2.2.6.5 Mitigation measures

In a multi-tenant environment, cloud providers need to ensure that mitigation measures are in place to protect all their customers in the shared environment from security breaches. There are six types of security that cloud providers must provide: physical, transmission, storage, access, data and application security (Erpcloudnews, 2011).

2.2.6.5.1 Physical security

According to Erpcloudnews (2011), when a physical security breach occurs, "somebody with malicious intent has physical access to the hardware where either your application is running or where your data is stored". Therefore, the same author states that a very important component of a software security and a business continuity plan is the physical surroundings of the software and the database.

Cloud tenants need to ensure that cloud providers have sufficient physical security measures in place. Data centres should have security guards patrolling the premises around the clock (Rudo, 2011a). Access to the building should be logged and controlled strictly. In addition, authentication technology such as fingerprint scans, ID badges and retina scans can be implemented to tighten access (Erpcloudnews, 2011). As multiple customers need to be protected in a multi-tenant public cloud environment, the physical security of these data centres is often much better compared to on-premise server rooms (Ledford, 2014).

2.2.6.5.2 Transmission security

Transmission security can be defined as "the process of securing data transmissions from being infiltrated, exploited and intercepted by an individual, application or device" (Techopedia, 2017b). Data in transit can easily be intercepted if not protected. A concern of

encrypting data before it's stored onto the cloud was found to be a challenge (Al-Johani and Youssef, 2013). Encryption limits the damage that can be done, but it does come at a cost to performance: if too many processing cycles are needed to encrypt and decrypt the data, system delays can be expected if more additional expensive hardware isn't added (Erpcloudnews, 2011). Encryption builds confidence in SaaS tenants which generates trust in cloud providers.

Secure communication should be used while data is in transit and at rest. Public key cryptography (RSA), Data Encryption Standard (DES), Triple DES and Secure Socket Layer (SSL) are four common encryption algorithms which can be implemented (Erpcloudnews, 2011). SSL is the most common used by cloud ERP providers and supported by majority of web browsers. Hyper Text Transfer Protocol Secure (HTTPS) is designed to provide secure web communications over insecure networks and is the protocol for Hyper Text Transfer Protocol (HTTP) communications over SSL or Transport Layer Security (TLS) (Jackson and Barth, 2008). While HTTPS allows for secure communication between the server and web browser there is a need for secure communication between SaaS ERP and other third-party applications, therefore integration also needs to be secure. Web services technology integrates heterogeneous islands to homogeneous component-based solutions (Stal, 2002).

SaaS tenants should ensure that SaaS providers have state of the art transmission security in place.

2.2.6.5.3 Storage security

In this context, storage security encompasses data access and data disposal. Corporate data can either be retrieved through the business logic (ERP system) or directly via the database.

Section 2.2.8.1 will explain that the cloud model requires cloud providers to provide database administration services. An important concern raised by Erpcloudnews (2011), is that cloud providers should prevent their employees from snooping around on client data by having procedures in place. It should also be forbidden to store customer data on employee devices. Background checks should be done on employees and confidentiality contracts should be enforced (Landy and Hakhinian, 2014). Google for example has sound policies and controls in place to protect the security of customer data, whereby data access is controlled and when it comes to data disposal, old data on hard disks containing customer data has to go through a data destruction process before it may leave Google's premises (Google Cloud Platform, n.d.).

SaaS tenants should ensure that SaaS providers have proper storage security procedures in place when their data is being accessed or disposed of.

2.2.6.5.4 Access security

Access security, also known as perimeter security, refers to the implementation of routers, firewalls and intrusion detection systems to tightly control digital access to networks from unauthorised users (*Perimeter security*, n.d.) By not implementing access security, unauthorised users (hackers) won't be blocked when sending queries to the cloud server, grabbing resources or stealing passwords.

SaaS tenants require a system that's up and running at all time. Cloud providers must build a redundant infrastructure with high availability withstanding malicious cyber-attacks. These attacks can be classified as either deception attacks or Denial-of-Service (DoS) attacks (Amin et al. 2009). According to Amin et al. (2009), by launching a DoS attack, the enemy's mission is to jam communication channels, cause harm to user devices, block devices from sending and receiving data, attack communication channels and flood the network traffic. Its sole purpose is to interrupt the online services either temporarily or permanently. DOS attacks have emerged since the early 1980s as simple one-on-one attacks while Distributed DoS (DDoS) attacks started in 1999 (Zargar et al. 2013). Sanmorino and Yazid (2013) describes that the purpose of DDoS attacks is "to spend server resources that become targets of attacks, namely by flooding victim computer with huge traffic, preventing legitimate users to access services on the server". Multiple Zomby or Botnet computers would send large amount of traffic at once and continuously to a target system (Zargar et al. 2013).

To control access, firewalls can be applied in hardware, software or as a combination of the two. Multi-tenant cloud applications are slightly different. Erpcloudnews (2011) states that cloud providers should have processes in place as the same application code and resources are accessed by multiple users so when one of the tenant's application has been compromised, the other tenants should be protected. SaaS tenants should ensure that SaaS providers have access security in place.

2.2.6.5.5 Application security

According to Erpcloudnews (2011), application security covers two areas: the way in which the application code is managed and how the application authenticates and manages users.

2.2.6.5.5.1 Application code

Software developers need access to an application's source code when writing new functionality or updating existing software functions and features. As a preventative measure, cloud ERP providers should include processes to manage any programming changes made to a production build system (Erpcloudnews, 2011). This process will ensure that no rogue code was inserted adversely putting the system at risk.

Software providers need to manage what can be integrated by whom. Resources of third-party providers could also negatively impose on the application security through configuration and integration flaws. It's suggested that a Security Development Lifecycle (SDL) process should be followed by the cloud provider which not only includes security review of the code, but also include a process for integration with third-party software and open source (Landy and Hakhinian, 2014).

2.2.6.5.5.2 Authenticate and manage users

SaaS-based ERP systems should be protected with strong authentication and authorisation features. Authentication ensures that only those with valid user credentials (username and password) obtain access, while authorization controls what services and data objects individual valid users may access (Erpcloudnews, 2011). In addition to establishing data rights, Preventative measures are listed in table 16 below.

Preventative measures	
1	Strong passwords, password change on specific time intervals and enforcing lock-out from excessive failures.
2	To stop hackers guessing usernames and passwords from remote locations. Access can be restricted to the system by IP address.
3	Apply two-factor authentication which is an additional layer of security. Achieved through the use of security tokens.
4	The use of key fob devices generating passwords that can only be used for a limited time.
5	Sending secondary, one-time passwords to a mobile phone via SMS.

Table 16: Authentication and authorisation preventative measures (Erpcloudnews, 2011)

Erpcloudnews (2011) made a statement that a cloud system's application security is more secure than a client-server system as the business logic resides at the server

instead of components installed on user machines. But, by not having proper application security policies, one is only as safe as can be as a shocking 63% of the confirmed data breaches reported in the 2016 Verizon DBIR was due to user credentials which involved weak and default passwords as well as stolen passwords obtained through hacking and malware (Verizon, 2016).

As an authorisation preventative measure, users should only be authorised to have access to certain functions and features. By applying Segregation of Duties (SoD) in the system, more than one person is required to finalise a task. SoD is defined as “an internal control designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any task” (Rouse, 2014).

Erpcloudnews (2011) added that user identity is also critical for creating an audit trail of activities for compliance activities. Audit trails will assist in determining who can see what data and verify any changes that have been made in the data.

2.2.6.5.5.3 System audit and certification

Another proactive measure a cloud provider can follow, is to test how secure their own software is and look into hiring ethical hacking services to find any issues by attacking the system. It's good software practice to hire external companies like auditors to commission periodic security assessments (Landy and Hakhinian, 2014). SaaS providers can gain stronger levels of trust if they push their systems through a certification process to ensure security controls are in place and that the system complies with regulations and conforms to ethical and auditing standards. Landy and Hakhinian (2014) noted that cloud providers should specify if they earned a certification, e.g. SOC2 Type 2 and that their software complies with the type of industry it can be used for, e.g. pharmaceutical. ISO 27001 and ISO 9001 are two more well-known standards to secure information assets.

Potential and existing SaaS tenants have the right to request review and testing reports from SaaS providers.

2.2.6.6 SaaS-tenants and security

Cloud users need to be informed about what providers are doing about security and use it as a decision criterion. It's vital to evaluate cloud providers prior to implementation of the system as the protection depends on the vendor's security. A pre-assessment and risk prevention of threats one might be exposed to should be done (Durowoju et al. 2011). A good check is to

verify if security professionals have done vulnerability scans on the SaaS-based ERP system and if the vulnerabilities were patched by the providers.

SaaS tenants should take responsibility and protect their core systems. To keep a system protected from internal and external threats, application security needs to be enforced. It's advisable to set up account policies in the system to define secure passwords. Ultimately it boils down to educating employees, the use of proper user and credential management and going the extra mile. By educating employees, people are informed of the risks cloud ERP systems are exposed to (Ledford, 2014). Employees shouldn't share their user credentials and properly password-protect their laptops and mobile devices. Users should also be educated on data loss prevention and not share critical information outside of their corporate network or public cloud infrastructure. Personal data should also be protected as per the POPI Act discussed previously.

Owners of SaaS-based ERP need to protect their systems by enforcing proper user and credential management. It's critical to implement authorisation controls because data has different degrees of sensitivity. As Google puts it, the "cloud platform provides the fundamental capabilities needed to build secure applications; however, it is your responsibility to enforce the appropriate movement and access to this data at the level of your application" (Google Cloud Platform, n.d.). Users should therefore be provided with the minimum required access by setting up of role-based security rights keeping SoD in mind. Their authorisation controls should also be tested properly to verify what they can see and do in the system and that nobody can delete or approve their own transactions.

2.2.6.7 Security conclusions

In this section it was questioned if the security of cloud-based systems in the hands of another is hands-down better than the security of on-premise and in-house ERP systems. In a multi-tenant environment, SaaS-based ERP providers have multiple clients to protect, thereby having a massive impact on their reputation should something go wrong. Ledford (2014) notes that this pressure makes SaaS providers invest more time and money into providing robust security measures and more resources to apply to security threats than SaaS tenants.

By investing time, money and effort in mitigation measures such as physical, transmission, storage, access, data and application security as well as discovering of breaches internally, hiring of ethical hackers and third party reviewers to do vulnerability tests and by getting certified through the application of data security standards, cloud providers can actively prevent security breaches and give their SaaS tenants peace of mind.

One can only ascertain that system security has improved over time, however the sections above revealed that hackers are becoming more successful and efficient in breaching system security and shifted their focus from the individual to organisations. Hackers would rather attack systems which have less security measures in place, in most cases these are in-house systems (Ledford, 2014). With enough planning and technology cloud systems can be more secure than on-premise systems (Linthicum, 2015). If the greatest risk to most software applications is people, then the answer to the question of how secure your cloud-based ERP system is, is that “it is as secure as the systems that protect it and the people who access it” (Ledford, 2014). It isn't only the responsibility of the cloud provider to protect the system and its infrastructure, system owners should evaluate their providers, educate their users and enforce strict password policies.

Data security and data privacy have been identified as two major security risks for adopting SaaS-based ERP. Extracts for existing literature studies have not only assisted in understanding these risks and their causes, it also highlighted qualities one should look for in a service provider to minimise the risk.

2.2.7 SaaS ERP risk: Loss of control over system availability

This section will investigate why system uptime and network quality were identified in section 2.2.4.4 as two of the potential challenges of cloud computing. In case an outage occurs, SaaS-tenants and cloud providers should be prepared by having business continuity plans in place. It is essential to read the small print in SLAs specifically on planned and unplanned downtime.

2.2.7.1 Cloud Uptime

Ideally cloud providers want to promise a software service that's available 24-hours a day. Truth is, cloud outages can occur at any time and both scheduled (planned) and unscheduled (unplanned) downtime might occur frequently.

IT infrastructures require hardware maintenance, upgrades and software updates which should be part of a planned or scheduled downtime periodically. The SLA between a cloud provider and SaaS-tenant will usually stipulate these types of downtimes. The interruption of services might have detrimental effects when downtime is scheduled during office hours. Cloud providers should try to run planned downtime afterhours and for as short as possible. By being proactive, cloud providers should also send out a maintenance notification in

advance of any planned downtime indicating the scheduled date and time (Ficco et al. 2015), as well as a reason and an indication of how long the system will be offline.

The performance of the cloud service must remain constant. This isn't however always achievable as predictable and unpredictable failure can cause downtime at any time. Srinivas et al. (2012) noted that technical snags and internal flaws might arise and that the occurrence of peak time breakdowns is quite high; therefore, load balancers, high end servers and data replicators must be installed for when needed. It's critical that cloud providers have risk mitigations plans in place. Marcus and Stern (2003) provided a list with reasons for cloud downtime:

- Failure Modes
- Hardware
- Environmental and Physical Failures
- Network Failures
- File and Print Server Failures
- Database System Failures
- Web and Application Server Failures
- DoS Attacks

Amazon is a well-known cloud business platform hosting provider. In 2015, Amazon web services suffered a major disruption when some of the internet's biggest sites and apps were sporadically unavailable for a couple of hours after more than twenty services on the AWS platform began to fail (Heath, 2015). This problem was caused by a database system failure. Two years later, the Amazon Simple Storage Service (S3) was down for several hours when one of the employees accidentally entered the wrong command and took more servers offline than intended (Del Rey, 2017). Service providers should ensure cloud technicians don't repeat these mistakes and be pro-active by preventing similar mistakes.

2.2.7.2 Network performance/quality

A practical description of network performance involves a "description of speed, capacity and distortion of transactions that are carried across the network" (Huston, 2003). Network quality is an important factor in system availability, system performance and usability. The experience of an on-premise ERP system on a local network is generally faster as external performance issues such as internet speed, delays and loss of packets are avoided. Response time expectations can lead to disappointment when moving the system to the cloud.

According to Huston (2003), to make a reasonable prediction on the performance of the transaction, one needs to know the characteristics of the network transaction as well as the profile of network performance between two network end points such as the latency, available bandwidth, loss and jitter rates and packet reorder probability.

The next section will explain how network quality involves the measurement of throughput, latency, data loss, data quality and availability.

2.2.7.2.1 Quality of Service (QoS) measurements

The goal of Quality of service (QoS) provisioning is to achieve a more predictable or guaranteed level of network performance, so that information which is carried by the network can be better delivered and that resources of the network is utilised optimally (Reddy et al. 2006).

Network-based QoS depends on five factors explained in table 17, adapted from Jain (2006). The table also lists QoS measures of each factor. Measures such as the “nines of availability” are often quoted without insight.

QoS	Comments
1	<p>Throughput</p> <p>Determines how much data gets through. It analyses the rate at which the packets travels through the network, i.e. the amount of data being sent/received per time unit.</p> <p>Preference: Maximum rate</p> <p>QoS measure:</p> <ul style="list-style-type: none"> • Speed of broadband services.
2	<p>Latency</p> <p>Determines the time it takes for the data to get through. Jain (2006) explains that delay refers the time which a packet takes to travel from its starting point to its destination and the number of drops in the connections.</p> <p>Low-latency networks is when small delays occur in the network connection, whereas high-latency networks are network connections which suffers from long delays (Techopedia, 2017a). SaaS ERP users will become frustrated if the latency is too high.</p> <p>QoS measure:</p> <ul style="list-style-type: none"> • Ping response time
3	<p>Data loss</p> <p>Determines how much data gets lost on the way. The rate at which a packet is lost by measuring the number of packets lost for every 100 of</p>

		<p>packets sent. Packet loss impacts applications performance. Long bursts of loss aren't common (Borella et al. 1998).</p> <p>Preference: Minimum as possible</p> <p>QoS measures: (Borella et al. 1998):</p> <ul style="list-style-type: none"> • Number of packets transmitted • Number of packets lost • Loss Rate
4	Data quality	<p>Determines if the data gets through in the right state. Packet Error Rate (PER) is the errors which are present in a packet due to corrupted bits caused by noise and interference (Balasubramanian, 2006).</p> <p>QoS measures: (Shin et al., 2007, Shafik et al. 2006)</p> <ul style="list-style-type: none"> • Packet Error Rate (PER) • Bit Error Rate (BER) • Signal to Noise Ratio (SNR) or Signal to Interference plus Noise Ratio (SINR)
5	Reliability	<p>Determines how reliable the connection is.</p> <p>The availability of a connection measured in service uptime or downtime.</p> <p>QoS measures:</p> <ul style="list-style-type: none"> • Ping to see if service is available • SaaS tenants: Use of companies assisting in monitoring cloud providers such as Cloud Harmony and Nasuni (Earls, 2015). • SaaS Providers measuring reliability as a percentage of uptime in a given period which is frequently the basis for SLAs (Erpcloudnews, 2010). <p>According to Marcus and Stern (2003), Uptime is measured by cloud providers by the “nines of availability” or number of nines, e.g. 99.99% availability.</p>

Table 17: Quality of Service factors

Unlike conventional ERP, SaaS ERP requires internet and if the internet fails, business can come to a standstill! Low latency, consistent data flow and guaranteed throughput (bandwidth) are three important requirements when moving business critical systems to the cloud (Your cloud success requires network strength, 2015).

2.2.7.2.2 Bandwidth in South Africa

Unlike many websites which are stable on slow broadband or even non-broadband connections, cloud-based applications require high bandwidth to be stable and usable (Srinivas et al. 2012). Customer bandwidth requirements are increasing year after year.

Nielsen's Law of Internet Bandwidth states that a high-end user's bandwidth grows by 50% per year (Nielsen, 1998).

MyBroadband has released their 2018 first quarter speed test statistics. It was found that South Africa's average download speed is 14.1Mbps, while the average upload speed is 9.4Mbps (MyBroadband, 2018). Depending on the telecommunications infrastructure, organisations have a couple of connectivity options to choose from. Digital Subscriber Line (DSL) is still a widely used bandwidth technology in South Africa. DSL was originally designed for voice but can also send data through twisted copper cables. In 2016, XDSL had the fastest ADSL download speed of 8.19Mbps, while MTN business had the best upload speed with 1.48Mbps (MyBroadband, 2016b). Currently in South Africa, one of the leading ISPs: VOX telecom provides the highest download speeds. 7 Mbps download and 1.19 Mbps upload speed can be achieved through their Asymmetric digital subscriber line (ADSL) service (MyBroadband, 2015). In the next category, 27.97 Mbps download and 2.81 Mbps upload speed can be achieved through VOX telecom's Very-high-bitrate Digital Subscriber Line (VDSL) service (MyBroadband, 2016a).

A faster alternative to DSL is Ultra-Fast Broadband (UFB), which is a high speed cable more commonly known as fibre which is specifically designed to transmit data at a high speed via fibre optic cables. BitCo provides the highest data transmission speed in South Africa with 214.5 Mbps download and 212.23 Mbps upload speeds (MyBroadband, 2016a). A third type of bandwidth technology is mobile and wireless communication technology. MTN is currently South Africa's leading mobile ISP promising 48.06 Mbps download and 14.2 Mbps upload speed (MyBroadband, 2016a).

By verifying the minimum bandwidth requirements, SaaS tenants need to ensure that a feasible bandwidth technology is selected thereby not jeopardising the cloud experience. It suggested that cloud users should make comparisons between the available bandwidth technologies by comparing speed, distance, consistency and availability (Community Editorial Team, 2014).

When cloud connection issues are experienced, it's advisable for SMEs to do a QoS assessment and evaluate not only their own ISP, but also the reliability of their cloud provider(s). In the event that issues like these might occur, a business continuity plan is vital.

2.2.7.3 Business continuity plans and Service level agreements

Cloud users should be prepared for when a cloud outage might occur, whether in the short term or long term. It essential to read the small print in SLAs specifically on downtime. By planning business continuity strategies, SaaS tenants and providers will have an action plan for when the unexpected occurs.

2.2.7.3.1 Business continuity plans

“Moving to the cloud simplifies planning but is does not alleviate it” (Erpclooudnews, 2012). Severe system outages may cause damage to a business if there are no business continuity plans in place for failover to additional infrastructure.

Erpclooudnews (2012) states that the trade-off to be made is the risk and the cost of the outage versus the cost of the continuity solution, example real-time failovers or onsite backups. A business continuity plan should plan for software slowdowns and more severe outages as per table 18 below.

Event	Scenario	Possible business continuity plan
Software slowdown	System speed is very slow	Inspect local network or log support issue with provider(s).
More severe outage	Planning for events when the SaaS service is out for hours, days, or weeks. Plan depends on business and application type	Wait it out/ “Be patient” plan
		<ul style="list-style-type: none"> - Manual system. - Recapture when online - Ensure provider has redundancy & disaster recovery plans
		Onsite data backup <ul style="list-style-type: none"> - Incase data is lost, get an onsite database copy if possible - Backup by using 3rd party hosting provider - Run reports from backup to mitigate risks
		Full redundancy <ul style="list-style-type: none"> - Fail over between different infrastructures.

		- Confirm if SaaS provider has a fully redundant architecture
Specific situations which may occur	<ul style="list-style-type: none"> - Hardware failure - Entire server goes down - Network firewall fails - Area-wide disaster - Rogue employees causing damage 	Service provider should in most cases have a backup plan for each situation in place to restore the service when offline.

Table 18: Business continuity plan per event type (Erpcloudnews, 2012)

2.2.7.3.2 Service level agreements (SLAs)

Contractual agreements between the SaaS provider and SaaS tenant are stipulated in the SLA. SaaS tenants pay provider for an agreed availability of resources. The SLA will usually stipulate the types of downtimes.

When it comes to cloud performance, two types of SLA's are used which may be from the same or different providers.

1. Cloud provider SLA

Traditional SLAs have been extended to include cloud resources. Erpcloudnews (2010) gave the following examples of Amazon and Azure. Amazon for example has a storage and a compute SLA. The S3 storage SLA promises a 99.9% uptime during a monthly billing cycle while the EC2 compute SLA includes a 99.95% availability during a service year. Windows Azure on the other hand is promising a 99.95% uptime in their computing connectivity SLA and a 99.9% availability of the database, storage and service SLA.

2. Cloud application agreements

A single provider can act as both the cloud hosting provider and application provider. If the SaaS ERP is hosted on another provider's infrastructure, then the cloud application SLA usually rides on top of cloud provider SLA (Erpcloudnews, 2010). Erpcloudnews (2010) gave two examples: NetSuite SaaS-based ERP is a provider with both a cloud provider and application provider SLA's promising a 99.5% uptime per month, while Acumatica's cloud application SLA promises a 99.5% uptime; their SLA covers the Microsoft Azure's SLA as their software is hosted by Microsoft.

SLA details

If the promised uptime percentage isn't achieved, providers may face financial penalties which are usually either in the form of credits or refunds (Erpcloudnews, 2010).

As discussed, the basis for SLAs is usually a measurement of percentage uptime, however the factors listed in table 19 might also play a role:

	Factors	Comments
1	Downtime calculation period	Downtime is measured differently by providers
2	Credit or refund	Credit on next month's account vs. refund to a prior payment.
3	Scheduled downtime	Scheduled downtime might be excluded from SLA calculations.
4	Latency and performance	A service with a slow response time can still be considered as up.
5	Notification	Unscheduled downtime occurring out of office hours.

Table 19: Downtime factors (Erpcloudnews, 2010)

SaaS-tenants needs to read the fine print carefully, especially if system uptime is considered to be a top adoption factor.

2.2.7.3 Cloud availability conclusions

System uptime and network quality were identified as SaaS-based ERP challenges. When cloud connection issues are experienced, it's advisable for SMEs to do a QoS assessment and evaluate not only their current bandwidth infrastructure and ISP, but also the reliability of their cloud provider(s). In the event that downtime issues might occur, a business continuity plan is vital. Contractual agreements between the SaaS provider and SaaS tenant are stipulated in the SLA. SaaS tenants pay provider for an agreed availability by of resources. The SLA will usually stipulate the types of downtimes.

Scheduled and unscheduled downtime and connectivity issues have been identified as two major system availability risks for adopting SaaS-based ERP. Extracts for existing literature studies have not only assisted in understanding these risks and their causes, it also highlighted qualities one should look for in a service provider to minimise the risk.

2.2.8 Provider support and trust

It was mentioned in section 1.2 that cloud providers didn't view support and trust as important SaaS-based ERP adoption factors. As indicated, previous research has however determined that trust was identified as one of the top factors from a customer's point of view.

2.2.8.1 Cloud provider support

In section 2.2.4.3, one of the main benefits of SaaS-based ERP is better IT support from external experts. Organisations who don't necessarily have internal IT resources, can rely on the resources of their cloud vendor for support (Castellina, 2012).

Providers have access to better skills. Peng and Gala (2014) indicated that IS consultants and ERP experts were expected to be knowledgeable on IT infrastructure and cloud ERP. Working more closely with ERP experts enable SMEs to be aware of the latest technology, system features and functions, changes in the industry as well as best practices.

In a study by Seethamraju (2014), one of the five determining factors in deciding to adopt SaaS-based ERP is that customers want a provider which will stand by their side and support them on the product throughout their journey. Outsourcing cloud application support has its challenges. In a SaaS-based ERP environment, organisations don't only rely on normal day-to-day ERP functionality support as in the past, they now also rely on support of the whole infrastructure. The business model of a software cloud provider has changed significantly, much broader end-to-end support is required on an application, network, device and security level. Cloud providers have more responsibilities as the need to provide database administration (DBA) services, act as hardware technicians, network technicians, security technicians, provide Operating System (OS) support and fulfil system administrator roles (Gross and Veague, 2013).

Another change in the cloud provider's business model is that providers need to support multiple clients around the globe and that support can't be restricted to normal office hours. What was observed in a research done by Seethamraju (2014), was that organisations realised the cost of switching cloud providers can be quite high, they would rather build a long-term relationship with the provider than the 'freedom to switch' between providers.

2.2.8.2 Cloud provider trust

Section 2.2.4.4 indicated that one of the major challenges affecting the SaaS-based ERP adoption, is to be able to trust providers with your systems (Awad, 2014, Faasen et al. 2013).

In the Burton group analysis, it was found that “building an IT organisation’s confidence in a solution requires a combination of consistent performance, verifiable results, service guarantees, transparency and plans for contingencies” (Reeves et al. 2009). Cloud performance, uptime, SLAs and business contingency plans have been addressed in this chapter.

While customers see trust as an important adoption factor, it was not seen as important by providers in developed markets (section 1.2). To encourage SaaS adoption, it’s imperative for providers to guarantee data security and connectivity uptime. The cloud relies on trust. Trust relies on healthy customer-supplier relationships (Romeo, 2014) and confidence (Awad, 2014).

SaaS tenants have little control over how their data is secured, managed and stored in a cloud environment. A break in security such as a password leak can easily break the trusting relationship. Dave Bell, chief information security officer at Blue Bell commented that “with SaaS, customers have to trust the provider and have no recourse other than to cover themselves with paper and work security necessities in their terms and conditions contracts” (Romeo, 2014).

One needs to trust a whole chain of providers, each of whom have access to your data, network, infrastructure, application and/or backups. Therefore, third parties also have an impact on the trust element. Cloud users need to ask important questions like who has access to their data and can individuals employed by the providers be trusted with the data at their disposal. “Cloud-sourcing involves the use of many services and many cloud-based services provide services to each other and thus cloud-based products may have to share your information with third parties if they are involved in processing or transferring of your information” (Srinivas et al. 2012). Companies aren’t always aware if their data is shared and with whom. This raises an important concern. Poaching (abuse) and theft of critical confidential data and intellectual property is categorised as an outsourcing opportunism risk (Azarnik et al. 2012).

Gupta and Misra (2016) found that people factors which incorporate cloud provider support and trust have a positive impact on the success of a cloud ERP implementation. Trust involves prompt turnaround time on support queries, providers employing quality staff, cloud performance, cloud connectivity uptime, data security and data privacy.

2.3 Conclusion

Doing business in a country with a volatile market is a challenge for organisations as it stands. In recent years, companies have become very reliant on ERP in managing their business processes. Traditional ERP isn't only very expensive for SMEs, these organisations have relatively simple business processes and therefore traditional ERP is a total overkill.

A major platform change has transpired the last decade. We no longer need to install software on our local computers. Cloud computing products are delivered as shared services to a pool of users via the internet which is rented on demand. An example of such a product is SaaS-based ERP which evolved from traditional ERP. While many types of enterprise applications have moved into the cloud, ERP is one of the very last. Previous research suggests that SMEs are the first to use SaaS-based ERP, mid-size companies will follow suit, but these might rather opt for the private cloud or a hybrid cloud deployment model. Last to follow are larger companies as they have already invested a lot of money in their existing systems and operate in more complex environments.

In a public cloud model, cloud providers are hosting the infrastructure, system and data, therefore making them responsible for configuring, maintaining and upgrading the physical and virtual servers as well as all the software installed on them. These external companies also have a duty to protect client data and to ensure that the system is up and running. By adopting SaaS-based ERP, organisations fear that they will lose control over the security and privacy of their data making their systems vulnerable to data breaches. In addition, loss of control over system performance and uptime might also cause rejection of the system.

The purpose of this qualitative research study is to explore the adoption of SaaS-based ERP by SMEs in an emerging economy like South Africa, when control of mission critical business systems is placed in the hands of cloud providers. Although this chapter has addressed this concern to an extent through a literature review, chapters four to eight will provide new knowledge of research findings specifically to SMEs in an EME.

The literature review questioned if the security of cloud-based systems is really hands-down better than the security of on-premise ERP systems. The traditional boundary has changed, cloud requires a next generation security. With a multi-tenant environment, SaaS-based ERP providers have multiple clients to protect, hence they need to invest money, time and specialised resources in building secure systems. One can only ascertain that system security has improved over time, however hackers are becoming more successful and efficient in breaching system security and have shifted their focus from the individual to organisations. Not only is the cloud provider responsible for protecting the system, its data and infrastructure,

system owners should evaluate their providers, educate their users and enforce strict password policies.

System uptime and network quality were also identified as SaaS-based ERP challenges. When cloud connection issues are experienced, it's advisable for SMEs to do a QoS assessment and evaluate not only their current bandwidth infrastructure and ISP, but also the reliability of their cloud provider(s). In the event that downtime issues might occur, a business continuity plan is vital. Contractual agreements between the SaaS provider and SaaS tenant are stipulated in the SLA. SaaS tenants pay provider for an agreed availability of resources. The SLA will usually stipulate the types of downtimes. Clients need to read the fine print carefully.

Better IT support from external experts was found to be one of the main benefits of SaaS-based ERP. The business model of a software cloud provider has changed significantly, much broader end-to-end support is required on an application, network, device and security level. Providers have access to better skills.

In a SaaS model, one needs to trust a whole chain of providers, each of whom have access to your data, network, infrastructure, application and/or backups. People factors which incorporate cloud provider support and trust have a positive impact on the success of a cloud ERP implementation.

Data security, data privacy, downtime and connectivity issues have been identified as major risks for adopting SaaS-based ERP. Extracts for existing literature studies have not only assisted in understanding these risks and their causes, it also highlighted qualities one should look for in service providers to minimise the risk.

This research study is positioned as potentially fulfilling several steps in the innovation process. Specifically clearing up the necessary understanding of both the technology and its benefits and drawbacks, evaluating whether the technology can be confirmed as being successful (by asking adopters about their experience) and then encouraging further adoption by communicating this confirmation.

Chapter 3: Research Design Methodology

Research is about creating new knowledge and can be defined as “a scientific and systematic search for pertinent information on a specific topic” (Kothari and Garg, 2014).

As a start, a research problem is identified. By making use of a research methodology, the problem is then systematically solved. A research methodology refers to strategies used by researchers to guide them in making choices with respect to sampling, data collection and analysis which ensures that their work can be critiqued, repeated and adapted (Lapan et al. 2012). This chapter covers the research design methodology and explains the research topic, the aim and objectives of the research study, the primary and secondary research questions to be answered as well as the research method used to answer these questions.

3.1 Research topic

Cost, flexibility, scalability, improved system performance, mobility and collaboration have been listed as driving factors why organisations should adopt cloud computing. Previous research shows that a great deal of organisations have already integrated at least some sort of SaaS solution into their business, such as email, office suites, document sharing and storage, time tracking, expense management, Customer Relationship Management (CRM) software and payroll. These are only a few examples of software that can be delivered as a service over the internet.

Traditional ERP systems, the backbone of a business, have usually been too expensive for smaller organisations to purchase, implement and operate on. Fortunately for technological enhancements, cloud computing makes it possible for companies to afford business software by renting ERP on a subscription, pay-as-you-go or usage basis. The business application as well as the server infrastructure is owned and maintained by cloud service provider(s). Due to cash flow, limited capital and the human resources the public cloud is an ideal option for SMEs.

Despite a myriad list of benefits of moving over to SaaS-based ERP, a few challenges have been identified. One of the main disadvantages of SaaS-based ERP is that an organisation is losing direct control of its system by putting their system uptime, data, security and trust in hands of others. By losing control, SaaS-tenants are faced by a few challenges.

3.2 Research aim and objectives

Thomas and Hodges (2010) defines a research aim as a “statement indicating the general aim or purpose of a research project” and a research objective as “specific statements indicating the key issues to be focused on in a research project”.

The aim of this research thesis is to determine the current usage of SaaS and examine if data security, data privacy, system availability, provider support and trust have a negative effect on the adoption of SaaS-based ERP by SMEs in an emerging market economy.

The objectives of this research thesis are:

- To establish into which adopter category SMEs in an emerging market currently falls, specifically with their adoption of SaaS solutions.
- To identify which three SaaS-based ERP adoption factors SMEs in emerging markets consider as the most important and to compare the results with developing markets.
- To determine how provider support affects the adoption of SaaS-based ERP by SMEs in an EME.
- To determine how cloud downtime and connectivity affect the adoption of SaaS-based ERP by SMEs in an EME.
- To verify if local providers and SMEs are doing their part in fighting against internal and external security breaches and to determine the effect of a major general security breach on the adoption of SaaS-based ERP.
- To investigate how the cloud has changed a software provider’s business model and what effect this change has on the formation of trusting relationships between providers and customers.
- To determine how SMEs in an EME feel about outsourcing control of their IT to cloud providers and if they are concerned that their data might be in the hands of external parties.

3.3 Research method

This research study followed an inductive approach. The data generation method determines if the approach is deductive or inductive. A data generation method is defined as “the means by which you produce empirical (field) data or evidence, which can either be quantitative or qualitative” (Oates, 2006). Qualitative data analysis is where non-numeric data like words are studied and broken down whereas quantitative data is numeric data. The main purpose of the inductive approach is “to allow research findings to emerge from the frequent, dominant, or

significant themes inherent in raw data, without the restraints imposed by structured methodologies” (Thomas, 2006).

Qualitative research allows for the exploration of human issues. Interviews were therefore deemed as appropriate as it tends to be more flexible. Data was collected through semi-structured interviews designed for three types of research participant groups: SMEs using conventional ERP, SMEs using SaaS-based ERP and SaaS-based ERP providers. From a customer perspective eight SMEs have been interviewed, while from a provider’s point of view two cloud application providers have been interviewed.

Once the data was collected, the interview recordings were transcribed so that the data could be analysed by interpreting and categorising it. Neuman (1997) points out that the categorisation is on the basis of themes, patterns, concepts or similar features. The research strategy used to conduct the qualitative data analysis used in this study is based on Thomas’ general inductive approach which is commonly used in social science research. The reason why this strategy was chosen is because it provides an uncomplicated approach for deriving findings in the context of focussed evaluation questions (Thomas, 2006).

Thomas (2006) explained that the purpose of the general inductive approach is to “(a) condense raw textual data into a brief, summary format; (b) establish clear links between the evaluation or research objectives and the summary findings derived from the raw data; and (c) develop a framework of the underlying structure of experiences or processes that are evident in the raw data”. To provide answers to the primary and secondary research questions listed in the section below, the ten transcribed semi-structured interviews were summarised, categorised and links between categories were identified which were subsequently incorporated in a theory.

3.4 Research questions

In the following section, the purpose statement discussed in chapter 1 is narrowed down to find answers to specific research questions.

The primary research question is:

How does giving up control of data security, data privacy, cloud availability and the dependency on internet connectivity affect the adoption of SaaS-based ERP for SMEs in an emerging economy?

To support the primary question, the following secondary questions will be asked:

- What are the actual benefits, challenges and risks experienced by South African SMEs operating on of SaaS-based ERP versus conventional ERP?
- Based on Roger's diffusion of innovation theory, into which adopter category would South African SMEs currently find themselves in their adoption of SaaS solutions?
- Which SaaS-based ERP adoption factors do SMEs and cloud application providers in emerging markets consider the most important and how do the results compare with studies done in developed markets?
- When comparing SMEs who have already adopted SaaS-based ERP with those running on conventional systems, how does provider support affect the adoption of SaaS-based ERP?
- What is the effect of cloud downtime on the adoption of SaaS-based ERP by SMEs in an emerging economy?
- What are the effects of last mile connectivity, broadband technology options and connection latency on the adoption of SaaS-based ERP in an emerging economy?
- Are cloud providers and SMEs in an EME doing their part in fighting against internal and external security breaches?
- How would a general major security breach effect the adoption of SaaS-based ERP?
- How has the cloud changed the software provider's business model and if so, how does it impact building trusting relationships with SaaS tenants?
- How do SMEs in an EME feel about outsourcing control of their IT to cloud application providers, cloud business platform hosting providers and other third parties and are they concerned that their data is in the hands of external parties?

3.5 Conclusion

This chapter concludes the prologue part by giving an overview of the research problem and explaining how the research methodology will solve the problem systematically.

To provide answers to the research questions, findings from the observations of raw data will be discussed in part two.

PART 2: Analysis

Chapter 4: SaaS-based ERP Adoption

4.1 Introduction

The first part, titled the prologue, gave a background of the major themes. In chapter four to eight of the analysis part, the research methodology is applied by analysing the data collected from the semi-structured interviews.

This chapter will start by giving background on the ten research participants. The main purposes of this chapter are: to begin with an understanding of the rationale behind decisions to adopt and to compare actual benefits and challenges of SaaS-based ERP with conventional ERP. Based on Roger's diffusion of innovation theory, it should also be possible to determine in which adopter category these South African SMEs should be classified. Finally, these ten participants need to identify the most important adoption factors for them which will then be compared with SMEs from a study done previously in a developed market economy.

4.2 Research participants in this study

The following section provides background on the eight SMEs and two cloud application providers.

4.2.1 SME Customers

Four of the eight SMEs in this study have already migrated to a SaaS-based ERP/accounting system as shown in figure 8, the other half is made up of either on-premise ERP, hosted ERP (private cloud) or a combination of the two (hybrid).

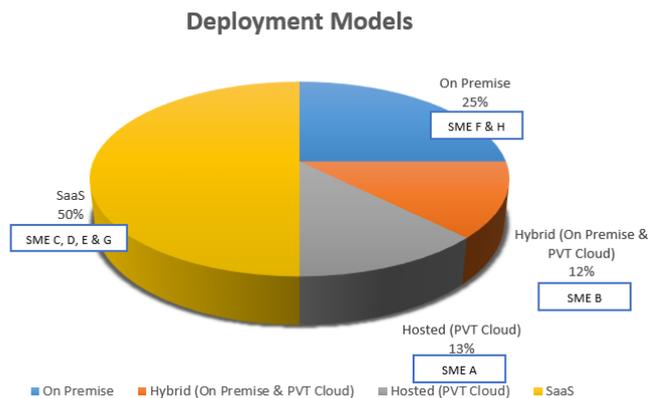


Figure 8: SMEs deployment model breakdown

These participants are operating across various industries as listed in table 20.

Deployment Model	Industry	Deployment Model	Industry
On-Premise	Retail	Public Cloud	Publishing
	Imports, Exports, Manufacturing		Catering
Hosted (Private cloud)	Plumbing		Telecommunications
Hybrid (On-Premise & Hosted)	Retail & distribution		IT

Table 20: Deployment model per Industry

Figure 9 is a map of where these SMEs are located. Six of them are based in the Cape Town metropolitan, while the other two are located in Johannesburg and in Polokwane respectively. SME “B1” which is in Polokwane, is part of a national franchise group. SME “B2” and “B3” are two franchises which are located franchises in the remote towns of Tzaneen and Burgersfort. The director of SME “B1” has shares in “B2” and “B3” and was therefore talking on their behalf. Six are, while two others.

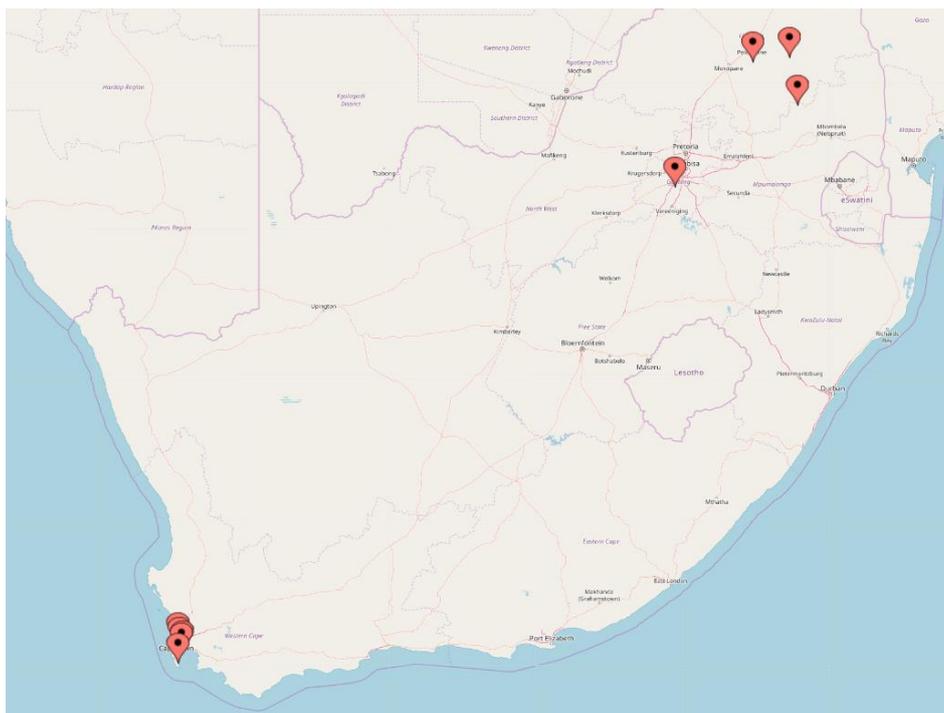


Figure 9: SME locations within South Africa (MapCustomizer, 2018)

Six out of the eight SMEs have branches in other parts of South Africa. The ERP/accounting systems used by these SMEs are popular both locally and globally.

4.2.2 Application providers

Two local application providers have been interviewed. Table 21 indicates that these are established software distribution partners and have their roots in on-premise ERP and hosted solutions. Although the public cloud model is fairly new to the providers, revenue streams have started to shift more towards the SaaS model.

	Provider 1	Provider 2
Product	International / Popular	International / New Entrant
Location	Pretoria, South Africa	Cape Town, South Africa
Established	Acquired in 2016 by a British company which was established in 1999.	2010
Number of employees	10 consultants 5 support personnel	20 consultants
Deployment models	All	All
SaaS experience	3 Years	9 Months

Number of SaaS Customers	12 – 15 customers	3 Customers
Number of SaaS Users	+ - 120 users	+ - 80 users

Table 21: Cloud application provider background

4.3 Adoption of SaaS and SaaS-based ERP by SMEs in emerging markets

To establish into which adopter category these SMEs will fall, specifically with their adoption of SaaS solutions, it is first required to examine and compare the actual benefits, challenges and risks that were experienced by the participants in terms of deployment models. Subsequently, the usage of cloud computing file sharing, file storage and other SaaS business applications by SMEs in the emerging market are evaluated.

4.3.1 Benefits, Challenges and risks of SaaS-based ERP vs. conventional ERP/accounting systems

The eight participants will be grouped into two groups: those who have already migrated to SaaS-based ERP and those who are still operating on on-premise and hosted ERP. Those on SaaS-based ERP will be referred to as the SaaS group while the latter as the Conventional group. Both groups were asked to identify their perceived and actual benefits, challenges and risks.

4.3.1.1 Comparison of perceived and actual ERP benefits

When an organisation needs to replace their ERP system, perceived benefits of an intended new system are gathered from sources such as word of mouth, marketing material and nowadays strong influences from social media.

More often than not, those perceived benefits ought to be realised once the new software is in place and hopefully more benefits should surface... This section compares the perceived and actual benefits of ERP/accounting systems experienced between the two groups.

Conventional Group

Research participants in this group listed process improvements, integration, performance, user friendliness, personalisation and visibility as key expectations. Instability of the

underlying infrastructure experienced at all four SMEs in this group had a negative effect on achieving the expected benefits and can lead to huge dissatisfaction.

SaaS Group

While only one SME, SME “D”, have used an on-premise financial system prior to using SaaS-based ERP, the other three SMEs operated mainly on spreadsheets. Coming from a manual business tool based to an integrated solution provides many benefits.

Expected and actual benefits of participants in this group included ubiquitous access (especially for distributed operations), quick turnaround time, better infrastructure, support, business intelligence and shared access with business partners. Benefits experienced but not originally expected are faster data capturing, less duplication of work, better reporting, integration and automation. There was however some disappointment with software updates changing the cloud solution’s look and feel.

A feeling of passion and excitement the SaaS group filled the room more, when the research participants were questioned on system benefits. SMEs in the conventional group aren’t only lagging behind on legacy technology but could also be frustrated with a hodgepodge of loosely integrated components.

Whatever the reason might be, this section suggests that if a system doesn’t meet your expectations and/or lacks functionality, when support is of an inferior standard or when frustration is caused by poor system performance, system connectivity and excessive downtime causes, then negativity will override any positive experience.

4.3.1.2 Comparisons of ERP challenges and risks

The challenges of implementing a new system are real. Almost always the marketing view of ample functionality, or even worse minimal configuration, turns out to be a complex effort of customisation to make the system work differently because of missing functionality, or severely challenging automation and integration. In every project there is a relative movement when the team must stop, look at itself in the eye and answer the question: “This is way more difficult than we thought, do we still want to do proceed with it?” The answer to that question and the executive support of that answer are what determines the success or failure of the project.

Costs, functionality, software licensing and change management were ERP challenges identified in the literature review. These challenges were also raised by both groups in this study.

Conventional Group

Section 2.2.2.2 of the literature review mentions that traditional ERP is either located on-premise or hosted and that the software can be installed on physical or virtual servers. Participants in this group have underestimated hardware specifications, virtual servers are easier to scale up. SME “A” had to incur additional costs by switching from an on-premise to a hosted environment. The new physical server, as per provider specifications, was not performing as expected.

Many international systems aren’t designed for the lower local bandwidth situation. Two participants in this group experienced slow and unstable internet connections and had to upgrade their ADSL lines. Even though SME “A” upgraded to a 1:1 fibre connection, they still to this day experience network inconsistencies. There are network dips and slow connection speed at certain times.

The business structures of some of the organisations are quite complex. SME “B1” is a privately-owned retail franchise in Polokwane established in 2012. Their franchisor was established in 1980. There are 23 franchisees nationwide, some owned by head office and others owned privately. Franchise “B1” is running on an on-premise ERP system. However, the other two franchises mentioned previously (“B2” and “B3”) are running on the same ERP application, but their system, like the rest of the franchise, is hosted at a data centre. SME “B1” spent big amounts on switching their system between on-premise and hosted solutions. Originally their ERP system was on-premise, then their franchisor requested that all the franchisees had to migrate to a central system located at head office. From there, the system moved to a third-party data centre where it was hosted in Johannesburg. Since being hosted, franchise “B1” started to experience constant system and connection issues as explained in the sections later. Due to these challenges their business suffered severely and relationships with the franchisor started to sour. To get their business back on track, a reimplementation back to on-premise was done. The root of the problem lies in Polokwane’s poor telecommunications infrastructure as explained in chapter six. To their disappointment, once their software licenses expire, franchise “B1” is forced to revert to the franchisor’s private cloud.

Many packaged systems have a data design that doesn’t fit local conditions or requirements. It’s often very difficult to change the underlying data without affecting other system

functionality and upgradability. SME “A” faced challenges of system functionality not fitting the business to a system that isn’t fully integrated causing duplication of work, room for error and inaccurate costing. Both SME “B” and “F” complained about duplication of work. SME “B” is unable to send out automated external documents via email to their customers and management accounts have to be created manually every month. Limited stock functionality was reported by both SME “F” and “H”. The former SME had to design an in-house stock system, while the latter manage their stock on spreadsheets. Two of the SMEs (“F” and “H”) have outgrown their system as the high volume of business transactions and number of users is putting strain on it. The issue isn’t the server, it’s the application. These organisations are pushing the system to its limits. An unstable database is one of the biggest challenges and risks identified by SME “F” and “H” causing database corruption issues and long downtime periods, refer to chapter six.

Additional challenges identified by these SMEs are lack of reporting capabilities and barcode scanning functionality, drill down limitations, costly user licensing models, poor data integrity and poor support levels.

In summary, on-premise and hosted ERP systems have been around for many years and they are applications of well-known brands! Two of the four SMEs in the Conventional group have outgrown their existing system; the same two sometimes suffer from up to three days of downtime because the system’s foundation is built on a poor database design. Three of the four SMEs in the Conventional group complained about limited functionality affecting the usability of the system. Ironically, chapter four will later indicate that usability was found to be the SaaS group’s top adoption factor and it didn’t even make the top three of the Conventional Group’s list.

SaaS Group

Moving critical business functionality off premise requires a very good stable telecommunications infrastructure to meet performance and reliability needs. The application also needs to be designed with cloud in mind, for example remote access, volumes of data and data integrity. One needs to test the application and chosen deployment infrastructure well with regards to performance, throughput, reliability and scalability limits. Performance can have serious impacts on business processes, e.g. timeous processing of financial transactions.

Two research participants in this group are experiencing slow internet speed issues at times, while downtime used to be a challenge for one of the two. Downtime had a direct impact on

SME “D’s” debtor book as customer invoices were not going out in time, delaying customer receipt collection. Refer to chapter six.

Cost is another challenge. SME “C” share user login credentials as cloud costs mount quickly with number of users and transactions. Data security is discussed in chapter seven. Trusting the integrity of the data and additional manual work involved are two more challenges faced by this participant. SME “C’s” customer statements aren’t accurate, this is caused by wrong receipt and invoice allocations (most probably user inflicted). Their automated banking isn’t working because of integration issues with their bank. As a workaround, bank statements have to be imported manually which leaves room for error as one needs to modify the import file. Certain functions aren’t automated as expected.

Some functionality may be expected but isn’t provided, for example compliance reporting and best practice processes. Best practice is one of the adoption factors mentioned in section 1.2. The SaaS-based ERP system SME “D” uses, allows one to go back and edit final posted transactions such as sales invoices, this is frowned upon in accounting and auditing circles. SME “E”, a telecommunications company needs to look at ways to be able to manage their open job cards better. Sometimes functionality may be available in another software package, for example CRM, but this involves a further integration effort.

In the literature review, Trimi et al. (2005) listed change management as a challenge. This was also indicated as a significant factor for SME “G”. People tend to like the current system, they are used to it. Unless managed properly, it will always be a challenge, regardless of the type of system. You need to take them along the journey. This challenge can be mitigated by adding change management approach as part of the ERP project.

Switching over to a new ERP or financial system will always bring upon new challenges, whether running it on-premise, or in the private or public cloud. Even though South Africa’s telecommunications infrastructure, especially in remote towns, seems to be one of the biggest cloud obstacles, one change is however inevitable and that’s change!

Cloud Application Providers

Cloud application providers were asked what their customer’s main challenges are. Provider 1 verified that last mile connectivity, broadband technology options and connection latency are some of the major non-functional related challenges. These three challenges were not listed as cloud or SaaS-based ERP hindering factors in the literature review, however section 2.2.4.4 confirmed that overall system performance is a challenge. One of their restrictions is that their cloud application may only be installed at certified data centres.

According to application provider 2, the biggest challenge they experience is getting around high database licensing costs. The infrastructure their system runs on is only economically feasible when a customer requires a high volume of end-user licenses. It's therefore very expensive for a ten-user system. Provider 2 is however negotiating better pricing options with their cloud hosting provider.

When asked what the reasons are usually why some potential SaaS-tenants wouldn't want to run their ERP/accounting system in the cloud, provider 1 listed last mile connectivity, connection speed, offline capability, third party integrations, recurring payments and the perception that it's expensive as the main reasons. Provider 2 only commented that "we are dealing with guys who are growing fast... youngsters!" The customers they focus on are mainly new entrants, owned by a younger generation who can embrace new technology faster and adapt to trends.

Step three of the diffusion of innovation theory in section 2.2.5 was the decision to adopt or reject new technology. By being aware of benefits and challenges the decision to adopt SaaS-based ERP can be made easier.

4.3.2 Roger's diffusion of innovation theory: Adopter category of local SMEs

Based on Roger's diffusion of innovation theory, it's required to determine in which adopter category these SMEs would currently find themselves in their adoption of SaaS solutions. This section compares the extent of ERP, cloud file sharing and storage as well as other SaaS business applications being used by the participants.

4.3.2.1 The extent of ERP/Accounting systems being used

In the following section, SMEs in both groups are compared in terms of organisation age, access to IT human resources, previous systems used, duration of system usage and the number of system users.

SaaS Group

SME "C", "D", "E" and "G" are four SMEs that run their business on a SaaS-based ERP/accounting application. Figure 10 indicates that these organisations are quite young of age, the average age is approximately 9 years.



Figure 10: Number of years trading (SaaS)

Even though these organisations are classified as SMEs, three of the four operate from more than one location. None of these SMEs have an internal IT department, although they are dependent on themselves, they might rely on an outside contact person or a dedicated third party to assist when there is a need for technical assistance. SMEs don't usually have a dedicated internal IT team as noted in the literature chapter, section 2.2.8.1.

Interestingly enough, the majority of these participants didn't migrate from the conventional ERP route, they converted directly from office productivity tools such as spreadsheets. Figure 11 shows that only SME "D" previously used an on-premise accounting package. The SaaS group have used their previous systems for an average of five to six years. As the literature indicated, the bulk of organisations keep their systems for two to seven years and SMEs have limited funds available, hence making use of spreadsheets is a cheaper alternative.

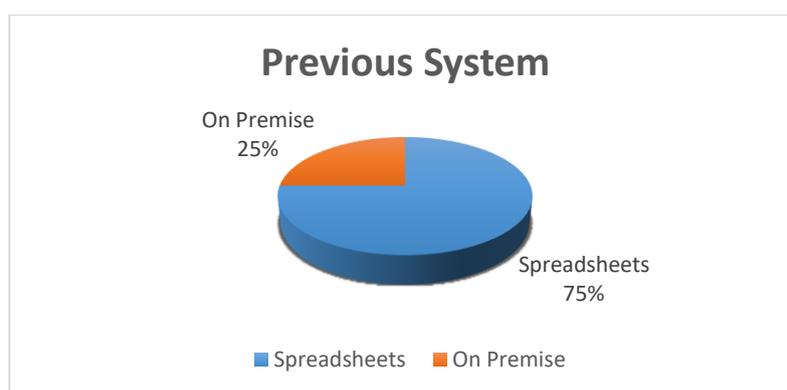


Figure 11: Previous system used: (SaaS)

These four SaaS-tenants have been running on their SaaS-based ERP/accounting package between one to three years. The main reasons for replacing their previous systems were:

- Business growth
- Accessibility, being able to log in from anywhere
- Empowering branches through decentralised processing

- Ease of use
- Better stock control
- Integrated systems
- Automated business processes
- Improved system functionality

Although the head count in these organisations ranged between 4 and 44 employees, figure 12 shows that only 17% of the employees are classified as system users. Only one of the four SMEs in this group use the stock and complete distribution modules. SME “G” admitted that they aren’t utilising the system to its fullest extent.

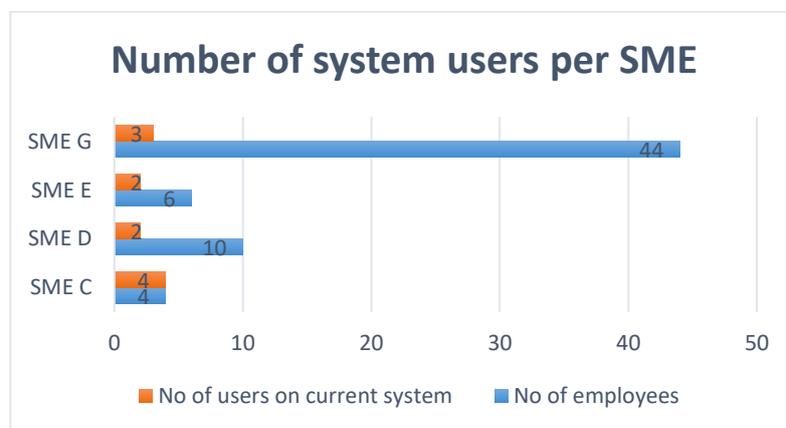


Figure 12: Number of system users (SaaS)

It was found that none of these SMEs wanted to replace their current cloud-based ERP/accounting system. SME “E” did want to integrate with a CRM system and is looking at SaaS options. Research participants were asked to rate the functionality of their SaaS-based ERP/accounting system. Figure 13 indicates an outstanding score of 85%.



Figure 13: Functionality rating (SaaS)

Seeing that most of the SMEs in the SaaS Group didn't convert from conventional ERP, they are probably immature in their functionality needs and it seems they are quite happy with what's provided. They have not had sight of the more extensive functionality available in on-premise ERP solutions and they have not yet come up against the typical limitations of SaaS-based business packages. The literature review mentions that cloud-based solutions provide very standard functionality and any customisation or integration effort very quickly requires a move to an on-premise solution, or a private or hybrid deployment model.

Conventional Group

The Conventional Group would be able to make better comparisons between on-premise and cloud-based ERP as most have an ERP background. Two of the four SMEs in this group are operating on on-premise ERP systems (SME "F" and "H"), while SME "A" is hosted at a data centre and although SME "B1" is on-premise, the rest of the franchise group is running in the private cloud. Figure 14 indicates that these organisations have a similar average age to the SaaS group of 9 years.



Figure 14: Number of years trading (Conventional)

Even though the organisations in this group are classified as SMEs, three of the four operate in more than one location. Most of these SMEs have a range of in-house IT capabilities with technological problem-solving expertise. Two SMEs in this group (SME "F" and "B") have an internal IT department. There is an IT helpdesk at franchise "B's" head office, i.e. the franchisor. All four SMEs are making use of a dedicated third party to assist with technical issues.

Section 2.2.2.1 of the literature indicated that most companies usually keep a system between two to seven years. Unlike the majority of SMEs in the SaaS group, all four SMEs in the Conventional Group have been working on other ERP or accounting software

previously and have also replaced their previous software due to various reasons. In the previous section it was mentioned that SME “B1” moved from on-premise to a hosted solution, but due to challenges they then moved back to on-premise. Franchise “B1” was running 2.5 years in the private cloud until they pulled the plug and did a reimplementation back to on-premise; they have been running on-premise for a year now.

SME “A” operated for eight years on their previous on-premise ERP system and two years on their current hosted ERP system. This SME isn’t satisfied and have plans to replace their system soon. In the previous section it was mentioned that SME “H” and “F” experience corrupted database issues causing downtime which is out of their control. SME “H” operated on their previous small on-premise accounting package for three years; it’s been two years now on their new on-premise accounting package. SME “F” was unable to provide the required system usage statistics, however they too want to replace their current on-premise system!

The main reasons why these organisations replaced their previous systems are:

- Functionality
- Integration
- Control and processes
- Automated business processes
- Better product support
- Growth
- Scaling
- Stability

The main reasons why franchise “B1” moved away from the being hosted through a private cloud are:

- Processing speed issues - the system was extremely slow and hanging
- Slow connection causing printing issues - simple print jobs taking several minutes
- System downtime
- Loss of sales
- Frustrations experienced by customers, staff and management

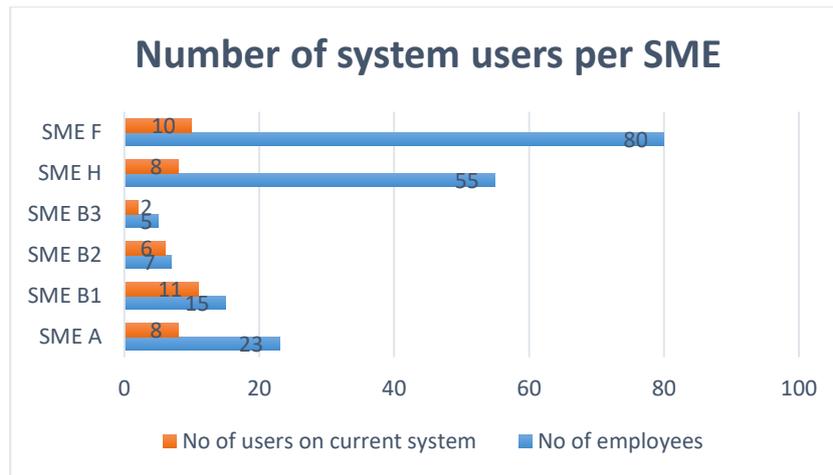


Figure 15: Number of system users (Conventional)

In figure 15, the employee head count of these organisations ranges between 15 and 80 people, while only 21.4% are classified as system users. Although this figure is slightly higher than for the SMEs in the SaaS group, two SMEs in the conventional group don't use the stock modules within their on-premise accounting software. SME "F" has developed their own in-house stock system, while SME "H" is managing the stock of their main warehouse in spreadsheets.

Three of the four participants in the Conventional Group are planning on replacing their existing accounting/ERP system within the next five years. Most are evaluating cloud-based alternatives to their current system.

Research participants in the Conventional Group rated the functionality of their current system much lower. Figure 16 indicates an average functionality rating of 53%.



Figure 16: System functionality rating (Conventional)

To conclude, SMEs in the two groups had different views and experiences. The majority of the SMEs who adopted SaaS-based ERP, have not been using conventional ERP or accounting packages previously. Instead, their business was created on word processing documents and spreadsheets. These SMEs are also less complex in nature compared to the Conventional group and probably immature in functional needs, functionality was rated a high of 85%. Currently these SMEs have no plans of replacing their SaaS-based ERP application.

Most of the SMEs in the conventional group have used smaller on-premise or single user accounting software previously. System functionality was rated 32% lower than the SaaS Group's rating. Most want to replace their current system and are evaluating cloud-based ERP alternatives.

4.3.2.2 The extend of cloud computing file sharing and storage being used

To evaluate current cloud computing adoption trends, research participants were asked about their file sharing and storage habits, such as the use of Dropbox and Google drive.

Although office suite documents like spreadsheets are still being stored on local computers and in some instances on office-based shared drives, all eight SMEs are making use of cloud storage. It was found that the predominant cloud computing storage option is Dropbox followed by Google Drive and that cloud file sharing and storage are adopted fully. One SME in the SaaS group is concerned with storing financial data in the cloud and only store employee timesheets.

4.3.2.3 The extend of SaaS business applications being used

To evaluate current cloud computing adoption trends, research participants in both groups were asked to indicate the business applications used in their organisation and if the application is either installed on-premise, hosted at a 3rd party provider or if the software is running in the public cloud. Business applications include email, HR and payroll, time keeping or job cards, expense tracking, CRM and supply chain management systems.

SaaS Group

Table 22 contains a list of business applications per deployment model for SMEs in the SaaS group.

System	Installed on-premise	Hosted at a 3 rd party (Private Cloud)	SaaS	Other (E.g. Spreadsheets)
Business email			C, D, E & G	
File sharing (Local Server, Dropbox, google docs)			C, D, E & G	C, D, E, G (Excel on PC/Server)
HR management (payroll)			D, E & G	C (Outsourced)
Time management			G	D, E
Expense tracking			G	D (Excel)
CRM		G		

Table 22: Business application usage (SaaS group)

While all four SMEs in this group make use of cloud email providers, three of them are running a cloud-based payroll system as shown in figure 17.

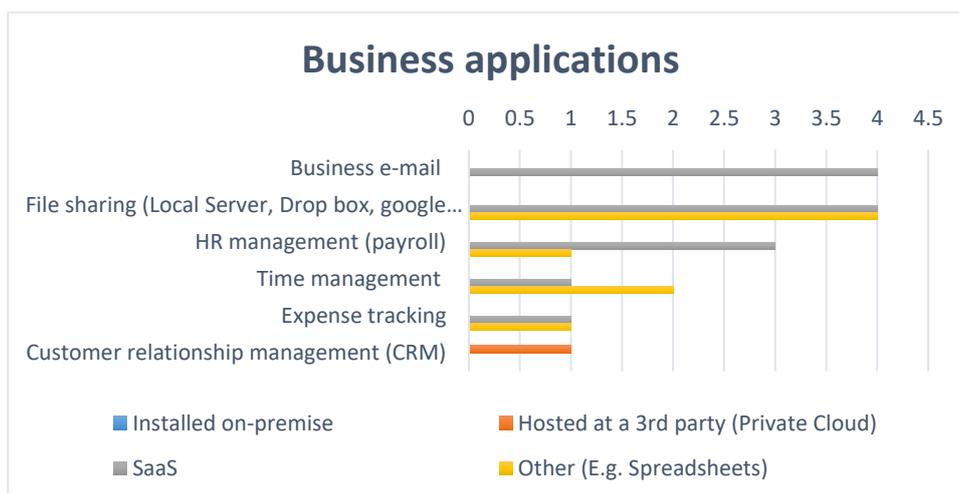


Figure 17: Business applications by deployment model (SaaS group)

Only one of three SMEs uses cloud-based time management system, while two other use spreadsheets to capture time sheets/ job cards. Only one SME make use of SaaS expense tracking software and has a CRM system deployed in the private cloud. SME “E” is interested in adopting a SaaS-based CRM system.

Conventional Group

In contrast to the SaaS group, table 23 indicates that cloud-based business applications are less popular in the conventional group.

System	Installed on-premise	Hosted at a 3 rd party (Private Cloud)	SaaS	Other (E.g. Spreadsheets)
Business email	A, F		B, H	
File sharing (Local Server, Dropbox, google docs)			A, B, F, H	A, B, F, H
HR management (payroll)			B	F & H (Manual) A (Outsourced)
Time management				A (Manual) B (Manual attendance registers) H (clock in system export to Excel)
Expense tracking				A, F (Manual)
Other (specify)	F & H (Stock management)			

Table 23: Business application usage (Conventional)

Figure 18 portrays that two of the four SMEs in this group are making use of cloud email, while only one make use of a cloud-based payroll system. Time management and expense tracking is still being processed manually on spreadsheets. SME “A” will be replacing their manual job cards soon as they plan to move over to an integrated SaaS-based ERP system. This move will result in less duplication of work and frustration of loosely integrated components.

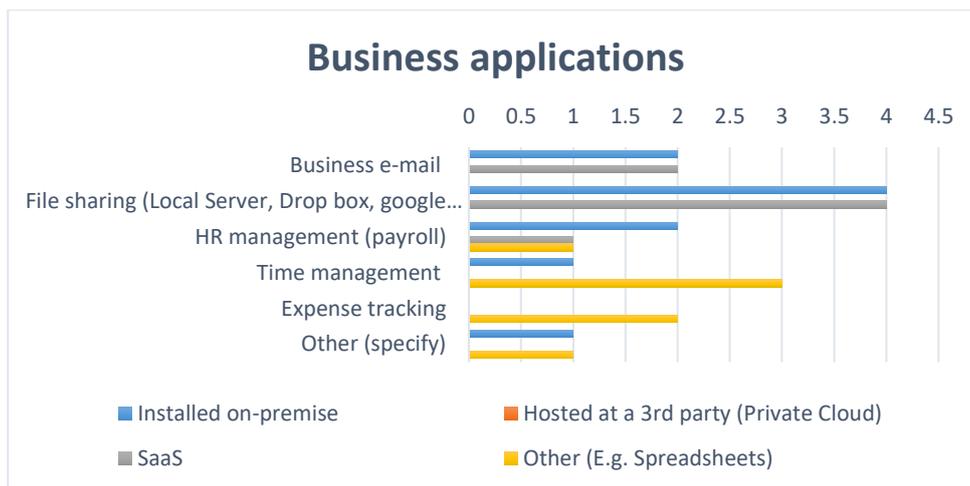


Figure 18: Business applications by deployment model (Conventional)

Due to lack in functionality two SMEs don't make use of their ERP's stock module. SME “F” makes use of an in-house stock management system while SME “H” relies on spreadsheets.

In section 2.2.4, it was stated that ERP was to be one of the very last applications to move over to the cloud. This trend can be seen here as all the SMEs in the SaaS Group had more cloud-based business applications. When research participants in the SaaS Group were asked how they feel about putting control of their SaaS-based ERP system in the hands of third parties, SME “D” stated that they have already done so with the cloud payroll system and were quite comfortable with it. There is a growing interest in both groups to adopt SaaS business systems.

4.3.2.4 Adopter category of SaaS solutions by local SMEs

In the literature review, Roger’s diffusion of innovations theory for adopting new technology explained that there are five adoption categories which classify members of society on the basis of innovativeness. Granting that Dropbox was launched a decade ago and is being used by over 500 million users (Ciaccia, 2017); file sharing and storage in the cloud have matured as it has been adopted by all the research participants in this study. One would want to classify any new adopters in the “Laggard” category. If we however take other business applications in consideration the picture will change a bit. Figure 19 illustrates the adoption of SaaS-based business applications by the eight SMEs.

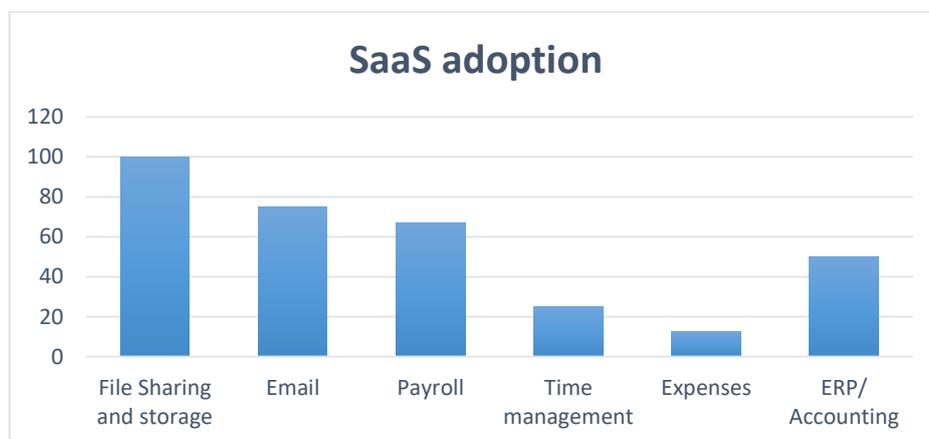


Figure 19: Adoption of SaaS-based business applications

Based on the results above, figure 20 indicates that 53% of the business applications (including ERP) used by SMEs in this research study is of a SaaS type. The adopter categorisation therefore indicates that SaaS has been accepted and approved, by a good number of SMEs in this study. Especially the smaller, less complex businesses who are ahead of the adoption curve.

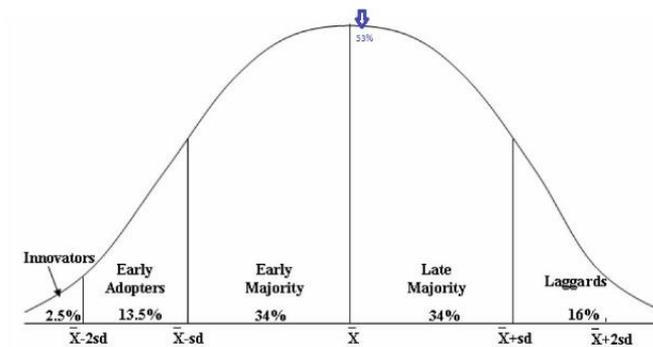


Figure 20: Adopter categorisation of SMEs on the basis of innovativeness

If any of these SMEs would want to adopt a new SaaS-based business application, they would therefore fall in the “Late Majority” category.

4.4 Critical SaaS-based ERP adoption factors

The following two sections will investigate which SaaS-based ERP adoption factors do the SMEs and cloud application providers consider as most important and how the results compare with studies done in developed markets. The thirteen factors of adoption have been discussed in section 1.2.

4.4.1 Critical SaaS-based ERP Adoption factors identified by SMEs in EMEs

In this study, research participants in both SaaS and Conventional groups were given the same list of thirteen adoption factors plus one new factor. Each SME have been asked to identify the three most important factors when adopting SaaS-based ERP. Existing SaaS tenants were asked what was important back when they initially migrated to the cloud ERP, while conventional customers were asked what they would consider as important should they want to migrate. Each participant also had to indicate which one of the three top selections is their primary adoption factor.

The thirteen adoption factors are availability (uptime), analytics, best practices, compatibility, costs, data integrity, flexibility, implementation, integration, security, trust, ubiquity and usability. Support was added as a fourteenth factor.

Holistic View

Table 24 shows the results of the top three adoption factors per SME, containing a total of 24 values.

Group	Conventional Group				SaaS Group			
Solution	On -Premise		Hosted	Hybrid	Public Cloud			
Factor	SME H	SME F	SME A	SME B	SME C	SME D	SME E	SME G
Top 1 factor	Data Integrity	Analytics	Trust	Availability	Implementation	Availability	Support	Data Integrity
Top 2a	Integration	Data Integrity	Data Integrity	Data Integrity	Usability	Best practices	Usability	Availability
Top 2b	Flexibility	Security	Security	Trust	Cost	Trust	Flexibility	Usability

Table 24: Top three adoption factors per SME

By counting the overall number of votes, figure 21 illustrates that data integrity received a total of five votes making it the most important adoption factor, followed by availability, usability and trust with three votes each.

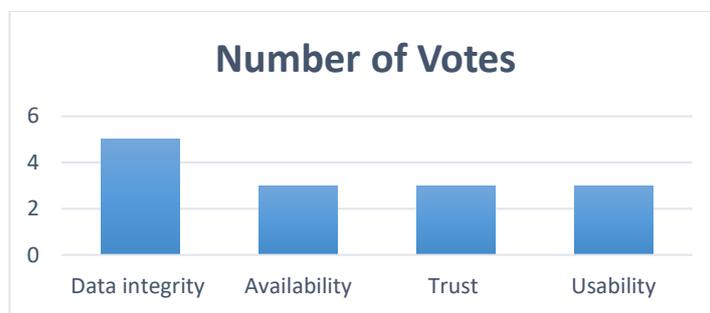


Figure 21: Top adoption factors by number of votes

In order of importance, figure 22 shows that participants consider data integrity as the most important adoption factor; it received two top one votes and three secondary votes. Followed by availability with two top one votes, and one secondary vote. Trust, with one top one vote and two secondary votes came third.

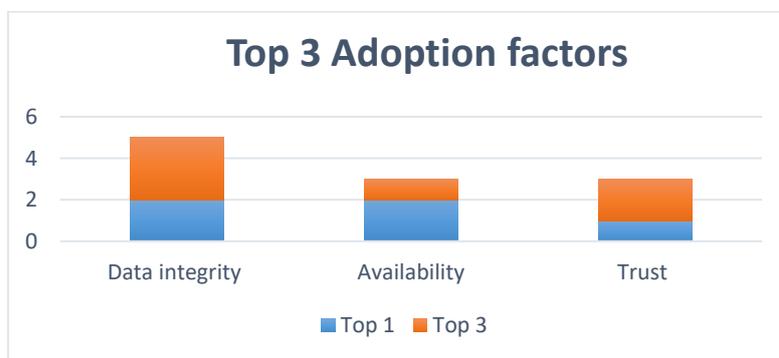


Figure 22: Top 3 adoption factors

A comparison by customer grouping

When comparing the results between the two groups, table 25 and figure 23 indicates how the outcomes differ immensely.

Adoption Factor	Conventional Group	SaaS Group
Most important (Top 1)	Data integrity (4 Votes)	Usability (3 Votes)
Important	Security (2 Votes)	Availability (2 Votes)
Important	Trust (2 Votes)	Data integrity (Top 1 Vote)

Table 25: Top 3 adoption factors by group

SMEs in the Conventional Group considered data integrity as the most important adoption factor. If there are any data anomalies found between various stock, sales and especially financial reports, they wouldn't adopt the SaaS-based ERP software! Section 2.2.4.2 has not listed data integrity as a SaaS-based ERP hindering adoption factor in the literature review, thereby making it a very important aspect for these participants.

Security was considered as the number one SaaS-based ERP hindering factor in the literature study. Although it was not considered as a top 3 adoption factor holistically in this study, SMEs in the conventional group did view it as their second most important factor followed by trust. While running on conventional ERP and having less SaaS business applications such as email and payroll, the security and trust factors show that these SMEs are more conservative, yet more complex in nature and are more cautious in putting their mission critical business systems and data in the hands of a cloud provider. The study agrees with the literature that SMEs who are more complex are less likely to be first adopters.

Interestingly enough, security was not even seen as a top adoption factor for SMEs in the SaaS Group. By having adopted SaaS-based ERP and more SaaS-business applications like payroll, these SMEs are probably more exposed to social media and modern technology and feel more secure. They are more concerned about how usable the system is by measuring to what degree its functionality can be used.

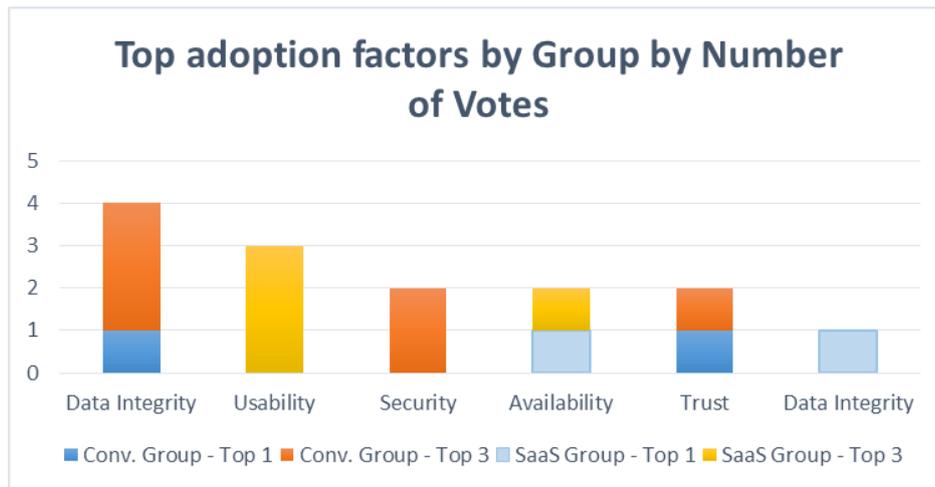


Figure 23: Top adoption factors by deployment model

SMEs in the SaaS group rated usability as the most critical adoption factor. In section 4.3.2.1 of this chapter it was found that SMEs in the Conventional Group rated their system functionality much lower. The usability factor however didn't even feature on the top three list of the Conventional group. Availability was second most important adoption factor for the SaaS group, followed by data integrity.

4.4.2 Critical adoption factors identified by cloud application providers in EMEs

The two local cloud application providers were asked what their customers would consider as the most important adoption factors. Provider 1 reckoned that cost and trust are the two most important factors and stated that usability and ubiquity also play a vital role. According to provider 2, the factors are all important, but "it also depends on the customer and the industry they are in". For one of their customers, integration is definitely number one, followed by security and analytics. Provider 2 added that "data integrity is important to everybody and trust is also important."

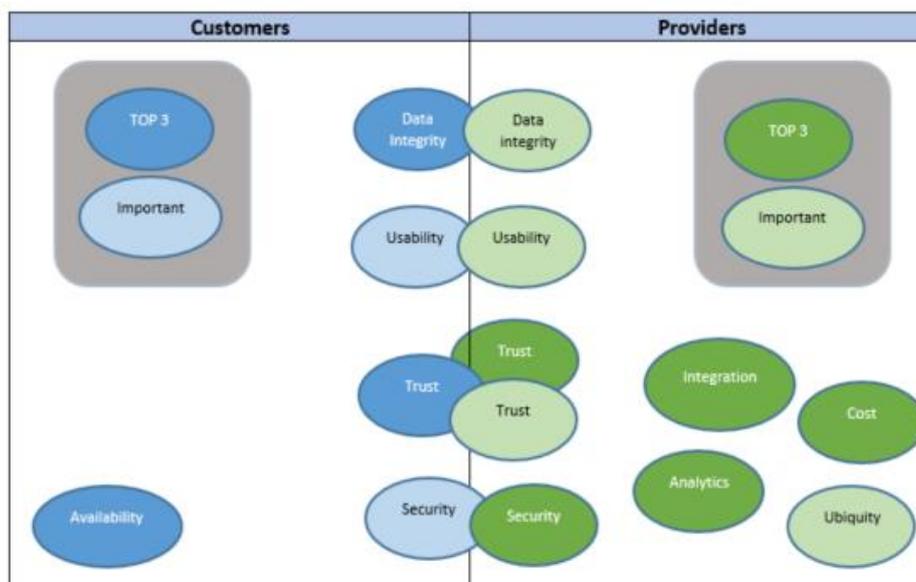


Figure 24: Top adoption factors of SME and provider participants in an EME

Figure 24 illustrates a mapping of the top adoption factors identified by the SMEs and local providers in this study. An interesting notion is that all the most critical adoption factors identified by the local SMEs are addressed by the local providers, except for availability. Should SMEs be concerned that cloud availability and uptime aren't on the local provider's top list? The following section as well as the chapter six will elaborate more.

4.4.3 Comparison of critical adoption factors between market economies

Section 1.2 made reference to a European research study done in 2013/2014. Based on their findings, cost was rated as the top one adoption factor amongst those SMEs operating in a developed market economy (DME).

In this study, only SME "C" considered cost as an important factor. Chapter five reveals that when research participants were presented with four SaaS-ERP quotes only one of the four preferred the cheaper option because it was cost effective. The rest preferred brand awareness, local support and a system which is popular amongst local peers above costs. Another observation made in this study was that all of the local SMEs in the SaaS Group indicated that they are satisfied with being charged a fair rental price. The literature review explained that in a SaaS model, capital expenses are transferred to operational expenses. Seeing that only one of the four SMEs in the Conventional Group was satisfied with a once off capital expense and yearly renewal fees, cost does seem to play a role. Cost was also seen as a top one adoption factor by European providers. Local providers in this study agreed that cost is seen as one of the most important adoption factors. As the focus of this study is on

losing control and not on cost implications, further research is required to understand why cost didn't make the top three list of the local participants.

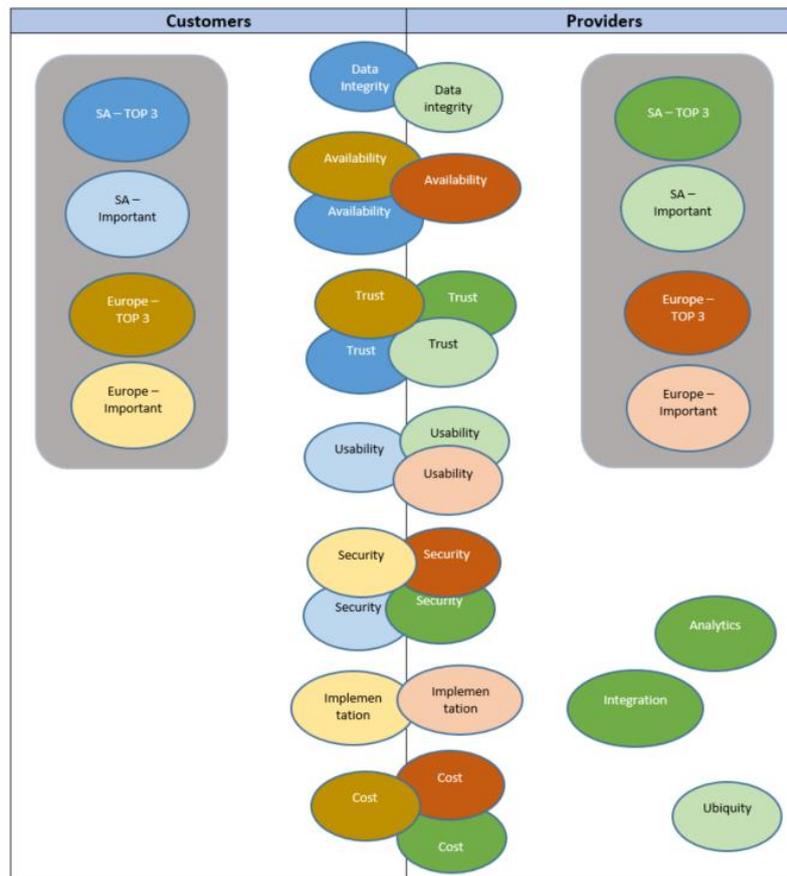


Figure 25: Top adoption factors comparison- SMEs and providers in an EME vs. DME

Even though trust and availability were considered as the second and third most important adoption factors by both the local participants and developed markets, the order of these two factors were different. SMEs in the DME viewed trust as more important while availability was more important locally. Chapter six indicates that cloud availability in a country with an inferior telecommunications infrastructure clearly has a bigger impact. European cloud application providers also viewed availability as one of the top adoption factors. An issue was raised in the previous section that the local cloud providers might not see availability as important, international providers however definitely covers availability from the DME research results! The local participants agree with the European findings on the importance of security, however it was not listed it in the top three. Both European and the local providers viewed security as very important. Another observation is that usability received the third lowest rating by the European participants compared to it being fourth most important factor locally. Even though this is a big gap, the usability factor is more on-par with the European cloud application providers who also rated usability in fourth place. The local cloud providers agree that usability is considered as an important adoption factor.

The important adoption factors from a provider's point of view, locally and internationally, are mapped with the customer's point of view in figure 25. Provider 2 viewed integration and analytics as very important adoption factors. These two factors received a low overall score by local customers, however SME "F" did mention that analytics was their top 1 adoption factor, while SME "H" considered integration an important adoption factor.

The research findings illustrated in figure 25 confirm that of the thirteen adoption factors, availability, trust, usability, security and cost from both customer and provider's point of view agrees to a considerable extent between the local research participants and developed market economies.

4.5 Conclusion

Chapter four analysed the adoption of cloud computing by SMEs running on conventional ERP with those on SaaS-based ERP to determine in which adopter category the local participants find themselves at this point in time and to establish which SaaS-based ERP adoption factors these SMEs considered as important. The results were compared with participants in a DME.

This chapter provided answers to five secondary research questions. Firstly, it was required to determine to what extent SaaS-based accounting systems / ERP are being used by the local SMEs. Four of the eight SME participants have already adopted SaaS-based. The majority of these SMEs are less complex in nature and have not used conventional ERP or accounting packages previously. Instead, their business was originally running on word processing documents and spreadsheets. Only a small percentage of their employees are using the system. With an average functionality rating of 85%, these SMEs have no plans to replace their SaaS-based ERP/accounting systems. Secondly, it was required to understand and compare SMEs operating on the older conventional deployment models such as on-premise and hosted ERP applications. It was found that the majority of participants in the Conventional group have used smaller on-premise or single user accounting software previously. Only a moderate to small percentage of their employees are using the system. The majority of these SMEs are however planning on replacing their current system. Although these SMEs have rated their system functionality 32% lower than those in the SaaS group, their business structure is much more complex, they are probably more mature in their functional needs and have been faced with typical limitations of business applications.

Thirdly, it was required to determine to what extent cloud computing file sharing and storage are being used by SMEs operating in an EME. Office suite documents such as spreadsheets

are still being stored on local computers and in some instances shared drives at offices. All eight SMEs have already adopted cloud sharing and storage. The predominant cloud computing storage option is Dropbox followed by Google Drive. It was also found that cloud file sharing and storage are used to quite an extent, except one participant who doesn't store any financial data in the cloud and only use it to store employee timesheets. While file sharing and storage is a lower-risk form of cloud computing, it was also required to determine to what extent a higher risk form of SaaS business applications, are being used by these SMEs. It was previously stated that ERP is found to be one of the very last applications to move over to the cloud. This trend can be seen as all the participants in the SaaS Group have adopted more cloud-based business applications than the Conventional group. Most of these SMEs have initially adopted cloud payroll systems prior to adopting SaaS-based ERP. SMEs in the Conventional group have already invested a lot of hard-earned money, sweat and tears in other technologies. There is also an interest in adopting new SaaS-based systems, such as SME "E" who is in dire need of CRM and SME "A" who plan to take over the world by adopting SaaS-based ERP, time management and expense tracking soon.

Based on the basis of innovativeness, it was lastly required to determine in which adopter category these participants would find themselves specifically by comparing different SaaS business solutions. This study has found that based on Roger's DOI theory, if any of these eight participants were to want to adopt a new SaaS business application, they would fall in the "late majority" adoption category as 53% of the business applications used by the SMEs in this research study is of a SaaS type.

Chapter 5: Cloud Support

5.1 Introduction

This chapter investigates the effect of provider support on the adoption of SaaS-based ERP.

Support in this context isn't only limited to the support provided by the cloud application provider, it encapsulates a whole value chain of providers. To be able to connect to the SaaS-based ERP system, Internet Service Providers (ISPs) need to provide support when the network is down or very slow. If the system is hosted at a third-party hosting provider such as Amazon or Azure, cloud application providers also require infrastructure and connection assistance from hosting providers on an ongoing basis.

In order to determine if support influences SaaS-based ERP adoption, research participants were firstly asked to select a cloud application provider from a list of mock-up quotes, with each quote governed by different circumstances. Participants had to indicate whether they would migrate to one of the SaaS-based ERP or rather operate on an on-premise or hosted ERP application. In the second part of the chapter, SMEs and cloud providers were asked to rate the various providers in the value chain.

5.2 The impact of support on SaaS-based ERP adoption

The following section tests the impact of support on the adoption of SaaS-based ERP/accounting applications.

As a business scenario, research participants were given a list with five mock-up multi-tenant ERP quotations and were asked if they had to replace their current system, would they consider one of these quotes or would they rather prefer an on-premise or hosted application. The quotes covered various elements ranging from cost, brand familiarity, support turnaround time, availability of local support, training facilities and many more. The five quotations, in order of monthly rental cost, are laid out in table 26.

Quote	Background	Support
1 <i>System:</i> <i>CloudX</i>	<ul style="list-style-type: none"> • Cheapest option • Unknown system • Foreign provider in an unpopular country. • CloudX is hosting the system and data. 	<ul style="list-style-type: none"> • You found one video of the product. You like the system and it looks like it will meet your requirements. • International helpdesk, however no availability of local support. Due to time

		<p>zones, it might take a few days to solve support queries.</p> <ul style="list-style-type: none"> • Consultants aren't fluent in English.
2	<p>System: CloudY</p> <ul style="list-style-type: none"> • Application provider is a new entrant in the market. • Although the provider is unknown to you, the system and data is hosted at a well-known, secure, state of the art cloud provider who is responsible for server maintenance, upgrades, security and backups. 	<ul style="list-style-type: none"> • No local support, there is a 24-hour international support desk. • Good support turnaround time and English communications skills. • Plenty of online help. Videos, group forums, training documents and online training courses.
3	<p>System: CloudZ</p> <ul style="list-style-type: none"> • Well-known international brand. You however personally don't know of anyone using the system. • Location of cloud servers is unknown. 	<ul style="list-style-type: none"> • Four-year footprint in international market. First local SaaS-tenant adopted system only a year ago. • Two local support offices, JHB and CPT. One training facility in JHB. • Support turnaround isn't always quick. • Good product reviews
4	<p>System: CloudSA</p> <ul style="list-style-type: none"> • Slightly higher subscription cost, yet affordable. • Locally a well-known product. • The servers are hosted locally in a secure data centre. 	<ul style="list-style-type: none"> • Extensive network of local partners to provide support • Training facilities in all local major cities • You have two or three friends who also use the system at their business. They all sound very happy, except for your one contact who said that they sometimes get frustrated with the speed of the system when connecting via their ADSL internet line ... the system hangs and might be slow on certain days.
5	<p>System: Cloud-Scale</p> <ul style="list-style-type: none"> • As Quote 4, except that the system works on a usage billing model instead of a flat rate. • System resources can be scaled up or down as per daily/weekly/monthly and seasonal requirements. • Location of servers is unknown. 	As above (Quote 4)

Table 26: SaaS-based ERP selection scenarios

Research participants were asked to select one of the quotes above or alternatively:

- I. Select an on-premise ERP system, or
- II. Select a hosted ERP system.

Outcomes:

It was found that five out of six participants prefer SaaS-based ERP, while one favours an on-premise system.



Figure 26: Results of SaaS-based ERP selection scenarios

None of the SMEs desired an application or provider that's they are not familiar with, where no local support is available, or a system which can't be recommended by a trusted source, even if the cost is low. SME "D" prefers to stay with their current multi-tenant system, they are very price sensitive and not prepared to spend large subscription fees every month.

In figure 26, two of the five SMEs prefer Quote 3. Although SME "B1" is part of a greater franchise group, if they had a say they would accept Quote 3 as it isn't only cost effective but also provides local support. SME "C" (who listed cost as a top adoption factor in chapter four), also preferred this quote because it isn't only a bit cheaper, but also a well-known brand.

The remaining two participants prefer Quote 4. Recommendations, local support and training facilities play a big role for SME "E". In the second part of this chapter, SME "F" will indicate the importance of personal relationships with their application provider. Quote 4 is ideal for them as it a well-known package supported by an extensive network of partners.

5.3 Provider support findings

SME participants were asked to rate the support they currently receive from both their application provider and ISP. Cloud business platform hosting providers also play a major role in supporting the cloud value chain. None of the cloud providers in this study hosted the application they sell and implement and therefore had to rate the services and support received from their cloud hosting providers.

5.3.1 Application provider support

In figure 27, participants who already migrated to SaaS-based ERP were more confident in the performance of their cloud application and therefore rated their application provider support higher (blue) than the Conventional group (green).

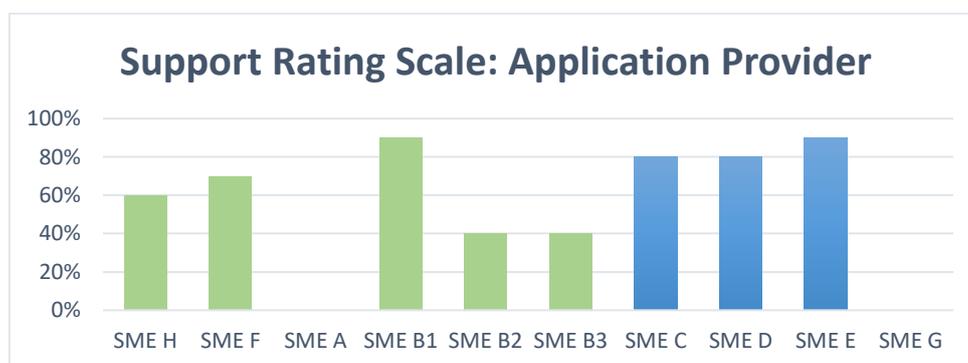


Figure 27: Support rating scale - Conventional vs SaaS

Organisations would typically use the provided support in the beginning, but after building up their own internal capabilities and knowledge, they would become less dependent on their application provider over time.

SaaS group

Chapter four revealed that SaaS-tenants rated their ERP functionality 85%. It was stated that these SMEs are less complex in nature and had less functional requirements than SMEs in the Conventional group.

SaaS tenants are rating the support receive from their cloud application provider a high average of 83%. It was also found that the SaaS-tenants were less dependent on a support desk. SME "G", an IT company, was unable to give a rating as the only contact they have had was when they initially registered for the software and for their annual subscription

renewals. SME “D” added that the support desk might not always reply promptly, but she will eventually receive feedback.

Conventional Group

Chapter four found that customers running on conventional ERP rated their system functionality an average of 53%.

The Conventional group rates their application provider support an average of 65%. Some of the participants in this group had a few bad experiences. SME “A” didn’t want to rate their application provider due to all the frustrations they have experienced as mentioned in chapter four. The organisation has lost integrity and trust in the provider mainly because the provider didn’t deliver on what was promised. There were times when management had to shift their focus on system related issues instead of the actual business. Although SME “F” rated their service provider moderately high, they have to wait in a “help desk ticketing queue” for help. A personal face-to-face relationship would be ideal, preferably consultants who has knowledge of your business. Although SME “H” receives free support as part of the annual maintenance fees, database corruption issues are a major setback as their on-premise ERP system is down while their application provider takes up to 72 hours to repair the database.

The rating would have been 53% if franchise “B1” was still on a hosted solution. Seeing that Franchise “B1” moved back to on-premise, the interviewee was speaking on behalf of franchise “B2” and “B3”. Franchise “B1” is serviced by a local provider partner that’s located in the same business park. This participant rated their local partner’s support 90% as the relationship is good and support is within reach. The franchisor and franchises “B2” and “B3” who connect to the hosted ERP system, have a full-time system administrator employed at head office and is supported by a partner provider in Johannesburg. According to SME “B1”, the system administrator’s service is terrible, don’t ask me why he is still there”. Franchise “B2” and “B3” prefer support closer to them as they too feel like a number in a ticketing system. The support turnover of the Johannesburg provider is slow, some of the high priority issues takes two to three days to be resolved.

5.3.2 Internet service provider support

Both cloud application provider participants indicated that the recommended requirements to connect to the multi-tenant ERP is only a computerised device, internet browser and an active internet connection.

ISP's are responsible for the provision and support of broadband technologies. SMEs were asked to rate their ISP support.

Figure 28 indicates that the SaaS group (blue) rates their ISP support an average of 65% and the Conventional group at 58%. A main reason why the former rated their ISP providers better in general, is because all of these participants had to upgrade their bandwidth technology to resolve many internet connectivity issues.

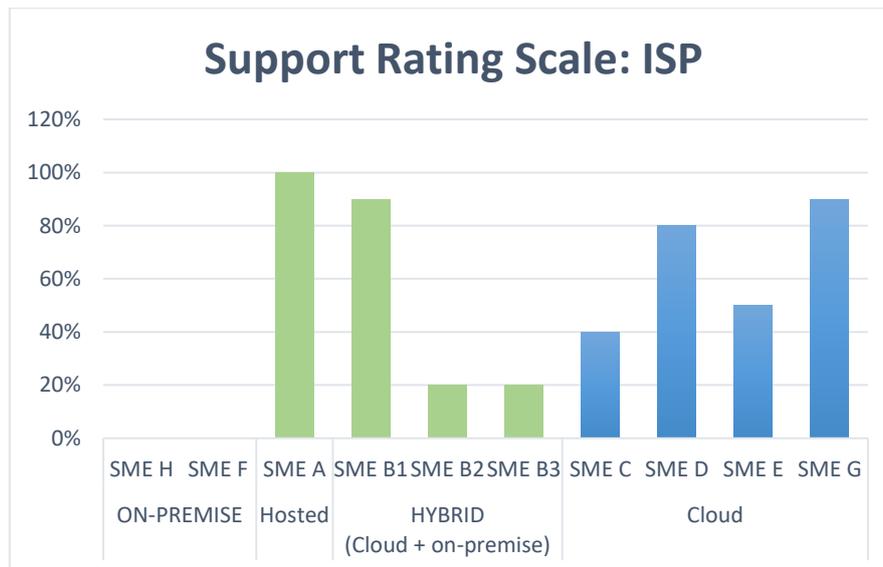


Figure 28: Rating scale - ISPs

In the Conventional group, both SME "F" and "H" were unable to give a rating, internet connectivity is however not a requirement when using on-premise ERP. If franchise "B1" didn't upgrade their ADSL line and moved their system back to on-premise, then their ISP rating would have been just as bad as the other two franchises. Chapter four and six explain how these franchise daily experience severe connectivity issues.

5.3.3 Cloud business platform hosting provider support

In cases when a cloud business platform hosting provider, such as Amazon or Azure, is responsible for hosting the SaaS-based ERP system, then cloud application providers will require infrastructure and connection support on an ongoing basis. Although SaaS-tenants don't work with these entities directly, cloud application providers were asked to rate the services and support from these entities.

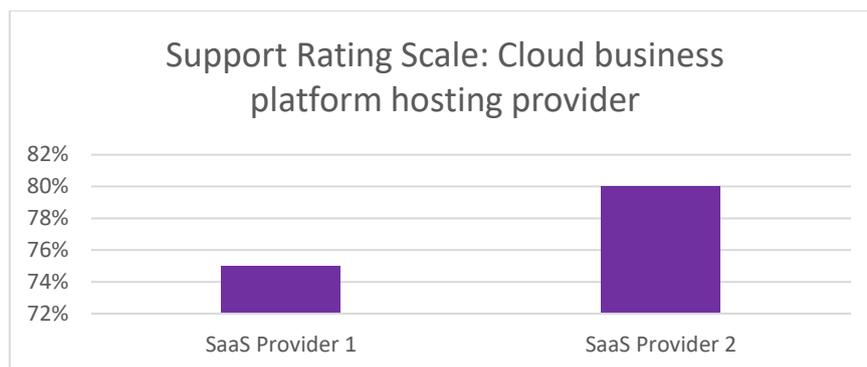


Figure 29: Rating scale - Cloud hosting provider

Above in figure 29, cloud hosting providers receive a high average of 77.5%. Provider 1 noted that their current hosting provider has excellent knowledge, skills and provides them with quality service, however an increase in the scale of projects is forcing Provider 1 to switch to another certified cloud hosting provider.

One challenge provider 2 had was that the new cloud technology proved to be a massive learning curve. It took them up to six months to understand the new cloud technology, commenting that “it’s very good, but not very simple”. Their multi-tenant system is running at a well-known international cloud business platform hosting provider. According to provider 2, the international support desk is helpful, techspeak is a major challenge... “You need to know how to ask the question... they might not understand exactly what you mean or what you need and if you don’t know what’s available, you won’t know what to ask”. Good news for this participant is that their cloud hosting provider is planning on building a data centre locally in South Africa soon. Change in a provider’s business model will be discussed in chapter eight.

5.4 Support issues and loss of business

SMEs were asked if their business suffered any financial losses when experiencing critical support issues from their providers. None of the SMEs in the SaaS Group were negatively affected by poor quality support. As a backup plan, all the participants noted that they would operate manually should something serious happen. Refer to business continuity plans in chapter six.

Two out of four participants in the conventional group admitted that low quality support by their application provider had a negative impact on revenue. It was earlier noted that SME “A” should have focussed more on their business instead of the system and connection related issues their providers should have resolved. Another SME on a hosted environment who suffered is franchise “B”. Slow connection and printing issues caused a loss in sales as some

of their customers moved over to the competition. Without a reliable bandwidth technology, they sit with an unworkable system. Printing from the system sometimes takes more than a minute and a half. According to them, “the customers are frustrated with the situation. In our Tzaneen branch, we had a customer who recently asked us if we have fixed our system speed issues. He stopped buying from us due to this frustration! We have lost customers in this process”. Both franchisor and provider partner have been on-site in an attempt to try and fix the issue. Last mile connectivity is discussed in chapter six.

When cloud application providers were asked if critical support issues have resulted in customer complaints, a decline in profits or loss of customers and business, provider 1 responded that they “have not lost any of their customers in their multi-tenancy cloud system, it’s possibly rather the opposite”. Provider 2 agreed by commenting that “the cloud is the reason why we got business, not lost business!”

5.5 Conclusion

In this chapter, the collected interview data was analysed to determine what the effect of provider support is on the adoption of SaaS-based ERP.

A scenario was sketched whereby research participants had to select from a list with five SaaS-based ERP systems, or alternatively migrate to an on-premise or a hosted solution. Five of the six participants prefer SaaS-based ERP, while only one favoured an on-premise system. None of the SMEs desires an application or provider that’s unknown to them, without local support, or a system which can’t be recommended by a trusted source, even if it’s the most affordable option.

SMEs in the Conventional group were rating their application provider’s support much lower. Two of these participants rely on their application provider heavily when they experience database corruption issues. Strong personal relationships are very important for these participants, this is however a challenge according to Provider 1 in chapter eight.

The SaaS group was less dependent on application provider support. Although their businesses are less complexed, their systems are easy to learn, user friendly and there are plenty of online help available. The previous chapter points out that last mile connectivity and bandwidth technology are two SaaS-based ERP challenges. Participants revealed that they are not overly positive about their ISPs and rates them an average of 62%. Although the SaaS group rated their ISPs slightly higher, all of these participants had to upgrade their bandwidth technology since using SaaS-based ERP for better internet connectivity.

Cloud application providers and ISPs are not always the only entities responsible for providing a seamless cloud experience. The two cloud application providers have rated the services and support they have received from their cloud business platform hosting provider an outstanding average of 78%

SaaS providers confirmed that they are only gaining from the cloud, evidently seen in the shift of revenue streams. None of the existing SaaS tenants have lost revenue because of the cloud. Two of the SME participants states that issues with their hosted ERP system caused a knock in revenue, mostly because of bad service received from their application provider and a poor telecommunications infrastructure. Inferior bandwidth technology might have affected SMEs in the SaaS Group as well should they have been in the same physical location using the same bandwidth technology, software design however plays a role as well.

Although SMEs are price sensitive, these participants would rather subscribe to a well-known SaaS-based ERP brand that offers local support and invest in superior bandwidth technology to get most out of their system.

Chapter 6: Cloud Availability

6.1 Introduction

Chapter six investigates the effect of cloud downtime and connectivity challenges on the adoption of SaaS-based ERP. Research participants were asked questions on scheduled downtime, unscheduled downtime, data loss during downtime, provider downtime penalties, business contingency plans, last mile connectivity, broadband technology and connection latency.

6.2 The impact of cloud downtime on SaaS-based ERP adoption

Before examining the experiences of actual scheduled and unscheduled downtime by the research participants, tolerances for downtime will be tested first to determine the impact it has on the adoption of SaaS-based ERP.

Chapter five presented a scenario whereby research participants were given a list of five multi-tenant ERP quotations. They were asked if they had to replace their current system, would they consider one of the quotes or rather go for an on-premise or hosted application. Four out of five of the participants preferred SaaS-based ERP while the remainder would replace their existing system with an on-premise system. After research participants made their choice, they were then presented with four scenarios and had to decide whether they would still go with their initial choice, or select one of the other quotes, or revert either to an on-premise or hosted application. Their choices were tested against the following scenarios:

Scenarios:

1. The cloud provider/host you selected is planning downtime by doing server maintenance every month. Downtime of up to six hours can be expected, however the provider's schedule is very reliable and always schedules downtime after hours or on Sundays. A downtime notification is sent out 48 hours in advance.

Figure 30 illustrates that three of the four participants would be satisfied with a transparent and reliable agreement scheduled not within business hours or on Sundays. Only one participant would select another SaaS-based ERP alternative as they are worried about after-hours stocktaking. Planned downtime outside business hours therefore has no effect on the SaaS-based ERP adoption as none of the participants would revert to on-premise system.

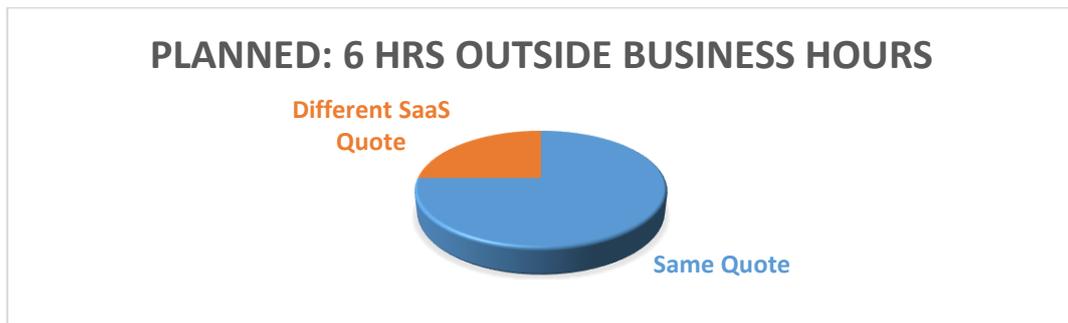


Figure 30: Scheduled downtime outside business hours

2. In scenario two, planned downtime is scheduled within business hours and might take up to three consecutive hours. The provider gives their assurance that it will happen at most once a month. A 48-hour downtime notification is sent out.

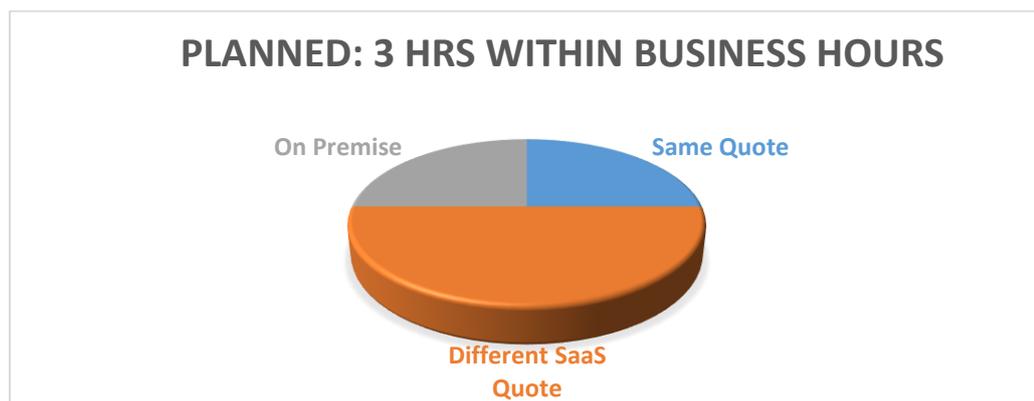


Figure 31: Scheduled downtime within office hours

Figure 31 indicates that this scenario would only be acceptable to one of the four participants while another would prefer an on-premise system. The two remaining SMEs would prefer an alternative SaaS-based ERP provider. Although SaaS-tenants will be notified in advance, most of the participants are worried about downtime scheduled within office hours. Planned downtime within business hours therefore has an effect on the SaaS-based ERP adoption.

3. As in scenario two, but no downtime notification is sent out.



Figure 32: Unscheduled downtime within business hours

As per figure 32, downtime up to three hours within office hours and without any form of notification is unacceptable to all four participants! While three would still go with an alternative SaaS-based ERP option, one would revert to an on-premise system. Downtime of an unplanned nature occurring within business hours and without notification will have an effect on the adoption of SaaS-based ERP adoption.

4. In the last scenario, a severe cloud server outage caused by human error occurred causing system downtime of three consecutive days.

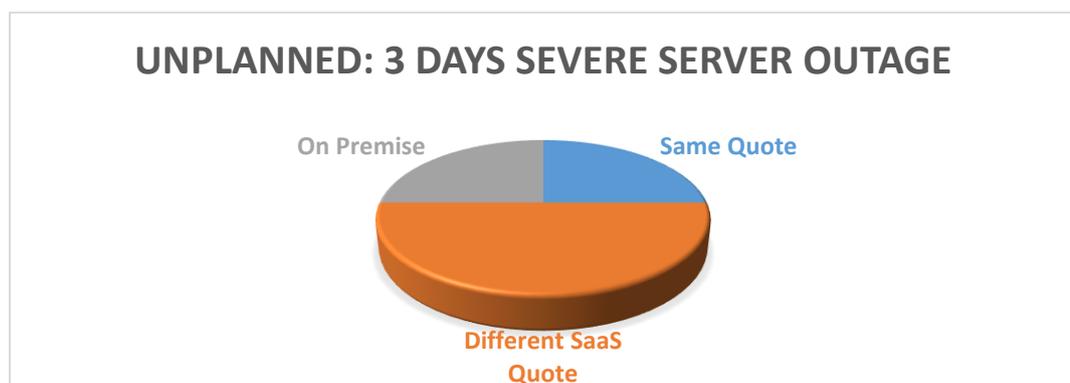


Figure 33: Severe server outage

Figure 33 illustrates that such a severe business disruption would be unacceptable to most of the four participants as three would migrate to a different provider. Assuming that some would see this as an indicator of unreliability, only one would remain loyal to this provider. Two of the participants would still prefer cloud but would select another SaaS-based ERP option while the rest would abandon cloud totally and revert to an on-premise system. Only

a few hours of downtime would be tolerable for the respondents. A severe cloud outage over a period of days will have a great effect on SaaS-based ERP adoption. Most SMEs wouldn't reject SaaS-based ERP, they would however only prefer a different cloud provider.

Summary of findings:

Clients fully understand that they will need to deal with cloud downtime, however it shouldn't have a negative effect on their business. It's therefore essential that cloud application providers, cloud hosting providers and ISPs schedule downtime to happen after-hours. To be able to plan around downtime, users need to be notified in advance. Scheduled downtime during office hours should be avoided as far as possible and if need may be, only as short as possible. Although scheduled within business hours, unscheduled downtime and a severe cloud outage will have an effect on SaaS-based ERP adoption, it will have a far greater effect on a cloud providers' retention.

6.3 Actual scheduled and unscheduled downtime

The following section investigates how participants in both Conventional and SaaS groups are currently affected by scheduled and unscheduled downtime.

6.3.1 Scheduled downtime

Conventional Group

None on the SMEs in the Conventional Group suffered from major planned downtime issues. These SMEs are in control of their system and can plan downtime for when it will suit them best. Some ERP settings require one to kick users off the system, but SME "F" mentioned it's quick and only takes a few minutes. The longest SME "A" was down was three days when data was migrated to a new server at the hosted provider.

SaaS Group

Downtime is typically scheduled after-hours, at least once a month. Most often this is because cloud providers are doing planned system upgrades and server maintenance.

There were some experiences of downtime during business hours, but in a multi-tenant environment, providers started to realise that the cloud created a change in their own business models as they can't be limited to normal support hours (see chapter eight). SME "C" is one example of a SaaS-tenant who was down on multiple occasions when they migrated to the

cloud back in 2014. Their longest planned downtime was a whole morning. SME “E’s” system was down at most for an hour during office hours, while SME “G” was once down for almost three hours. Late night work is being affected, often without notification. When SME “D’s” cloud provider schedules downtime for after-hours, it impacts them negatively as the participant works late nights assisting her husband with his accounts. They don’t always receive downtime notifications. In chapter four it was mentioned that their invoicing process is delayed by downtime which directly impacts cash flow.

It was found that most of the time, ISPs contribute significantly more to downtime than application providers did. For SME “C”, the cloud application provider used to be the reason for downtime, now it’s their ISP.

All four SMEs in the SaaS group are notified 24 to 48 hours in advance of scheduled downtime, which is either via a system notification or email sent by the provider. A system notification is a more powerful medium as the email is only sent to the main contact person. The participant at SME “G” is mostly unaware of scheduled downtime as only the director receives the downtime email. SME “E” hardly ever read the system downtime notifications as it’s always scheduled for after hours. Experience shows that moving to an environment where your concerns are being considered, lead to you having to plan around unavoidable downtime.

6.3.2 Unscheduled downtime

Conventional Group

Some of the SMEs in the Conventional group experienced unscheduled downtime during office hours, due to database locks, corrupted databases and outages at hosting providers, ISPs and the electricity supplier.

SME “A” experienced about two incidents during business hours the last two years. An outage occurred at their ISP causing downtime of almost two days. On a second occasion, they were down for almost three hours due to system issues at their hosting provider.

Franchise “B1” had roughly two unscheduled downtime occasions with their on-premise system. The whole town experienced an entire blackout for almost three hours, there was no electricity and no internet. When franchise “B1” was still operating on the franchisor’s hosted application, unplanned downtime happened regularly; the system was initially deployed at the franchisor’s head office. At one stage unscheduled downtime occurred daily with two and a half hours of downtime being the longest the research participant recalls, “sometimes we were down for 40 minutes to an hour and half. When late in the afternoon, you leave the office in a state and then walk into the same issue the next day”. The root of the problem was at the time

of the interview still unknown. The issue might be with their third parties and not by the application itself. All stakeholders have been asked to be onsite to address the issue.

SME “F” and “H” suffer from regular downtime which is caused by a corrupted database taking days to be restored by their application provider. The longest SME “F” was once down for three days. It takes about 48 hours to do the restore, according to SME “H” who has the same on-premise system. In the last two years, SME “H” had corrupted database issues on two or three occasions. According to the office manager, the longest they were down was an outrageous four working days over a period of six days. Database locks also cause downtime for SME “F” as the database would lock some of the users out more or less twice in a month. All the users are then informed to save and log out as the only way to fix the issue is to restart the database server. These issues might symptoms of outgrowing their system, see chapter four. A scalable system for these two SMEs will be ideal.

SaaS Group

Participants in the SaaS group had little experience of unscheduled system downtime, much less than the Conventional Group. Most of the downtime some experienced was mainly due to their ISP being down and connectivity issues. Connectivity plays a critical role in Cloud ERP.

Neither SME “C” nor “G” experienced unscheduled downtime before. If they are unable to log in, the problem is with their ISP. SME “D” was only once unable to log into the system within office hours. This participant’s husband, who is the also owner, logs more than her into the system during business hours and mentioned that there are times during the day that he can’t connect to the system via his LTE mobile hotspot. He was however able to open other webpages. Their catering business is located in an industrial area and insulated with thick concrete walls which might possibly affect his connection. SME “E” had an issue once with their ISP and were unable to log into the system for two to three hours. As a backup plan, they managed to connect to the system via wireless bandwidth technology.

Managing your own server onsite requires the availability of resources, appropriate knowledge and system management with thorough disaster recovery plans in place.

6.3.3 Cloud application providers and downtime

The following section investigates the cloud application provider's view of planned and unplanned downtime.

Scheduled downtime

Downtime is scheduled mostly for hardware upgrades and routine server maintenance. Both providers are proactive and send out emails when downtime is scheduled, as the literature review recommends in section 2.2.7.1.

SaaS-based ERP Provider 1 schedules downtime once in three to six months. Downtime is usually scheduled for overnight, or weekends in case of an emergency. The longest planned downtime within office hours was for an hour. Provider 1 will email the main contact person at each SaaS-tenant site in advance when planning downtime and commented that the drawback of the single email is that not everyone in the organisation is informed. SME "G" was found to be one such an example earlier in this chapter.

One of the main SaaS-based ERP hindering factors explained section 2.2.4.2 of the literature review is that one isn't in control of upgrades and that all the SaaS-tenants are affected with the upgrade. New advanced cloud technology however allows Provider 2 to update only certain SaaS sites when a new version of the ERP is released. They can determine to which company the update must apply and only those companies will be affected by downtime. Provider 2 would rather batch a number of non-critical updates and then schedule downtime approximately once every four months once a stable version is released. At times they will arrange with their client(s) to do the updates during business hours, if it isn't feasible then downtime is scheduled over weekends. When their multi-tenant ERP is offline, users will get an error when trying to connect.

To ensure all the parties are informed of any scheduled downtime, it's also the cloud hosting provider's duty to inform their cloud application providers in advance when planning hardware or operating system upgrades who should in turn notify their SaaS tenants.

Unscheduled downtime

About a year ago, provider 1's cloud business platform hosting provider ran automatic operating system updates when an unforeseen software bug caused drama. According to Provider 1, "the first time the downtime occurred was for nearly two hours within office hours. We were able to sort the issue out and restarted the server. Then, this event reoccurred. There were about 3 reoccurrences". For a period of three to five days this issue has reoccurred. "The

whole platform wasn't down, it was a black-screen-per-user freeze up. Users who were logged in were able to work, however any new login attempts experienced the issue". There was no consistent pattern. By being part of a supportive community, these types of issues can be addressed faster. In reaction to this, the cloud provider became more proactive by verifying operating system update notes carefully and only schedule downtime to do the automatic updates when it's required.

Provider 2 commented that their cloud business platform hosting provider who is a well-known international company, is very reliable and neither they, nor their SaaS-tenants, ever suffered from any server related unplanned downtime. "It's early days for us as well. We are also new to this. There is no reason why there should be downtime, other than self-inflicted. Certainly not the application and certainly not the cloud provider". When Provider 2 needs to do critical unplanned upgrades, they will kick the users off and within only a couple of minutes perform the ERP updates. Scheduled downtime is however preferred as it's much more controlled and less annoying for their users who can't log in and they need to.

These experiences indicate the importance of choosing a provider with a history of reliability.

6.4 Service Level Agreements and cloud uptime percentages

Are SLAs doing any good and do people read all the small print? Are they perhaps not mostly used to apologise for any inconvenience and provide quick fixes? Section 2.2.7.3.1 of the literature review mentions that downtime is normally stipulated in the SLA and when uptime is compromised, certain providers might give a credit or discount as compensation.

None of the participants in the SaaS Group have been compensated. SME "D" only received an apology when they experienced downtime informing them that their provider is attending to the problem.

Provider 1 is serious about uptime and will compensate their customers if the system goes down. Although there is a clawback clause in their agreement, it isn't that big of a substantial amount which customers will get back. Provider 2 don't compensate directly as there is no penalty clause. If clients experience downtime, they will look at what the cause was and take it from there. Their customers probably won't be charged for the time spent in rectifying the issue.

6.5 Business continuity plans

When a cloud outage might occur, section 2.2.7.3.1 explains that providers and customers should be prepared and have a business continuity plan in place. In this study it was found that most of the SME participants don't have explicit plans and don't take precautionary steps.

Even though not documented, the research participants in the Conventional Group have their short- and long-term continuity plans mapped out. It depends on the situation, but they would usually operate manually and "wait it out" till the system is available again. In cases where a severe outage occurs, backups are available both on and offsite. An interesting observation is that three of the four SaaS participants were shocked with this question and replied with "I don't have a business continuity plan, this is bad!", "There is no backup plan" and "Wow! Holy cow! I haven't thought of that... because, it has never happened". Then, eventually the general response was to fall back to a manual system, wait for the system to go back online and then catch up.

Only some of the SMEs keep pdf copies of files such as invoices and statements should there be any account queries. Many SMEs did realise that they aren't doing enough on their side, such as a tech savvy research participant who became aware that the reports she generates and stores once a year for tax purposes isn't enough and needs to download important data with every month end. In cases where a severe outage occurs, it was communicated that their cloud application provider should have database backups and business contingency plans in place. The two cloud application provider respondents had formal business continuity plans documented.

Only one of the participants in the Conventional group have lost data after a downtime event occurred. They have lost a few transactions on the stock receiving side and had to roll back to a previous backup. The corrupted databases of the two on-premise SMEs were restored successfully every time.

6.6 Cloud connectivity

The following section is investigating the effect of last mile connectivity, broadband technology options and connection latency on the adoption of SaaS-based ERP in an emerging economy. It evaluates recommended requirements to connect to a multi-tenant system, connectivity challenges and current experiences of participants connecting via South Africa's telecommunication infrastructure to their critical business systems.

6.6.1 Connectivity requirements

The literature review pointed out that to be able to connect to cloud-based ERP system, a reliable telecommunications infrastructure is a necessity and that South Africa has one of the most developed telecommunication networks in Africa.

According to Provider 1, the internet connection should be uncontended, or close to uncontended providing one with sufficient dedicated bandwidth. Data takes longer to upload and download when a line is shared by a large pool of users, i.e. contended line.

6.6.2 Connectivity challenges

Chapter four identified that last mile connectivity, broadband technology options and connection latency are three major non-functional cloud challenges.

The final infrastructure node or link between the individual customer and the telecommunications provider is referred to as last mile technology (Techopedia, n.d.). Due to high costs involved in installing telecommunication networks, certain areas, especially rural areas, might not have access to the most advanced bandwidth services. Franchise group “B” has franchises in Burgersfort and Tzaneen. Poor last mile technology of these two rural areas will have a negative impact on SaaS-based ERP adoption as explained later in this chapter.

SME participants are connected to the internet through ADSL, fibre and wireless communication broadband technologies. According to Provider 1, most of their customers have upgraded their bandwidth. They recommend fibre, not only for the uncontended bandwidth which provides the best connectivity experience in South Africa today, but also the advantage over copper theft and by being immune to lightning. Although ADSL is cheaper and easier to obtain, Provider 1 commented that ADSL is best effort only and not suitable for business use. 4G/LTE is another recommendation, it's however an expensive alternative and it might become unsustainable in the long run if it becomes oversubscribed.

Provider 1 shared that latency and not line speed is the biggest factor, it has a direct impact on user experience and productivity. Section 2.2.7.2 describes latency is the time it takes for the data to get through, i.e. the response-time. According to them, once fibre pools are shared 1:20 or 1:50, latencies will start to rise as the connection will become over contended. They therefore recommend uncontended bandwidth of 1:1 or at worst a 1:2. If temporarily in a new fibre pool, users should abandon the pool once it fills up to 1:5. A major challenge that Provider 1 pointed out is that when data capturers are used to previously process on an on-premise system, then change to cloud connectivity can be a major challenge. This provider agrees with

the literature review that latency should be as low as possible, hence the higher the response-time, the more annoyed and less productive end-users will become, especially data capturers.

They suggest a latency of “ideally 20ms and lower for power users or data processors, however other users can easily transact on lines with latencies up to 100 – 120ms”. Another important consideration is that latency shouldn’t fluctuate and be consistent as users will become irritated if the connection becomes slower during the day as more users are added.

Provider 2 agrees that latency is an issue, but they also added that legacy applications were not designed to be hosted remotely. According to them it boils down to system design, with true cloud you are working as native as possible and not working through multiple technologies, while legacy systems is likely to be built on a stack of technology. Systems that are written specifically for the cloud should be designed to take into account connectivity issues. When designing web pages, designers should as a rule of thumb keep lowest common denominator in mind. One should keep in mind that not everyone is equipped with the latest web browser, best device and super-fast connection thereby designing web interfaces that degrade gracefully (Niederst and Robbins, 2003). It’s important that designers and programmers of SaaS-based ERP should keep this in mind.

6.6.3 Connectivity experiences

In the previous section it was found that most of Provider 1’s clients had to upgrade their bandwidth technology. The same is true for the SME participants. In table 27, three of the four SaaS participants had to upgrade their bandwidth technology due to connectivity issues.

Group	Conventional Group				SaaS Group			
Solution	On-Premise		Hosted (PVT)	Hybrid (PVT+OP)	Public Cloud			
SME:	SME H	SME F	SME A	SME B	SME C	SME D	SME E	SME G
Previous bandwidth technology		Not known	ADSL	ADSL		ADSL	Wireless communication	ADSL
Current band-width technology	ADSL	Fibre	Fibre	Better ADSL	ADSL	Fibre	Upgraded Wireless communication	Fibre

Table 27: Bandwidth technology upgrades per SME

In figure 34, four of the six upgrades in this study was to fibre, while one participant could only upgrade their ADSL package as fibre was not available in their physical location. One participant upgraded the bandwidth of their wireless communication technology.

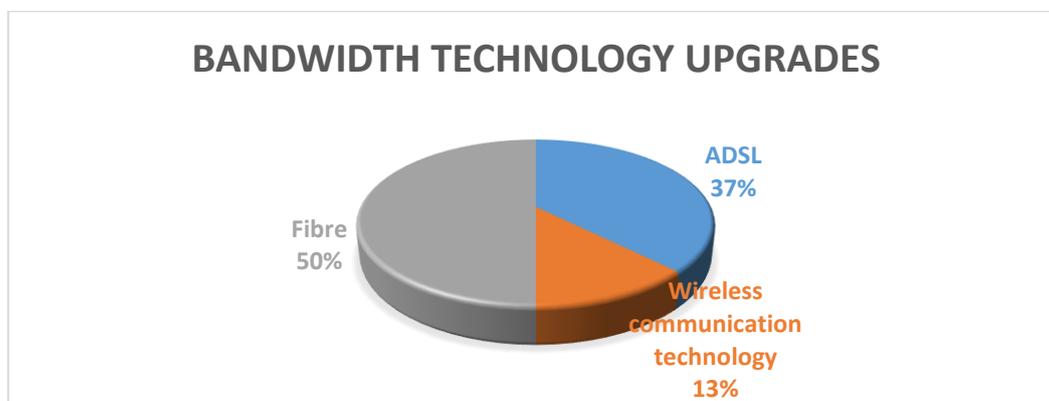


Figure 34: Bandwidth technology upgrades

Research participants rated their ISPs in chapter five. The following connectivity experiences were shared by participants in the Conventional and SaaS groups:

Conventional Group

The main benefit of connecting to an on-premise ERP system is that one connects via the local network which delivers outstanding response times. The local network isn't the cause of system performance issues at SME "F" and "H" discussed in the previous chapters.

SME "A" and "B" are both frustrated with the poor connectivity to their hosted applications. After upgrading their 4MB ADSL line to an uncontended 1:1 fibre line, SME "A" is still experiencing network dips and intermittent slow connection speed caused by network inconsistencies. Seeing that their ISP quality of service is still a big concern, their ISP provider has been summoned onsite a couple of times to run connectivity tests. After numerous requests, neither a solution nor the test results were provided to them.

SME "B" is a victim of the connectivity challenges discussed above. Poor last mile connectivity and high latency connections caused by outdated bandwidth technology infrastructures in the rural areas where some of their franchise operates in, was the main reason why SME "B1" (located in Polokwane) moved their hosted application back to on-premise. Franchise "B2" and "B3" who are currently operating on the private cloud, experience serious issues related to slow data capturing and printing speed, downtime, loss of sales and frustrations amongst customers, staff and management. These two distributed branches are located in Tzaneen and Burgersfort. According to the Telkom website, South Africa's leading wired and wireless telecommunications provider, the best bandwidth package one could get at the time of the

interview, was a 10 Mbps ADSL line in Polokwane, a 4Mbps line in Tzaneen and only 3G mobile communication technology in Burgersfort. These three towns didn't have VDSL, nor any fibre lines available and there was no ADSL in Burgersfort (Telkom, n.d.). The lack of a proper telecommunication infrastructure forced franchise "B1" to upgrade from a 2Mbps line to 10 Mbps ADSL line while being hosted and then to ultimately move their system back to on-premise.

SaaS Group

All four participants in this group had similar connectivity issues which now had an impact on their primary systems in the cloud. They all experienced huge improvements after upgrading their bandwidth technology.

SME "C" operates from the coastal town of Melkbosstrand and connects via a 10Mbps ADSL line. Telkom's website (n.d.) indicates that Fibre will be available soon, however residents are able to get up to a 40 Mbps VDSL line. The research participant explained that "there are times that the system and internet hangs, then we need to phone our ISP to reset the line". When the participant connects to the SaaS-based ERP system from, his 4G/LTE mobile technology provide a far better and faster system experience.

Since SME "D" upgraded to a 20Mbps fibre line they had far less connection issues and system processing is much more stable. The participant described their experience on the previous 2 Mbps ADSL line as "terrible" and often preferred to connect via a LTE mobile hotspot to get a better connection. Even though the fibre connection is much better, they still experience latency issues. A possible reason could be that their new fibre line is contended and shared by a large pool of users, however the issue is also on the cloud provider's side as system notifications inform cloud users that the provider is aware of speed issues and they are attending to the problem. In cases like these, the server performance and connectivity at the provider side could also impact the overall SaaS-based ERP performance.

When SME "E" initially subscribed to a 2 Mbps wireless communication technology, they too experienced slow internet speed, especially as more employees connected to the line. Latency still occurs after they upgraded to a 4 Mbps package, but not that often. SME "G" gave their fibre ISP a rating of 90% in section 5.3.2. When asked if it's very quick to move from one transaction line to another within the system, they downgraded the rating to 80%. It's unsure if SME "G" has an uncontended fibre line, but overall experience is much better compared to their previous ADSL line, "I never have to wait for anything actually, it's been a huge improvement".

In chapter five, SMEs the Conventional Group rated the support received from their ISPs 58% while SaaS-tenants rated their ISPs 65%. A change in ISP and bandwidth technology type reduced connectivity frustrations as the rating increased with 20% when SME “D” did a fibre upgrade.

6.7 Conclusion

The purpose of this chapter was to evaluate the effect cloud downtime and connectivity have on the adoption of SaaS-based ERP in an emerging economy.

SaaS-tenants fully understand that there will be cloud downtime, it shouldn't however have a negative effect on their business. It's therefore essential that cloud application providers, cloud hosting providers and ISPs schedule downtime to happen after-hours. To be able to plan around downtime, users need to be notified in advance. Scheduled downtime during office hours should be avoided as far as possible and if need may be, only as short as possible. It was found that unscheduled downtime within business hours and a severe cloud outage will have an effect on SaaS-based ERP adoption, it will have a far greater effect on a cloud providers' retention.

It was revealed that downtime is typically scheduled after-hours, at least once a month. Most often this is because cloud providers are doing planned system upgrades and server maintenance. On the upside, the server hardware and software is being maintained regularly. Some of the SMEs in the Conventional group experience unscheduled downtime during office hours, due to database locks, corrupted databases and outages at hosting providers, ISPs and the national electricity supplier. Participants in the SaaS group had little experience of unscheduled system downtime, much less than the Conventional group. In most cases unscheduled downtime was caused by the ISP's internet connectivity and not the application provider. Connectivity plays a critical role in Cloud ERP.

All four SMEs in the SaaS group are notified 24 to 48 hours in advance of scheduled downtime, which is either via a system notification or email sent by the provider. Both providers in this study are proactive and sent out emails to the main contact person at their SaaS sites. It was however found that a system notification is a more powerful medium as it reaches the entire SaaS-tenant user base. Downtime is normally stipulated in the SLA and when uptime is compromised, certain providers might give a credit or discount as compensation. Although one of the two cloud application providers do compensate their SaaS-tenants when downtime has been compromised, none of the SMEs in the SaaS group have been compensated or was aware if they are allowed to request a credit or discount on their next subscription. When a

cloud outage might occur, providers and customers should be prepared and have a business continuity plan in place. In this study it was found that most of the SME participants don't have explicit plans and don't take precautionary steps. Depending on the situation, the participants would usually operate manually and wait for the system to be back online and catch up. SaaS tenants were initially shocked with this question and realised that they aren't doing enough on their side. In cases where a severe outage occurs, it was communicated that their cloud application provider should have database backups and business contingency plans in place. The two cloud application provider respondents did have formal business continuity plans in place such as both onsite and offsite backups and data redundancy.

In both public and private cloud deployment models, a reliable telecommunications infrastructure is a necessity. Although it was found that South Africa's telecommunication network is considered as one of the most developed telecommunication networks in Africa, rural areas might not have access to the most advanced bandwidth services. Last mile connectivity, broadband technology options and connection latency were the reasons why one of the participants SMEs in this study was forced to migrate back to on-premise ERP.

Three of the four participants had to upgrade their bandwidth technology due to connectivity issues. Fibre was the preferred last mile connectivity choice; this option was however not available to all the participants. Upgrading to fibre had a positive impact on the adoption of SaaS-based ERP as it provided a better connectivity experience.

According to one of the providers, latency and not line speed is the biggest factor as it has a direct impact on user experience and productivity. They therefore recommend uncontended bandwidth. The second provider interviewed agreed that latency is an issue, but also added that it boils down to system design. According to them, systems that are written specifically for the cloud should be designed to take into account connectivity issues. Therefore, when designing SaaS-based ERP web pages, designers and programmers should as a rule of thumb keep the lowest common denominator in mind and designing interfaces that degrade gracefully.

It can be concluded that cloud downtime and connectivity therefore does have an effect on the adoption of SaaS solutions and that the user's experience of using network-dependant components in their existing landscape plays a huge role in the choice to move to SaaS-based ERP.

Chapter 7: Data Security and Data Privacy

7.1 Introduction

One of the central themes is that security is placed in the hands third parties when one is migrating to a public cloud deployment model. Section 2.2.6 of the literature review indicates that data security and data privacy have been identified as two major security risks for adopting SaaS-based ERP. The literature also shows that security in ERP is a cross-cutting concern as it has business (roles, responsibilities and separation of duties), application (access to functionality), data (access to data) and infrastructure (physical, server and network security) aspects.

The new SaaS landscape combines both internal and external components of corporate networks over a variety of secure and insecure networks. Several data security concerns have been identified, such as user authentication, authorisation and audits. These concerns raise questions such as: whether the user, device, or application is who it says it is; which functions and data the user or application is allowed to access; and what data was changed. Data privacy is an associated concern as it questions which external parties are allowed to see one's data. The traditional boundary changed; cloud ERP has introduced new network and web security issues demanding a change in conventional security defences. Several technologies have been employed to help with these concerns. To protect a company's SaaS-based ERP system against internal and external security breaches, the literature review has indicated that mitigation measures should cover six types of securities, namely: physical, transmission, storage, access, data and application security. It's also important to understand that security is about trading off risks and counter-measures. The higher the likelihood of a risk occurring and the bigger the scope of the damage, the more you would want to put security in place to prevent it. Often, a risk can't be completely mitigated but rather depends on how much risk you are willing to take. For example, to mitigate unauthorised access, one could remove all the user interfaces to external users but doing this might go contrary to the business purposes, like online banking. Security is therefore not merely putting in place measures that will take away all of the risk.

Security is also not just the responsibility of the cloud application provider. Although application providers have to build the necessary application security measures into their systems, the cloud business platform hosting provider is responsible to protect the server(s) on which the application is running. In addition, SaaS tenants have a responsibility to ensure that end-user security measures are in place and to educate their employees about the risks cloud ERP is exposed to.

Before evaluating whether local SMEs and providers are doing their part in securing their systems, tolerances for security breaches must first be tested to determine the impact it has on the adoption of SaaS-based ERP.

7.2 The impact of security breaches on SaaS-based ERP adoption

In the business scenario discussed in chapter five (table 26), research participants had to consider one of five mock-up multi-tenant ERP quotations or state if they rather would have preferred an on-premise or hosted application. Once the participant's decision was made, a new scenario was given to them to evaluate if they would still select the same quotation, select a quote from one of the other four SaaS-based ERP providers or switch to an on-premise or hosted application. Research participants were given a scenario to test moving important business data and processes to and from a platform that is less than secure.

Outcomes:

Currently, none of the SMEs or providers who participated in this study have been a victim of a data breach. It was found that most of the SME participants indicated that a security breach causes a serious consideration in changing their systems.

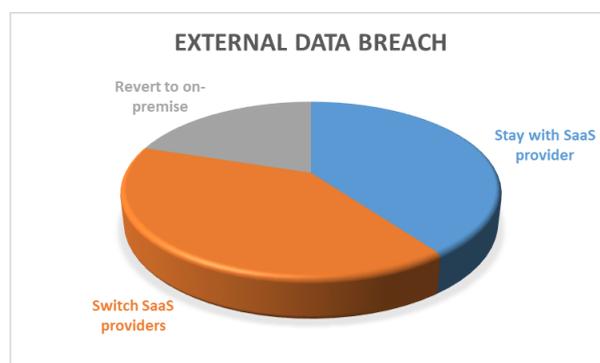


Figure 35: Effect of an external security breach

Figure 35 indicates that, while two out of five respondents will evaluate alternative SaaS-based ERP providers, a breach like this might be enough to force two participants back to an on-premise ERP system. Some participants may still stay loyal to their SaaS provider should a major security breach occur, due to their belief that their data would be of no value to external parties and therefore they have no cause for concern.

Interestingly, participants who are currently running on-premise ERP indicated that if they were in such a scenario, they would still prefer the cloud and only switch cloud providers. According to SME "F", "confidentiality to their information is critical", while SME "B" stated that the trust between them and their provider is broken. Two of the three SMEs who are currently on SaaS-

based ERP were unconcerned. SME “E” would still use the SaaS-based ERP system as “it could happen to anyone”, while the owner of SME “C” stated that “stuff like this happens every day and with the size of my company they won’t be able to do anything with my financial data”.

7.3 Internal and external security breaches

Are SMEs in emerging markets doing their part in fighting against internal and external security breaches? SaaS-tenants are also responsible for putting security-measures in place and to educate their system users about the risks to which cloud ERP are exposed.

Section 2.2.6.6 of the literature review states that SMEs who want to migrate their business software to the cloud should consult an expert in performing a pre-assessment and risk prevention of threats study. The literature, however, indicated that SMEs might not consider such a study as important or simply don’t have the financial and human resources for it. None of the participants in this study have done such an assessment prior to migrating to SaaS-based ERP as they didn’t consider it as important. Unsurprisingly, both of the cloud application providers have confirmed that SMEs aren’t focussed on security questions. Of course, larger organisations such as banks and insurance companies have dedicated staff and are very concerned about the risks. Smaller organisations just don’t have access to these rare, expensive skills.

When SMEs were asked if they are concerned about the security of their current ERP/Accounting application, or if there has been any incidents or data breaches whereby unauthorised access was gained, none of the participants could confirm this. Even after the recent data breach events at Facebook and Liberty financial solutions, security risks (for example, theft of client data, theft of identity, DoS attacks), although real and alarming, seem not to bother the smaller companies. Perhaps they think, being small, obscurity will protect them as criminals will go after bigger targets. Or perhaps they haven’t heard of their peers experiencing these risks.

7.4 SaaS tenants and Conventional Customer findings

The SMEs participating in this study are protecting their ERP system by enforcing usernames and passwords with every login. The usernames are created within the ERP system and are not being integrated with operating systems, any popular cloud services or social media platforms such as Google and Facebook. If a password is typed incorrectly multiple times, only one SaaS participant will be blocked temporarily. Of all the participants, the SaaS Group

will be locked out of the system if the session remains inactive for too long. Users of conventional ERP need to log out manually, if they even remember.

The literature review chapter mentions that it's advisable to set up account policies in the system. Typical SMEs aren't too concerned about security. Seven out of eight SMEs didn't use complex account policies and therefore never changed their passwords. SME "B" was the only company who configured the system so that some of the user password expire after a predetermined period. Most of the research participants don't know if the cloud provider is responsible for password policies or if they should manage it. Enforcing of password history, setting up of minimum password length and making use of password complexity are not being enforced by any of the SMEs.

Sharing of login credentials is a real problem among all participants. Five out of the eight SMEs interviewed share user accounts. Seeing that SMEs are smaller in size, people usually have a closer relationship with one another. Due to licensing restrictions, the bookkeeper in SME "A" can log in with the super user's account. At SME "B", user accounts are being shared by the sales reps, while a super user as SME "H" admits that "everyone here has got it, even the tea girl knows what my password is". Two user accounts are being shared by four employees at SME "C", as only two user licenses have been purchased. One of SME "G's" branches is family owned and so the director's wife may use his credentials when her user doesn't have the required access rights to perform a task. She says, "He's ok with it."

To view and use certain system functions, user security profiles have been configured at seven out of eight SMEs. SME "C", who shares two user accounts between four users, is the only SME that did not set up security profiles as both accounts have been set to full access, thereby exposing every setting, master and transaction record. Interestingly, two out of the seven SMEs haven't tested the data access rights in their systems. At SME "A", management does not specifically test the access of each user profile and commented that at go-live, end users have informed them if they cannot see data or are unable to do a specific task in the system and then it is added if really needed. Franchise "B" confirmed that user access profiles are more or less in place. Most importantly, the sale representatives can only see sales functionality and all of the non-financial users don't have access to financial data. This SME admits that the other user profiles need to be tested properly to verify that everyone can only see what they are supposed to see. The super user at SME "D" thinks that she might have checked the user profiles when they were created. At SME "F", new employees will usually start with a very limited access profile and over time more access is granted. Having years of experience with the specific on-premise system, the research participant at SME "F" is

confident with how the access profiles are configured. In this study, user profiles were configured for some of the SMEs to achieve Segregation of Duties (SoD). SME “A” was the only SME making use of built-in authorisation management whereby credit notes cannot be posted without supervisor approval. For the rest, SoD is mostly achieved by restricting access to certain functions. Although all eight SMEs are able to run audit logs reports which record changes on master and transactional data, only three out of eight SMEs really use it.

Granting access to service providers or third parties is another difficult area. Programmers and consultants often need complete access to be able to install and test software. Interestingly, none of the SaaS-based SMEs ever have the need for an external party to log into the system directly. In the Conventional Group, if SME “A”, “F” and “H” require support from their application provider, then access is only arranged via a TeamViewer session and not with direct system login details. SME “F” is precautionary and only provides viewing rights to external parties while SME “A” and “H” can see exactly what the external party is doing on their system via TeamViewer. Large corporates would manage this by using temporary super user login credentials which get managed very carefully.

In chapter four, SME “D” mentioned that it’s possible to share their SaaS-based accounting system with a third party such as an accounting firm. There is no need to have an additional license or even to create a system user; a precondition is that the third-party needs to be a user of a company that’s also on the same SaaS-based system. An individual need to be invited to join via a secure process which is not open to just anyone. This model provides an easy way for external parties to connect to the data in one’s system which does raise a concern. If the system of one of the linked third parties have been breached, it provides an easy way to access other systems unlawfully as well.

7.5 Cloud application provider findings

Data security is being treated as a top priority by the two application provider partners interviewed. The previous chapters show that Provider 1 may only host their SaaS-based ERP system at certain certified data centres, while Provider 2’s system is hosted in an international secure environment which is ISO 9001 approved. ISO 9001 is an industry managed regulatory requirement which was discussed in section 2.2.6.1.5 of the literature review. Provider 2 promises 256 Bit encryption throughout their software.

Both the SaaS-based ERP providers interviewed have user credential management built in directly into their systems. Provider 1's application can also be accessed via a Windows security (AD). Password complexity and policies can be specified per company.

Provider 1 did acknowledge that the technology used for their user verification is a bit outdated and that modern user authentication technology should be released within the next two years. They are aware how big the need is. According to Provider 1,

“some companies even go so far to having a business policy that says it's an immediate dismissible offence to give out your username and password to another colleague ... as much as that's correct, the fact that they should have an actual policy shows you where the vulnerabilities are. You know we are working with people. They talk, stand up from their PCs... walk away... and companies have to manage a policy like that.”

Provider 1 realise that there is a need for upgrading to more modern biometric-based secure access mechanisms such as face recognition and a biometric technique such as retina recognition. According to them, it is the only way to fully verify the identity of the person behind the keyboard. Provider 2 on the other hand is one step ahead. Biometrics is already incorporated into their SaaS-based ERP; it's possible to do retina and thumb print recognition provided that the necessary input devices are installed. Voice recognition isn't yet available. Provider 2 commented that voice recognition security is in its infancy. Although it is still developing, it's coming. Provider 1 questioned the practicality of voice recognition in ERP systems and indicated that “you should look at it always what's practical as oppose to what you should do to generate a reasonable degree of security?” Further research is required on this topic.

The SaaS-based ERP systems of these two providers will log users out of the system if an inactive session remains open. Both systems allow super user customers to configure their password complexity and create user role-based access. Provider 1 confirms that SoD isn't being used optimally by SMEs. In smaller companies, users have a bigger scope of job functions, as SME “F” also confirms. Audit trails are standard functionality.

7.6 Data privacy

Chapter two mentions that data might be disclosed to unauthorised individuals if strong security controls are not in place. Data privacy is another risk as SaaS-tenants are worried about their data being leaked. At the time of the interviews, none of the SMEs and providers

who were interviewed, nor anyone they know of personally, have experienced this yet. Data leaks shouldn't be taken lightly. Table 28 shows how the average South Africans have fallen prey to multiple data leaks.

No	Data leak	Source
1	Data of insurance customers disclosed through Liberty emails	(Niselow, 2018)
2	60 000 SA users on Facebook which had been improperly shared with a third party	
3	Personal records of 943 000 SA individuals and organisations from the ViewFines traffic fine platform that leaked online	
4	Personal details of over 60 million South Africans held by the Deeds Office.	
5	A flaw in Ster-Kinekor's booking website compromising up to 7 million South Africans	
6	An error in the email server of icanonline leaking personal information of several customers	(Otter, 2001)

Table 28: South Africans affected by data leaks

These statistics reveal how identity theft is classified as one of the fastest growing crimes. As per the previous section, both providers confirm that they have established mechanisms that will prevent data leakage.

7.7 Conclusion

One of the concerns raised is how a major security breach will affect the adoption of SaaS-based ERP.

The first aim of this chapter has been to determine if the experience of a substantial security breach will change a potential tenants' choice of SaaS provider or a choice of reverting to on-premise ERP. Local SMEs are cautious and risk-averse. If a cloud provider has been a victim of a security breach, most participants will take their business elsewhere. It has been found that the two of the four participants who would leave would still consider SaaS-based ERP and therefore evaluate alternative cloud providers, while another two would prefer to migrate to on-premise ERP. A major security breach would consequently have a significant impact on the adoption of SaaS-based ERP.

The second aim has been to determine if SMEs using ERP have security measures in place and if their end users are being educated on the security risks to which ERP systems are exposed. Security has a number of aspects from business to technology and infrastructure. Every party needs to contribute by presenting an unassailable secure front. Are SMEs bringing

their side? Unfortunately, many SMEs are rather lax in their security policies and practices and although challenge-response login is widespread, many other aspects are not, such as password strength and expiry; segregation of duties; and inspecting or reporting on audit reports. A small fraction of the participants reset user passwords, while more than half of these SMEs shared user login accounts. Although most of the SMEs in this study assign users to different security roles, not all these companies test the access rights of each user's security profile.

In the literature review, Sahin (2013) indicated that to maintain the cloud services, cloud providers generally have better hardware and technology than SMEs which enable them to provide more efficient secure systems. Both providers in this study see data security as one of their main priorities; their SaaS-based ERP systems are hosted in secure certified environments. Although both these participants acknowledge that modern biometric-based user authentication technology is more accurate in verifying who the user is, only one of them has already incorporated biometrics into their SaaS-based ERP system. Data privacy will be jeopardised if the security of the SaaS-based ERP system and its infrastructure are poor.

Chapter 8: Trust and change in business models

8.1 Introduction

Chapter eight investigates how the cloud has changed the business models of local application providers and how it has affected the formation of trusting relationships between providers and customers. Research participants working in senior positions at two local application provider partners have been questioned on changes in employee roles, technical skills, SLAs, operating hours and revenue streams. These are existing changes identified in the literature. The participants in this study have also identified a few new changes.

As aforementioned, by switching over to a multi-tenant ERP based system, companies aren't only sharing a platform with strangers, they are also giving up control of data security, data privacy and system availability to third parties and thereby are putting their trust in others. In chapter one, previous studies identify trust as the second most important adoption factor amongst SMEs in a developed economy who want to migrate to the cloud, while section 4.4.1 of this study found that trust is the third most important adoption factor amongst local participants. A second aim of this chapter is to determine how local SMEs view outsourcing control of their IT to cloud application providers, cloud business platform hosting providers and other third parties and consequently, whether they are concerned that their data is in the hands of third parties.

8.2 Changes in a cloud provider's business model

The cloud has introduced several transformations in the business models of cloud providers. Some of these changes have been identified in the literature while other new changes were identified by providers participating in this study, such as Provider 1 who had three years of cloud experience at the time of the interview. Their business model has changed dramatically, and they noted that it was a real challenge to incorporate a SaaS model into their business. They agree that there has been a big change in roles and the scope of roles of consultants. Account consultants are more productive because less time is spent on the roads as less on-site customer visits are required. Both an increase in productivity and a faster cloud implementation means that less staff is required by this provider. Provider 2 notes a change in employee morale. These changes are listed in figure 8.1 below.

Section 2.2.8.1 of the literature review states that the employee roles of application providers have changed significantly as there are more responsibilities, such as database

administration, security technicians, system administrators and many more. Previously, core roles were mainly to sell, implement and support on-premise software.

The IT landscape is constantly changing. New technologies such as cloud computing require specific set of skills. It's important for IT specialists to refresh their technical skills. In chapter five, Provider 2 indicates that when they have started with implementing cloud ERP, one of the major challenges experienced is that it is big learning curve for them as it is completely a different technology.

It has been discussed that cloud providers should try to stipulate uptime and availability percentages and that some might even offer their SaaS tenants a credit or a refund if uptime is compromised. Providers also need to stipulate the process around planned and unplanned downtime and how they will resolve temporary downtime or a complete downtime issue within a reasonable time period. Section 2.2.7.3.2 of the literature review indicates that if the cloud application is hosted on another provider's infrastructure, then the cloud application SLA is usually designed on top of the cloud provider SLA. In section 6.4 it has been found that only Provider 1 will compensate their customers if the system goes down.

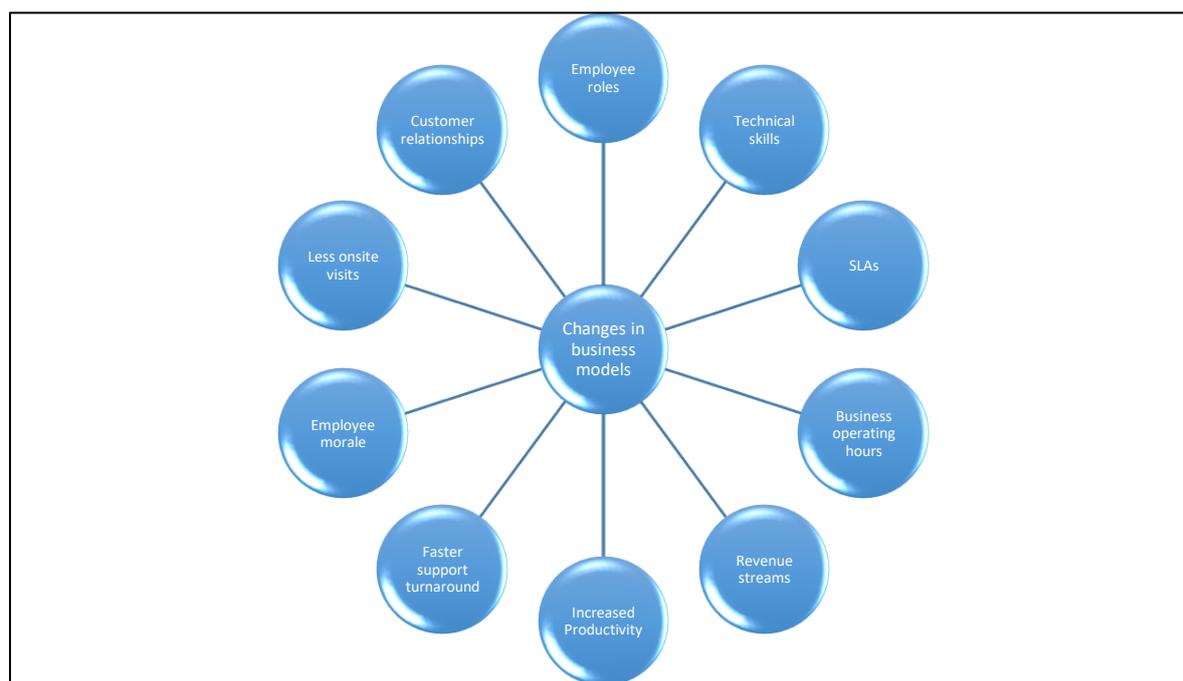


Figure 36: Ten changes SaaS has on a provider's business model

Changes in SLAs may impact a provider's operating hours. Section 2.2.8.1 of the literature review states that cloud providers need to support multiple clients around the globe and due to the nature of supporting multiple customers on one infrastructure, support can't be restricted to normal business hours. Chapter Five of this study shows that the availability of support is a significant factor when selecting a SaaS provider. When downtime is scheduled, chapter six

indicated that it had a negative effect on the SaaS-based ERP adoption by local participants if being scheduled within office hours. Section 6.3.3 finds that Provider 1 would usually schedule downtime for overnight or weekends, whereas Provider 2 is still more inclined to plan downtime during business hours with the approval of their clients.

Both ERP application providers have begun to move their businesses away from a declining interest in the traditional on-premise market to an increasing business in the cloud market. Traditional ERP is still a large part of their business. Although Provider 1 has noticed the shift towards cloud generated revenue, there is, however, a decline in ad-hoc billing, “cloud related revenue has less ad-hoc or bespoke consultant hours and tends to be more uniform inclusive monthly amounts”. Contrastingly, Provider 2 didn’t only experience a lot of frustration with the previous traditional ERP system they implemented for their customers, but it was also more of a financial liability for them. Although it’s still early, there is a noticeable shift in revenue streams as the new streams generated by their multi-tenant system have increased. According to the owner, “the beauty of the cloud model is that it’s a SaaS model, we don’t do a two million Rand deal at once; we do R350 000 deal this year and next year and the next”. Monthly rental fees make their cash flow planning easier because it’s recurring income.

This study has identified four new changes SaaS has on a provider’s business model. These are: improved productivity, faster support turnaround time, employee morale and customer relationships. According to Provider 1, one of the two huge benefits of SaaS is that account consultants are more productive because less on-site customer visits required means less time is spent on the roads. Another benefit this provider identifies is that the support turnaround time of a public cloud deployment model is significantly faster. A logical reason may be that tenants are on the same multi-tenant infrastructure, making it much quicker to connect to customer databases when resolving issues. Furthermore, by being on a homogenous infrastructure, it is much easier to determine the root of the problem if the issue is caused outside of the application. Hence, only the correction is applied to the whole infrastructure.

Feeling passionate about a software product one sells and implements is crucial as it builds confidence and enthusiasm in the applications, especially if the software package has a modern design and brings new challenges. Since Provider 2 started implementing the new SaaS-based ERP system nine months prior to the interview, a very positive outlook has emerged amongst the consultants. When asked how their business model has changed, it was said that “it gave our consultants hope” and “we found a product that we could implement and that we could be proud about and do great things and feel excited about and get passionate about”. A definite change in morale is apparent.

Lastly, this study has found that the cloud requires less onsite customer visits which also has an impact on customer relationships. Consultants can provide more support from remote locations. According to Provider 1, the challenge with being less on-site with customers is that some of their customers prefer personal contact, so they have to manage this. Chapter five finds that participant “F” requires regular face-to-face sessions and doesn’t want to be just a number in a support ticketing system. Provider 1 would still focus on maintaining strong relationships, and where explicit customer interaction isn’t always feasible, they will look at other ways to overcome it by virtual means.

The second part of the research question has been an investigation of how the formation of trusting relationships are affected by the cloud business model. Traditionally, onsite visits have helped build stronger personal relationships between a provider and customer. Trust is therefore built upon relationships. In a cloud model, Provider 1 indicates that the customer might never be formally introduced to the support consultant. Provider 1 finds that it is easier to form relationships when implementing on-premise systems as the relationship between the customer and consultants tends to be stronger. According to this provider,

“depending on the type of business model and the type of support required, trust is eventually built with the customer anyway, some site visits still occur and account consultants are still responsible for customer development roadmaps, but with smaller organisations that require little support it does become more challenging to build an explicit trusted relationship”.

For this provider, the relationship from a customer’s point of view has shifted from personal contact to “we’ve never had any issues”. In a cloud model, strong relationships are therefore formed differently, such as promising and proving uptime, secured data and keeping sensitive data private.

8.3 Creating and maintaining trust in SaaS

It has been repeatedly indicated that trust is one of the most important factors when deciding whether to switch to SaaS-based ERP. Trust comes with observed behaviour. The previous section reveals that in the cloud arena, trust in a modern sense, is built on software that’s fast and reliable, where one’s data is always available and secure.

The final research aim has been to determine how local SMEs feel about outsourcing control of their IT to cloud application providers, cloud business platform hosting providers and other third parties and whether they are unconcerned that their data is in the hands of external parties. It has been found that the majority of participants in this study are comfortable with

outsourcing control of their IT to cloud providers and that none of the existing SaaS tenants are concerned about the security of their current SaaS-based ERP applications. A research participant has interestingly observed that after discussing cloud uptime, security and trust in the interview, the participant couldn't believe they gave everything to their provider without careful consideration.

Research participants who are content with their company data in the hands of the other have been asked how they can convince others to make the switch. It has been found that all of the SaaS participants are satisfied and unconcerned. Some have not carefully considered all the risks before making the decision to migrate. Many of the participants only considered reputable providers and trusted brands. A sound SLA and local support is critical. Personal contact would be ideal, especially in more complex organisations.

In chapter five, research participants chose between five multi-tenant ERP quotes. None of the research participants prefer cost above an unfamiliar SaaS-based ERP application or where local support is unavailable, even if the system might be hosted at a well-known, state of the art cloud business platform hosting provider. Local SMEs tend to be cautious and risk adverse.

Do people trust a provider if they are certified? It has been mentioned that SaaS providers can gain stronger levels of trust if their system goes through a certification process by ensuring security controls are in place and that the system complies with regulations and conforms to ethical and auditing standards. In Chapter Seven, the local cloud application providers have given assurance that their SaaS tenants' data is stored in secure environments. Neither of the two cloud applications have been tested by ethical hackers or any external auditing third parties.

8.4 Conclusion

The first aim of this chapter has been to investigate how the cloud has changed the business models of local application providers and how it has affected the formation of trusting relationships between providers and customers. Ten changes in a cloud provider's model have been identified. Existing literature states that providers who have switched from providing traditional ERP to SaaS-based ERP will experience employee roles, technical skills, SLAs, operating hours and source of revenue streams. In this study new changes in the business model have also been identified. Research participants who are local cloud application provider partners experienced an increase in productivity, faster support turnaround, employee morale, fewer onsite visits and customer relationship changes.

It has been found that the cloud has an impact on how customer relationships are formed. Traditionally, onsite visits help with building stronger personal relationships between a provider and customer. Trust is therefore built more on established relationships. In the cloud model, fewer onsite visits means less personal contact which in turn means different interactions with clients and therefore different relationships. This affects trust somewhat. Harder work and a more proactive approach is required. In a cloud model, strong relationships are therefore formed differently, such as promising and proving uptime, secured data and keeping sensitive data private.

A second aim of this chapter is to determine how local SMEs feel about outsourcing control of their IT to cloud application providers, cloud business platform hosting providers and other third parties and if they are concerned that their data might be in the hands of external parties. It has been found that most of the SMEs in this study are comfortable with outsourcing control of their IT to cloud providers and that none of the SaaS tenants have concerns regarding the security of their SaaS-based ERP applications. Some were shocked with how easily they switched to the cloud without considering downtime, data security and data privacy concerns. None of the research participants were concerned that their company data is managed by third parties. Again, some have not carefully considered all the risks before making the decision to migrate. When convincing others to make the switch, participants have recommended considering only reputable SaaS providers who only implement trusted brands and provide good local support. Personal contact would be ideal, especially in more complex organisations.

It is not only SMEs in developed markets that see trust as a top cloud adoption factor, local SMEs also hold this view. Trust therefore plays an important role and is built over time, whether or not the software is reliable, fast and secure. One doesn't always know these things before one migrates. You can assume a well-known provider who others trust will be worthier of your trust. You can also be promised that they will respond to problems within a reasonable time period. The proof will however be in your experience.

PART 3: Epilogue

Chapter 9: Conclusions and Recommendations

9.1 Introduction

To conclude the research study and provide recommendations, Chapter nine provides a summary of the study with an overview of the research methodology; findings made in this study; trends and the meaning thereof; followed by the limitations and the significance of the results. The chapter will conclude by proposing additional research where gaps exist.

9.2 Summary of the study

9.2.1 Overview of the problem and methodology

The purpose of this qualitative study is to explore the adoption of SaaS-based ERP by SMEs operating in an emerging market, whereby control of mission critical systems is placed in the hands of cloud application providers and/or cloud hosting providers.

Many software applications designed for the individual are moving away from being installed on local desktops to being delivered as a service through the internet, i.e. SaaS. This trend can also be seen with software applications designed for organisations. A great deal of local and international organisations already moved some applications to the cloud and have integrated applications such as email, office suites, document storage, time tracking, expense management, CRM and payroll systems into their business. The final hurdle is to move ERP, the central software for most businesses, to be cloud-provided too.

Traditional ERP systems have always been too expensive for SMEs to acquire, implement and maintain. Fortunately for technological enhancements, cloud computing makes it possible for companies to rent ERP on a subscription, pay-as-you-go or usage basis. The business application as well as the server infrastructure is owned and maintained by cloud service provider(s). Cash flow, limited capital and human resource constraints make SaaS an ideal solution for SMEs. When renting SaaS-based ERP, organisations don't only use the business software, they also rent technical skills and expertise through support, best practice methodologies, integration and automation possibilities as well as a better hardware and network infrastructure.

Despite countless benefits of migrating to SaaS-based ERP, it also comes at a price. By hosting business software offsite, one is not in control of one's own IT anymore. Trusting third parties therefore plays a critical role as they have to be relied upon to run the application's infrastructure; to have it available when it is needed; to protect it from malicious internal and external attacks to ensure that one's data will not be shared with any unauthorised persons.

The question is then what really inhibits or encourages SMEs specifically to make the switch. In the literature review, previous studies have listed influencing factors on why SMEs should switch to the cloud computing and SaaS-based ERP as well as the main benefits one can achieve when migrating one's ERP to the cloud. Eight local SMEs have been interviewed to understand and analyse their experiences, of which four of these SMEs have already migrated to SaaS-based ERP. Two software partners who have experience in implementing both traditional and SaaS-based ERP have also been interviewed to understand the provision of SaaS from their perspective. Responses of these ten participants have been explored along the lines of certain identified themes and reveals interesting facts from which society can learn from.

9.2.2 Findings, trends and what it means in terms of literature

The goal of this research paper is twofold. Firstly, to determine the current usage of SaaS business applications by SMEs in South Africa, an emerging economy. Secondly, to determine the adoption of SaaS-based ERP; when both control and trust are placed in the hands of third-party providers to manage, protect and support the heart of a business.

The main themes that have emerged from the literature review are: data security, data privacy, system availability, internet connectivity, provider support and third-party trust. In order to provide answers to the main and supporting research questions, eight local SMEs and two local cloud application providers have participated in this study. These participants are mainly spread around the cities of Cape Town and Johannesburg, while one SME franchise had franchises in three remote areas: Polokwane, Tzaneen and Burgersfort. These SMEs specialise in different industries and are operating on a mix of on-premise-, hosted- and SaaS-based ERP systems. For the purpose of this research, SME participants have been divided into two groups: Conventional ERP and SaaS. Although the cloud application business partners have years of experience in traditional ERP, Cloud ERP is still new to them.

Prior to their existing on-premise ERP software, most SMEs in the Conventional group have used smaller single installation accounting packages and a combination of office suite spreadsheets on which to run their business. The majority of the SMEs in the SaaS group

have, however, mainly used office suite spreadsheets. Although the average age in business years of both groups is nine years, the complexity of SMEs in the SaaS group is much less. This study has found that on the basis of Roger's DOI theory, if any of these participants were to want to adopt a new SaaS business application, they would fall in the "late majority" adoption category. The peak of the innovativeness curve has been reached for SMEs partaking in this study as more than half of the business applications used in this research study are of a SaaS type.

Despite the belief that SaaS-based ERP systems are not as secure as conventional ERP systems and that cloud applications experience more downtime than on-premise systems, previous literature and experiences of these eight SME participants and two providers have proven the opposite. Participants in the SaaS group have little experience of unscheduled system downtime, much less than the Conventional group. In most cases, unscheduled downtime was caused by the ISP's internet connectivity and not the application or hosting provider. Connectivity plays a critical role in Cloud ERP. Bandwidth technology has a huge impact on the user's experience and that latency, rather than connection speed, plays a role. While most of the participants upgraded to fibre, poor last mile connectivity and high latency connections caused by outdated bandwidth technology infrastructures in rural areas are the main reason that one of the SMEs moved their traditional hosted application back to an on-premise ERP system. To maintain the cloud services, it has been found that cloud providers don't only have the expertise, they generally have better hardware and technology than SMEs which enable them to provide more efficient secure systems. Unfortunately, many SME participants have been rather lax in their security policies and practices and although challenge-response logon is widespread, many other aspects aren't, such as configuring password complexity, setting up access rights by segregation of duties and sharing of user credentials.

When new technology is released, it has been tested by the creators to a considerable degree. Once put in practice, challenges and basic requirements that have not been addressed will start to surface. Innovators and first adopters are therefore usually considered as guinea pigs. Cloud computing, as simple as it may sound, didn't happen overnight. Many of these first adopters will be able to show a list of growing pains they have had to go through, especially smaller organisations in developed markets. Cloud application and hosting providers have by now worked through most of these challenges and addressed critical requirements. Younger, more dynamic companies are embracing technology such as SaaS. Therefore, they leverage the technology to grow rapidly and become successful as they can now focus on what they do best instead of being distracted by trying to resolve in-house technological challenges.

Although local SMEs tend to be cautious and risk adverse, the cloud has been tried and tested. Application providers do however need to keep connectivity issues in mind when designing their applications. A key point is not to be ignorant. Firstly, upgrading one's bandwidth to a fibre connection is good, making sure that fibre with an uncontended bandwidth of 1:1 or at worst a 1:2 is available. Secondly, there are some qualities one should look for in a service provider. Some research should be done on potential cloud application providers and their hosting providers as there are some qualities one should look for in a service provider that would minimise the risk. Verify their policies around scheduled and unscheduled downtime, data security mitigation measures, who has access to your data and a review of how their clients rate their support. With this in mind and if one is doing one's part setting up a secure system, there is no reason not to step into the realm of cloud technology.

9.3 Limitations

Two limitations were identified in this research study. Firstly, none of the SaaS-based ERP tenants are located in remote areas. Chapter six demonstrates the negative effect that last mile connectivity, broadband technology options and connection latency has on some of the participants. Franchise group "B" has franchises in remote areas that need to connect to a hosted ERP system. Extremely slow internet connectivity and high latencies cause frustrations amongst system users and customers resulting in negativity and loss in revenue. Franchise "B1" has been forced to migrate back to on-premise ERP. It would have been ideal to have interviewed SaaS tenants from these areas as well, but due to resource, time and geographical constraints, this was unachievable.

Secondly, SaaS-based ERP providers interviewed in this study only serve a small pool of SaaS-based ERP tenants. Although interview invitations were sent out to SaaS-based ERP providers who serve a bigger customer base, only a handful replied to the invitation to participate. Their response was, however, too slow and eventually had to be excluded from the study.

9.4 Future works

In this study, the following four research areas have been identified where further research is required.

Cost is considered the most important adoption factor for European SMEs; however, it made the top three for only one of the local participants. Further research is required as to why cost

did not play a larger role locally. A possible reason could be that a provider's reputation and a software application of a well-known brand plays a more important role. Secondly, one of the observations made in this study is that the existing SaaS-based ERP participants are less dependent on a support desk than the on-premises participants. A further conclusion can be drawn that these SMEs are less complex and that a modern web-based ERP system could be easier to use and learn. Hence, usability has been voted as a top three adoption factor by three participants in the SaaS group. This research shows that the cloud has changed a provider's business model. However, it would be interesting to understand how cloud adoption changes the make-up of in-house technical skills, especially where there are IT departments in SMEs that are more complex in nature. One of the limitations of this study is that all the participants in the SaaS group are located within or close to cities. A case study of SMEs who use SaaS-based ERP with less than ideal connectivity would add additional value in terms of last mile connectivity, broadband technology and connection latency. The last area of further research that's required is the introduction of biometric and voice recognition as an authentication security measure. Further research is required to identify its feasibility, security and practicality.

9.5 Conclusion

Every year the Forbes Global 2000 and the Fortune 500 emphasise large corporations, admiring big corporates on a podium admiring their double-digit figures in sales, profit, assets and market value. However, smaller companies tend to be underestimated.

SMEs aren't only playing a major role in creating a healthy economic environment and uplifting the high unemployment rate but are also good indicators of what works on the ground, what products and services provide value for money and what makes a business succeed and grow rapidly. In this vein, SMEs in South Africa are early adopters of new mobile technology, innovative payment technologies and IaaS, PaaS and SaaS cloud services in areas such as document sharing and storage, email, payroll, expense management, time tracking and CRM. If SaaS-based ERP has been adopted by so many SMEs in developed markets, the question is then why SMEs in emerging markets, such as South Africa, are lagging the adoption of SaaS-based ERP.

As SaaS-based ERP systems are advancing through levels of technological maturity and the network of local partners who can provide support is growing, there is only one main stumbling block: unreliable last mile connectivity. Application software providers do however need to keep in mind that SaaS applications should be designed to take into account connectivity issues. The rest appears to be working and those who have already migrated are content.

Bibliography

Abor, J. and Quartey, P. (2010) Issues in SME Development in Ghana and South Africa. *International Research Journal of Finance and Economics*, 39, pp. 218-228.

Al-Johani, A.A. and Youssef, A.E. (2013) A Framework for ERP Systems in SME Based on Cloud Computing Technology. *International Journal on Cloud Computing: Services and Architecture*, 3(3), pp. 1-14.

Amin, S., Cárdenas, A.A. and Sastry, S. (2009) Safe and Secure Networked Control Systems under Denial-of-Service Attacks. In *HSCC* (469), pp. 31-45.

Awad, H.A. (2014) Cloud computing as an operational model for ERP services: Definitions and challenges. *International Journal of Innovation and Applied Studies*, 8(2), p. 499.

Azarnik, A., Shayan, J., Alizadeh, M. and Karamizadeh, S. (2012) Associated risks of cloud computing for SMEs. *Open International Journal of Informatics*, 1(1), pp. 37-45.

Baker, W., Goudie, M., Hutton, A., Hylender, C., Niemantsverdriet, J., Novak, C., Ostertag, D., Porter, C., Rosen, M., Sartin, B. and Tippett, P. (2010) *Verizon 2010 data breach investigations report*. Verizon Business., Available from: http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf [Accessed: 5 May 2017].

Baker, W., Goudie, M., Hutton, A., Hylender, C.D., Niemantsverdriet, J., Novak, C., Ostertag, D., Porter, C., Rosen, M., Sartin, B. and Tippett, P. (2011) *2011 data breach investigations report*. Verizon RISK Team, Available from: www.verizonbusiness.com/resources/reports/rp_databreach-investigationsreport-2011_en_xg.pdf, pp.6. [Accessed: 5 May 2017].

Balasubramanian, D. (2006) *QoS in cellular networks*. Washington University in Saint Louis. [Online]. Available from: http://www.cse.wustl.edu/~jain/cse574-06/cellular_qos.htm [Accessed: 10 March 2017].

Barnatt, C. (2010) *A brief guide to cloud computing: An essential guide to the next computing revolution*. London: Robinson Publishing.

Batra, R. (2011) *Deployment models* [Blog entry]. Available from: <https://networkingexchangeblog.att.com/enterprise-business/texas-style-bbq-and-cloud-value-propositions/#fbid=wmMDEFW0AGX> [Accessed: 4 April 2016].

Beal, B. (2012) *Microsoft expands its cloud ERP roadmap*. TechTarget. [Online]. Available from: <http://searchmanufacturingerp.techtarget.com/news/2240147039/Microsoft-expands-its-cloud-ERP-roadmap> [Accessed: 18 June 2015].

Beaman, K.V. (ed.) (2004) *Out of site: An inside look at HR outsourcing*. Austin: Rector-Duncan Inc.

Bento, R., Bento, A., Bento, A. and ISTM, M. (2015) How fast are enterprise resource planning (ERP) systems moving to the cloud?. *Journal of Information Technology Management*, 26(4), p. 35.

Bhardwaj, S., Jain, L. and Jain, S. (2010) Cloud computing: A study of infrastructure as a service (IAAS). *International Journal of engineering and information Technology*, 2(1), pp.60-63.

Bhatia, S. and Gupta, V. (2014) Role of Cloud Computing for Implementation of ERP in SMEs. *International Journal of Science and Research*, 3(11), pp. 2895-2898. [Online]. Available from: *IJSR*. <https://www.ijsr.net/archive/v3i11/U1VCMTQ2NA==.pdf> [Accessed: 4 November 2015].

Borella, M.S., Swider, D., Uludag, S. and Brewster, G.B. (1998) Internet packet loss: Measurement and implications for end-to-end QoS, In: *Architectural and OS Support for Multimedia Applications/Flexible*

Communication Systems/Wireless Networks and Mobile Computing., 1998 Proceedings of the 1998 ICPP Workshops. pp. 3-12.

Bryant, M. (2011) 20 years ago today, the World Wide Web opened to the public, *TNW News*, 6 August 2011. [Online]. Available from: <https://thenextweb.com/insider/2011/08/06/20-years-ago-today-the-world-wide-web-opened-to-the-public/> [Accessed: 23 January 2016].

Castellina, N. (2012) *SaaS and Cloud ERP Observations: Is Cloud ERP Right For You*. Aberdeen Group.

Castellina, N. (2013) *SaaS and cloud ERP observations: Enabling collaboration in the Midmarket*. Available from: <http://aberdeen.com/research/8754/ra-enterprise-resource-planning/content.aspx> [Accessed: 20 February 2017].

Chambliss, D.F. and Schutt, R.K. (2015) *Making sense of the social world: Methods of investigation*. 5th Ed. United States: SAGE Publications.

Ciaccia, C. (2017) *Dropbox Inc.* Investopedia. [Online]. Available from: <https://www.investopedia.com/articles/small-business/011817/dropbox-inc.asp> [Accessed 1 October 2017].

Columbus, L. (2014) *Gartner's ERP market share update shows the future of Cloud ERP is now*. Forbes. [Online]. Available from: <http://www.forbes.com/sites/louiscolumnbus/2014/05/12/gartners-erp-market-share-update-shows-the-future-of-cloud-erp-is-now> [Accessed 2 April 2015].

Community Editorial Team (2014) *DSL VS. Cable high-speed internet*. Comcast Business. [Online]. <https://cbcommunity.comcast.com/browse-all/details/dsl-vs.-cable-high-speed-internet> [Accessed 23 July 2015].

Cronje, J. (2018) Moody's keeps SA at investment grade, *Fin24*, 23 March 2018. [Online]. Available from: <https://www.fin24.com/Economy/just-in-moodys-keeps-sa-at-investment-grade-20180323> [Accessed: 23 June 2018].

Del Rey, J. (2017) Amazon's massive AWS outage was caused by human error. *Recode*, 2 March 2017. [Online]. Available from: <https://www.recode.net/2017/3/2/14792636/amazon-aws-internet-outage-cause-human-error-incorrect-command> [Accessed: 21 March 2017].

Duan, J., Faker, P., Fesak, A. and Stuart, T. (2012) Benefits and drawbacks of cloud-based versus traditional ERP systems. *Proceedings of the 2012-13 course on Advanced Resource Planning*. [Online] Available from: https://www.researchgate.net/publication/235759024_Benefits_and_Drawbacks_of_Cloud-Based_versus_Traditional_ERP_Systems [Accessed: 3 Noember 2015].

Durowoju, O.A., Chan, H.K. and Wang, X. (2011) The impact of security and scalability of cloud service on supply chain performance. *Journal of Electronic Commerce Research*, 12(4), pp. 243.

Earls, A. (2015) *Assessing cloud infrastructure provider performance in 2015*. TechTarget. [Online]. [http://searchcloudcomputing.techtarget.com/feature/Assessing-cloud-infrastructure-provider-performance-in-2015?utm_medium=EM&asrc=EM_ERU_53222473&utm_campaign=20160209_ERU%20Transmission%20for%2002/09/2016%20\(UserUniverse:%201937265\)_myka-reports@techtarget.com&utm_source=ERU&src=5478903](http://searchcloudcomputing.techtarget.com/feature/Assessing-cloud-infrastructure-provider-performance-in-2015?utm_medium=EM&asrc=EM_ERU_53222473&utm_campaign=20160209_ERU%20Transmission%20for%2002/09/2016%20(UserUniverse:%201937265)_myka-reports@techtarget.com&utm_source=ERU&src=5478903) [Accessed 24 March 2016].

Elragal, A. and El Kommos, M. (2012) In-house versus in-cloud ERP systems: A comparative study, *Journal of Enterprise Resource Planning Studies*, 2012(2012), pp. 1–13. [Online]. DOI: 10.5171/2012.659957. [Accessed: 6 March 2015].

- Emerging Money, (2012) *What is the difference between a developed, emerging and frontier market?*, Emerging Money, 11 May 2012. [Online]. Available from: <http://www.nasdaq.com/article/what-is-the-difference-between-a-developed-emerging-and-frontier-market-cm140649> [Accessed: 18 June 2016].
- Enterprisetech (2015) *Are you in control of your cloud data?* [Online]. Available from: <http://www.enterprisetech.com/control-cloud-data/> [Accessed: 9 February 2016].
- Epstein, B.J. and Jermakowicz, E.K. (2010) *WILEY Interpretation and Application of International Financial Reporting Standards 2010*. John Wiley & Sons. pp. 370.
- Erpclooudnews, (2010) *NetSuite Outage and Cloud Service SLAs*, ERP Cloud News. [Online]. Available from: <http://erpcloudnews.com/2010/04/netsuite-outage-and-cloud-service-slas/> [Accessed: 3 June 2015].
- Erpclooudnews, (2011) *Security Issues in Cloud ERP*, ERP Cloud News. [Online]. Available from: <http://erpcloudnews.com/2011/10/security-issues-in-cloud-erp/> [Accessed: 3 June 2015].
- Erpclooudnews, (2012) *Preparing for a Cloud Outage when running SaaS*, ERP Cloud News. [Online]. Available from: <http://erpcloudnews.com/2012/08/preparing-for-a-cloud-outage/> [Accessed: 3 June 2015].
- Faasen, J., Seymour, L.F. and Schuler, J. (2013) SaaS ERP adoption intent: Explaining the South African SME perspective, in: *Enterprise Information Systems of the Future*, Springer Berlin, Heidelberg, pp. 35-47.
- Färber, J. (2002) Network game traffic modelling. In: *Proceedings of the 1st workshop on Network and system support for games*. ACM. pp. 53-57.
- Fauscette, M. (2013) *ERP in the Cloud and the Modern Business*. [Online]. Available from: http://resources.idgenterprise.com/original/AST—0111292_ERP_US_EN_WP_IDCERPIInTheCloud.pdf. [Accessed: 29 July 2015].
- Ficco, M., Rak, M., Venticinque, S., Tasquier, L. and Aversano, G. (2015) *Cloud evaluation: Benchmarking and monitoring. Quantitative Assessments of Distributed Systems*, pp.175-199.
- Forrest, W. (2009) Clearing the air on cloud computing. *Discussion Document from McKinsey and Company*. [Online]. Available from: http://www.isaca.org/Groups/Professional-English/cloudcomputing/GroupDocuments/McKinsey_Cloud%20matters.pdf. [Accessed: 3 November 2015].
- Fripp, C. (2011) Cloud vs. Hosted services, What's The Difference? *IT News Africa*. 8 April 2011. [Online]. Available from: <http://www.itnewsafrica.com/2011/04/cloud-vs-hosted-services/> [Accessed: 30 October 2012].
- Garcia, J. (2015) *Back to basics: Cloud computing 101*. [Online]. Available from: <https://www3.technologyevaluation.com/research/TEC-report/TEC-2015-Report-Back-to-Basics-Cloud-Computing-101.html>. [Accessed: 10 October 2015].
- Gross, J and Veague, R. (2013) *3 Things You Must Know About Cloud ERP*
- Google Cloud Platform [no date] *Security and Compliance on the Google Cloud Platform*. [Online]. Available from: https://cloud.google.com/security/#google_security_model [Accessed: 18 June 2015].
- Gupta, S. and Misra, S.C. (2016) Compliance, network, security and the people related factors in cloud ERP implementation. *International Journal of Communication Systems*, 29(8), pp. 1395-1419.
- Heath, N. (2015) *AWS outage: How Netflix weathered the storm by preparing for the worst*. TechRepublic. [Online]. Available from: <https://www.techrepublic.com/article/aws-outage-how-netflix-weathered-the-storm-by-preparing-for-the-worst/> [Accessed: 20 September 2017].

- Heakel, R. (2017) *Emerging market economy*. Investopedia. [Online]. Available from: <http://www.investopedia.com/articles/03/073003.asp> [Accessed: 30 September 2017].
- Herstermann, C., Montgomery, N. and Pang, C. (2010) *Magic quadrant for ERP for Product-Centric Midmarket Companies*. [Online]. Available from: <http://sme.news-sap.com/files/2011/01/SAP-vol2art5.pdf> [Accessed: 20 September 2011].
- Huston, G. (2003) Measuring ip network performance. *The Internet Protocol Journal*, 6(1), pp. 2-19.
- Iol, (2016) Capitec leads ranking of best banks, *Independent media*, 16 March 2016. [Online]. Available from: <http://www.iol.co.za/business/companies/capitec-leads-ranking-of-best-banks-1998212> [Accessed: 11 April 2016].
- Iol, (2018) Icasa may slash data prices today, *Independent media*, 26 April 2018. [Online]. Available from: <https://www.iol.co.za/business-report/technology/icasa-may-slash-data-prices-today-14659071> [Accessed: 23 June 2018].
- Jackson, F. and Barth, A.F. (2008) Protecting High-Security Web Sites from Network Attacks. in: *Proceedings of the 17th International World Wide Web Conference (WWW 2008)*
- Jain, R. (2006) Quality of Service (QoS) in Data Networks. [Handout]. Washington University in Saint Louis. Saint Louis.
- Joch, A. (2015) *ERP cloud services reach a new level of maturity*. TechTarget. [Online]. [http://searchmanufacturingerp.techtarget.com/feature/ERP-cloud-services-reach-a-new-level-of-maturity?utm_medium=EM&asrc=EM_ERU_47612889&utm_campaign=20150917_ERU%20Transmission%20for%2009/17/2015%20\(UserUniverse:%201751806\)_myka-reports@techtarget.com&utm_source=ERU&src=5426698](http://searchmanufacturingerp.techtarget.com/feature/ERP-cloud-services-reach-a-new-level-of-maturity?utm_medium=EM&asrc=EM_ERU_47612889&utm_campaign=20150917_ERU%20Transmission%20for%2009/17/2015%20(UserUniverse:%201751806)_myka-reports@techtarget.com&utm_source=ERU&src=5426698) [Accessed: 28 September 2015].
- Kim, W., Kim, S.D., Lee, E. and Lee, S. (2009) Adoption issues for cloud computing. In *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia*. ACM. pp. 2-5.
- Koehler, P., Anandasivam, A., Dan, M.A. and Weinhardt, C. (2010) Cloud Services from a Consumer Perspective. in: *AMCIS*, pp. 329
- Kosasi, S., Harsono, A. and Yuliani, I.D.A.E. (2014) A Survey of the Latest IT Trends of Cloud Software-As-A-Service. in: *Proceeding of the Electrical Engineering Computer Science and Informatics*, 1(1), pp. 18-24.
- Kothari, C. and Garg, G. (2014) *Research Methodology: Methods and Techniques*, New Age Publishers
- Landy, J. and Hakhinian, M. (2014) *Securing Cloud Computing for Enterprise Collaboration*, Intralinks
- Lang, J. (2018) High data costs continue to hamper SME growth, *Moneyweb*, 19 May 2018. [Online]. Available from: <https://www.moneyweb.co.za/news/south-africa/high-data-costs-continue-to-hamper-sme-growth/?cn-reloaded=1> [Accessed: 23 June 2018].
- Lapan, S.D., Quartaroli, M.T. and Riemer, F.J. (eds.) (2012) *Qualitative research: An introduction to methods and designs*, San Francisco: Wiley, John & Sons.
- Ledford, J. (2014) *How Secure Is Your Cloud-based ERP System?*. [Blog entry] Available from: <http://it.toolbox.com/blogs/inside-erp/how-secure-is-your-cloudbased-erp-system-64403> [Accessed: 23 April 2015].
- Linthicum, D. (2015) *Creepy cloud horror stories to keep IT up at night*. TechTarget. [Online]. Available from: http://searchcloudcomputing.techtarget.com/tip/Creepy-cloud-horror-stories-to-keep-IT-up-at-night?utm_medium=EM&asrc=EM_ERU_53304256&utm_campaign=20160211_ERU%20Transmissi

on%20for%2002/11/2016%20(UserUniverse:%201942422)_myka-reports@techartget.com&utm_source=ERU&src=5479697 [Accessed: 24 March 2016].

Mahara, T. (2013) PEST-Benefit/Threat Analysis for selection of ERP in Cloud for SMEs. *Asian Journal of Management Research*, 3(2), pp. 365-373.

Makkar, M. (2012) EaaS-ERP as a service. *Journal of Information and Operations Management*, 3(1), pp.141-145.

MapCustomizer (2018). [Image] Available from: <https://www.mapcustomizer.com/> [Accessed 7 Sep. 2017].

Marcus, E. and Stern, H. (2003) *Blueprints for high availability*. 2nd ed. Indianapolis: John Wiley & Sons. ISBN 0-471-43026-9. [Online]. Available from: <https://imcs.dvfu.ru/lib.int/docs/Networks/Administration/Blueprints%20for%20High%20Availability,%200Second%20Edition.pdf>. [Accessed: 12 March 2017].

Mattison, J.B. and Raj, S. (2012) *Key questions about cloud computing ERP*. [Online]. Available from: https://www.accenture.com/t20151009T133552__w_/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_5/Accenture-Key-Questions-About-Cloud-Computing-ERP.pdf [Accessed: 23 April 2015].

M-Brain (previously Global Intelligence Alliance) (2012) *Business Perspectives on Emerging Markets 2012-2017*. [Online]. Available from: <http://www.slideshare.net/GIAGroup/business-perspectives-on-emerging-markets-20122017> [Accessed: 4 April 2016].

McCarthy, K. (2016) NetSuite hacker thrown in the cooler for a year, fined \$124,000, *The Register*, [Online]. Available from: https://www.theregister.co.uk/2016/06/06/netsuite_hacker_jailed_fined_124k/ [Accessed: 21 September 2017].

Mell, P. and Grance, T. (2012) *The NIST definition of cloud computing*. [Online]. Available from: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [Accessed: 16 April 2016].

MyBroadband (2015) Best ADSL ISP speeds in South Africa. *MyBroadband*. [Online]. Available from: <https://mybroadband.co.za/news/adsl/136488-best-adsl-isp-speeds-in-south-africa.html> [Accessed: 2 March 2017].

MyBroadband (2016a) Highest average ADSL and Fibre speeds in South Africa. *MyBroadband*. [Online]. Available from: <https://mybroadband.co.za/news/broadband/149759-highest-average-adsl-and-fibre-speeds-in-south-africa.html> [Accessed: 2 Mar. 2017].

MyBroadband (2016b) Top 10 fastest ADSL ISPs in South Africa. *MyBroadband*. [Online]. Available from: <https://mybroadband.co.za/news/adsl/171789-top-10-fastest-adsl-isps-in-south-africa.html> [Accessed: 30 May. 2018].

MyBroadband (2018) Average speed of South Africa's top ISPs. *MyBroadband*. [Online]. Available from: <https://mybroadband.co.za/news/broadband/254601-average-speed-of-south-africas-top-isps.html> [Accessed: 30 May. 2018].

Niselow, T. (2018) Five massive data breaches affecting South Africans, *Mail & Guardian*, 19 June 2018. [Online]. Available from: <https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans> [Accessed: 24 Aug. 2018].

Nair, A. (2012) *Layers of cloud computing* [Blog entry]. Available from: <http://connected2moodyprogrammer.blogspot.co.za/2012/09/what-is-cloud-computing.html> (Accessed: 4 April 2016).

- Neuman, W. L. (1997) *Social research methods: Qualitative and quantitative approaches*. Needham Heights, MA: Allyn & Bacon.
- Niederst, J., Robbins, J.N., (2003) *Learning Web design: a beginner's guide to HTML, graphics and beyond*. O'Reilly Media Inc., pp. 46.
- Nielsen, J. (1998) *Nielsen's Law of Internet Bandwidth*. [Online]. Nielsen Norman Group. Available from: <https://www.nngroup.com/articles/law-of-bandwidth/> [Accessed: 31 August 2017].
- Nielsen, T. (2014) *Security - whether in the cloud or the closet - must be a priority!*. [Blog entry] Available from: <https://www.jmark.com/security-cloud-closet-priority/> [Accessed: 12 January 2017].
- Nolle, T. (2015) *Learn from Amazon, Google when you build a private cloud*. TechTarget. [Online]. Available from: [http://searchcloudapplications.techtarget.com/tip/Learn-from-Amazon-Google-when-you-build-a-private-cloud?utm_medium=EM&asrc=EM_ERU_53019320&utm_campaign=20160203_ERU%20Transmission%20for%2002/03/2016%20\(UserUniverse:%201930758\)_myka-reports@techtarget.com&utm_source=ERU&src=5477298](http://searchcloudapplications.techtarget.com/tip/Learn-from-Amazon-Google-when-you-build-a-private-cloud?utm_medium=EM&asrc=EM_ERU_53019320&utm_campaign=20160203_ERU%20Transmission%20for%2002/03/2016%20(UserUniverse:%201930758)_myka-reports@techtarget.com&utm_source=ERU&src=5477298) [Accessed: 8 February 2016].
- Oates, B. (2006) *Researching information systems and computing*. London: SAGE.
- OECD (2010) *OECD Information Technology Outlook 2010*. Paris: OECD.
- Otter, A. (2001) Privacy infringements could cost icanonline millions, *ITWeb*, 30 July 2001. [Online]. Available from: <https://www.itweb.co.za/content/lwrKx73JBnnvmg1o> [Accessed: 24 Aug. 2018].
- Pang, C., Dharmasthira, Y., Eschinger, C., Brant, K.F. and Motoyoshi, K. (2013) *Market share analysis: ERP software* [Online]. Available from: <https://www.gartner.com/doc/2729518/market-share-analysis-erp-software> [Accessed: 4 January 2017].
- Pearson, S. (2009) Taking account of privacy when designing cloud computing services. in: *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*. IEEE Computer Society. pp. 44-52.
- Peng, G. and Gala, C. (2014) Cloud Erp: A New Dilemma to Modern Organisations?. *Journal of Computer Information Systems*, 54(4), pp.22-30.
- Perimeter security* [no date] The IT Law Wiki. [Online]. Available from: http://itlaw.wikia.com/wiki/Perimeter_security [Accessed: 10 May 2017].
- Prouty, K. (2011) *Aging ERP-When Old ERP is Too Old*. Aberdeen Group.
- Prouty, K. and Castellina, N. (2011) *Mobility in ERP 2011*. Aberdeen Group. [Online]. Available from: <http://hosteddocs.ittoolbox.com/02967054ramobilityinerpkp15nsp.PDF> [Accessed: 4 January 2017].
- Reddy, T.B., Karthigeyan, I., Manoj, B.S. and Murthy, C.S.R. (2006) Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions. *Ad Hoc Networks*, 4(1), pp.83-124.
- Reeves, D., Blum, D., Watson, R., Creese, G., Blakley, B., Haddad, C., Howard, C., Manes, A.T., Passmore, D. and Lewis, J. (2009) *Cloud Computing: Transforming IT*. Utah, Burton Group publication, pp. 84047-4169.
- Robb, D. (2016) *11 Cloud ERP Solutions to Consider*, Enterprise Apps Today. [Online]. Enterpriseappstoday.com. Available from: <http://www.enterpriseappstoday.com/erp/11-cloud-erp-software-options-1.html> [Accessed 13 February 2017].
- Rodrigues, J., Ruivo, P., Johansson, B. and Oliveira, T. (2016). Factors for Adopting ERP as SaaS amongst SMEs. *Information Resources Management Journal*, 29(4), pp.1-16.
- Rogers, E.M. (2003) *Diffusion of innovations*. 5th ed. New York: Free Press

- Romeo, J. (2014) *Finding peace of mind with cloud-based ERP*. TechTarget. [Online] Available from: <http://searchmanufacturingerp.techtarget.com/feature/Finding-peace-of-mind-with-cloud-based-ERP> [Accessed: 18 June 2015].
- Rouse, M. (2014). *Segregation of duties (SoD)*. TechTarget. [Online]. Available from: <http://whatis.techtarget.com/definition/segregation-of-duties-SoD> [Accessed: 15 May 2017].
- Rudo, P. (2011a) *How Cloud Computing Affects HIPAA Compliance*. Enterprise Features. [Online]. Available from: <http://www.enterprisefeatures.com/how-cloud-computing-affects-hipaa-compliance> [Accessed: 24 April 2016].
- Ryan, E. (2012) *The evolution of accounting software: past, present and future*. ASA. [Online]. Available from: <http://www.gaaaccounting.com/the-evolution-of-accounting-software-past-present-and-future> [Accessed: 27 January 2016].
- SouthAfrica.info, (2012) *South Africa's telecommunications*. [Online]. Southafrica.info. Available from: <http://www.southafrica.info/business/economy/infrastructure/telecoms.htm#.VxH7azB96Ul#ixzz45yeetjEN> [Accessed: 16 April 2016].
- Sanmorino, A. and Yazid, S. (2013) DDoS attack detection method and mitigation using pattern of the flow, In: *Information and Communication Technology (ICoICT), 2013 International Conference of*, IEEE. pp. 12-16.
- Sahin, I. (2006) Detailed review of Rogers' diffusion of innovations theory and educational technology-related studies based on Rogers' theory. *TOJET: The Turkish Online Journal of Educational Technology*, 5(2).
- Sahin, N.Y. (2013) *Cloud ERP Security: Guidelines for Evaluation*. Department of Computer and Systems Sciences, Sweden: Stockholm University.
- Schubert, P. and Adisa, F. (2011) *Cloud Computing for Standard ERP Systems: Reference ERP Framework and Research Agenda*, Koblenz: University Koblenz-Landau.
- Seethamraju, R. (2014) Adoption of software as a service (SaaS) enterprise resource planning (ERP) systems in small and medium sized enterprises (SMEs). *Information systems frontiers*, 17(3), pp.475-492.
- Sfondrini, N., Motta, G. and You, L. (2015) Service level agreement (SLA) in Public Cloud environments: A Survey on the current enterprises adoption. In *Information Science and Technology (ICIST), 2015 5th International Conference on* (pp. 181-185). IEEE.
- Shafik, R.A., Rahman, M.S. and Islam, A.R. (2006) December. On the extended relationships among EVM, BER and SNR as performance metrics. In *Electrical and Computer Engineering, 2006. ICECE'06. International Conference on* (pp. 408-411). IEEE.
- Shin, S., Park, H., Choi, S. and Kwon, W. (2007) Packet Error Rate Analysis of ZigBee Under WLAN and Bluetooth Interferences. *IEEE Transactions on Wireless Communications*, 6(8), pp.2825-2830. [Online]. Available from: <https://iic.kangwon.ac.kr/wp/wp-content/uploads/2015/07/Packet-Error-rate-Analysis-of-ZigBee-Under-WLAN-and-Bluetooth-interferences.pdf> [Accessed: 11 March 2017].
- Smith, M. (2014) *The Future Of Integrating ERP And Applications In The Cloud*. [Blog entry] Available from: <http://Ventanaresearch.Com/Blog/Commentblog.aspx?Id=4500#Sthash.Pnkz0jbq.Dpuf> [Accessed: 1 July 2015].
- Snider, E. (2013) *Cloud ERP: Growth, Trends and Outlook*. TechTarget. [Online]. Available from: http://bitpipe.computerweekly.com/detail/RES/1369238405_548.html [Accessed: 23 April 2015].

South Africa. Department of Justice and Constitutional Development (2013). *Act No. 4 of 2013: Protection of Personal Information Act*. Government Gazette. Cape Town. [Online]. Available from: www.justice.gov.za/legislation/acts/2013-004.pdf [Accessed: 24 June 2016].

Spathis, C. and Constantinides, S. (2004) Enterprise resource planning systems' impact on accounting processes, *Business Process Management Journal*, 10(2), pp. 234–247.

Srinivas, J., Venkata Subba Reddy, K. and Moiz Qyser, A. (2012) Cloud computing basics. *International Journal of Advanced Research in Computer and Communication Engineering*, 1(5).

Staeher, L. (2010) Understanding the role of managerial agency in achieving business benefits from ERP systems, *Information Systems Journal*, 20(3), pp. 213–238.

Stal, M. (2002) Web services: beyond component-based computing. *Communications of the ACM*, 45(10), pp.71-76.

Sultan, N.A. (2011) Reaching for the “cloud”: How SMEs can manage. *International journal of information management*, 31(3), pp. 272-278.

Techopedia, (2017a) Network latency. [Online]. Available from: <https://www.techopedia.com/definition/8553/network-latency> [Accessed: 2 March 2017].

Techopedia, (2017b) Transmission Security. [Online]. Available from: <https://www.techopedia.com/definition/25857/transmission-security-transec> [Accessed: 10 May 2017].

Techopedia, [no date] Last Mile Technology. [Online]. Available from: <https://www.techopedia.com/definition/26195/last-mile-technology> [Accessed: 17 Aug 2018].

Telkom, [no date] *Telkom Technology Coverage & Store Locator Map* Telkom. [Online]. Available from: <https://secure.telkom.co.za/today/ucm/> [Accessed: 7 October 2017].

Thomas, D. (2006) A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, 27(2), pp.237-246.

Thomas, D. and Hodges, I. (2010) *Designing and managing your research project*. London: SAGE.

Trimi, S., Lee, S., Olson, D. and Erickson, J. (2005) Alternative means to implement ERP. *Industrial Management & Data Systems*, 105(2), pp.184-192.

Your cloud success requires network strength (2015) The Hispanic American Publishing Group. [Online]. Available from: http://www.idglat.com/afiliacion/whitepapers/Your_Cloud_Success_Requires_Network_Strength.pdf?tk=/ [Accessed: 24 March 2016].

Verizon (2016) *2016 Data Breach Investigations Report*. Data Breach Investigations Report. [Online]. Available from: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf [Accessed: 5 May 2017].

Verizon (2017) *2017 Data Breach Investigations Report*. Data Breach Investigations Report. [Online]. Available from: https://www.verizonenterprise.com/resources/reports/2017_dbir_en_xg.pdf [Accessed: 30 May 2018].

Velte, A.T., Velte, T.J., Elsenpeter, R.C. and Elsenpeter, R.C. (2010) *Cloud computing: a practical approach*. New York: McGraw-Hill. pp. 1-55.

Woodie, A. (2015) *Has cloud ERP reached a tipping point?* [Online]. Available from: <http://www.itjungle.com/tfh/tfh041315-story02.html> [Accessed: 23 April 2015].

WorkPool, (2016) *What is POPI? The Protection of Personal Information (PoPI) Act explained*. [Online]. Available from: <https://www.workpool.co/featured/popii/> [Accessed: 24 June 2016].

“YungChou” (2010) *Cloud computing for IT pros (2/6): What is cloud* [Blog entry]. Available from: <https://blogs.technet.microsoft.com/yungchou/2010/12/17/cloud-computing-for-it-pros-26-what-is-cloud/> [Accessed: 4 April 2016].

Zargar, S.T., Joshi, J. and Tipper, D. (2013) A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, 15(4), pp.2046-2069.

Zscaler (2013) *What Does the Cloud Mean to Enterprise Security?*. Zscaler.

Appendixes

Appendix A

Appendix B