Justifications for the Implementation of Shadow IT Solutions by Functional Departments in an Organisation

A minor dissertation submitted in partial fulfilment of the requirements for the award of the degree of:

Masters in Commerce: Information Systems

University of Cape Town
By
Joshua Magunduni (MGNJOS002)

Faculty of Commerce
University of Cape Town
2019

Supervisor: Professor Wallace Chigona

3 October 2019

DECLARATION

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to and quotation in this thesis *Justifications for the Implementation of Shadow IT Solutions by Functional Departments in an Organisation*
3. from the work(s) of other people, has been attributed and has been cited and referenced.
4. This thesis *Justifications for the Implementation of Shadow IT Solutions by Functional Departments in an Organisation*
5. I have not allowed, and will not allow, anyone, to copy my work with the intention of passing it off as his or her own work.

Signature: ….Signed by candidate Date: October 3, 2019

Student: Joshua Magunduni (MGNJOS002)

PREFACE

Part of this thesis appeared in the ICT and Society 2018 conference; the comments received from the scholars and the acceptance improved the final version of this thesis.

PUBLICATION (CONFERENCE PAPER)

Magunduni, J., & Chigona, W. (2018). Revisiting Shadow IT research: What we already know, what we still need to know and how do we get there? In *ICTAS 2018*. Durban, South Africa: IEEE.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

Abbreviations

AME	Application Management Elements policy (at EPZA)
CIO	Chief Information Officer
EPZA	Pseudonym for the multinational company used in this study
ERP	Enterprise Resource Planning
EUC	End User Computing
IS	Information Systems
IT	Information Technology
KPI	Key Performance Indicators
SIT	Shadow IT

Acknowledgements

- I want to thank my supervisor Professor Wallace Chigona for his generosity and tremendous academic support.

- To my financial sponsors', thank you so much for helping me realise my dreams. It means a lot to me.

- I want to pay special thanks to all the respondents who took part and spent valuable time in the interviews for the study.

- I would also like to thank my family (*Mom, Dad, Phathutshedzo, Thendo and Gift*) for prayers, moral and emotional support. I dedicate this thesis to you.

- To all my friends, colleagues, and mentors. Thank you so much for the great support.

- Above all, I thank God for His grace and mercy.

"*Be strong and courageous. Do not be afraid; do not be discouraged, for the Lord your God will be with you wherever you go*." **Joshua 1: 9**

Abstract

Background: The implementation of information technology (IT) solutions by end-users, while bypassing organisational laid-down IT acquisition and implementation processes and controls, poses a significant challenge for most organisations. This phenomenon, which is known as Shadow IT (SIT), has major financial, legal and security implications for the organisation. Studies indicate that even when organisations implement IT policy to minimise the implementation of SIT, end-users may still find innovative ways to bypass the IT department when implementing unsanctioned software.

Purpose of the research: The objective of this study was to investigate how end-users (functional departments) who implement SIT in organisations justify their actions. The term Justification refers to the techniques employed by a social actor to indicate that their deviant behaviour is actually reasonable. Understanding justifications for SIT is essential for IT managers since they can understand them as justification and not confuse them with other phenomena and at the same time they can devise appropriate strategies to counter them. IT Managers who are not aware of the justifications for SIT may implement measures which may not be effective in curbing the phenomena.

Design/Methodology/approach: The study adopted an interpretivist approach. The study was guided by the 'Neutralisation Theory' from the social deviance discipline. The study examined whether an organisation had an IT policy which prevents end-users from implementing SIT, and also assessed the 'Neutralisation' techniques employed by end-users to justify SIT. The study adopted a case study approach based on a South African office of a multinational organisation. The study collected data through (i) semi-structured interviews with end-users from different functional departments who were involved with implementation of SIT and (ii) documentation (IT policy and email correspondences). The study adopted the purposeful sampling (snowball) technique to target the employees who were involved with the implementation of SIT. A total of 13 respondents were interviewed. The data was analysed using thematic analysis approach.

Findings: The organisation did not have an IT policy which prevented functional departments from implementing SIT. Instead, it had a policy which allowed functional departments to implement their own IT solutions as long as they inform the IT department to assess the software application for potential risks and compatibility with the existing landscape. Most respondents did not use Neutralisation techniques to justify the implementation of SIT due to the policy which allowed them to implement their own IT solutions. Nevertheless, the respondents who employed Neutralisation techniques mainly used *Denial of responsibility, Denial of injury and Appeal to higher loyalties* to justify SIT.

Originality/contribution: The study contributed to the justifications of SIT literature when it explored the concept of SIT in a corporate company setting – as opposed to earlier studies that used quantitative methods and experiments when exploring the concept of SIT. The study also makes a further contribution to literature by investigating SIT in an environment where functional departments are allowed to implement their own IT solutions – this was not explored by previous studies on Justification of SIT. The study also contributes to the practice where there is a need by IT management to minimise SIT by providing awareness of Neutralisation techniques which may be employed by functional departments to justify SIT. Through the understanding of the Neutralisation techniques, IT managers could make sound decisions when implementing measures to minimise SIT

1. Introduction

The study used a case of a multinational petroleum company to analyse how end-users justify the implementation of unsanctioned information technology (IT) solutions in their respective department. This chapter presents the research background, the problem statement, the research aim and objectives, the context of the study, the research approach, the research propositions, the research assumptions, research gaps, summary of the findings and contributions – and concludes with an outline of the chapters.

1.1. Background

Shadow Information Technology (SIT) is a significant challenge for most organisations and has major financial, legal and security implications (Chua et al., 2014; György & Cleven, 2012). The definition of SIT is systems "…*operating at the fringes of an organization, they covertly replicate the data and functionality of formally sanctioned systems*" (Behren, 2009, p. 124). Previous research suggests a myriad of the motivations behind the implementation of SIT which include a lack of trust and satisfaction with sanctioned systems (Mallmann & Maçada, 2016). Further, the improved technical knowledge of end-users, coupled with access to cloud-based IT solutions, may influence the creation of SIT (Gozman & Willcocks, 2015; Zimmermann & Rentrop, 2014). Occasionally, end-users implement SIT as workaround solution to address the limitations and issues related to formally sanctioned systems (Thatte & Grainger, 2010). For instance, most enterprise resource planning (ERP) software is highly integrated and has complicated user interfaces (Behrens, 2009; Gorla et al., 2010; Urus et al., 2011). So, end-users might decide to implement SIT from third-party vendors to simplify the process and to improve the user experience (Behrens, 2009; Gorla et al., 2010).

More recently, some literature has offered contradictory findings on SIT. Although it is generally associated with risks, some scholars argue that SIT could be beneficial to organisations (Behrens, 2009; Silic, 2015). Some of the benefits are related to increased end-user creativity and innovation, and also improved business performance (Silic & Back, 2014; Tambo & Bækgaard, 2013). Furthermore, end-users can identify and implement IT solutions which meets their specific needs (Haag et al., 2015; Silic & Back, 2014).

1.2. Problem statement and research question

SIT may benefit organisations by improving end-user creativity and business performance (Haag & Eckhardt, 2015; Silic & Back, 2014; Tambo & Bækgaard, 2013). At the same time, the use of SIT may expose organisations to many challenges such as unreliable reports, poor software maintenance, and enterprise architecture risk. These challenges may make organisations to become vulnerable to malware and viruses, make incorrect inferences due to poor reports, and have duplication of software functionalities – which may lead to financial losses.

Earlier studies on SIT explored the benefits of SIT, the risks of SIT, and internal controls to manage SIT. However, the topic of justifications for SIT by end-users is under-explored, and only a few scholars have attempted to explore this phenomenon (Haag, Eckhardt, & Schwarz, 2018). The term Justification refers to "*statements of a social actor that claim the positive value of a behaviour when it is called into question*" (Haag et al., 2018,p1). Understanding justifications for SIT is essential for IT managers to make sound decisions when implementing measures to minimise SIT. Managers who are not aware of the justifications for SIT may implement measures which may encourage end-users to implement SIT instead of reducing SIT (Haag et al., 2018). While scholars from many disciplines have used different theories to study justifications, IS scholars have studied Justification from the Neutralisation theory (Haag et al., 2018).

This study explored how end-users justify the implementation of SIT solutions. The following research question guided the study:

How do functional departments (end-users) justify the implementation of Shadow IT solutions?

1.3. Research aims and objectives

The objective of this study was to investigate the justifications used by end-users who have employed SIT. The study proposed the following sub-objectives:

1. To examine whether the IT department has implemented any form of IT policy or any IT control – to prevent functional departments from implementing SIT solutions.
2. To assess Neutralisation techniques used by end-users to justify the implementation of SIT.

1.4. The context of the study

The study was conducted in a multinational petroleum company located in Cape Town South Africa. For ethical reasons, the organisation is anonymised as EPZA. EPZA was ideal for this study because of the history of SIT solutions in the organisation which caused duplicate and inefficient IT functionalities. The company also has a policy (Application Management Elements), which outlines the responsibilities of the IT department and a functional department during the implementation of a new software application.

The AME policy offers three options for managing new software applications: dedicated software management, partnership software management, and arms-length software management. Software applications that fall under the dedicated software agreement are implemented and maintained exclusively by the IT department. Software applications that fall under the partnership agreement are implemented and maintained through a collaboration between a functional department and the IT department. Software applications that fall under the arms-length agreement are implemented and maintained exclusively by a functional department. However, the IT department requires all software that falls under the arms-length agreement to go through the IT architecture review – so that the IT department can assess the software applications with regard to compatibility with the IT infrastructure and mitigating security threats.

Nevertheless, over the years, most functional departments have bypassed the IT department when implementing software under the arms-length agreement. They had not notified the IT department to perform the architecture review prior to implementations. Consequently, the company experienced significant financial losses due to the duplication of software functionality across the company, and redundant and inefficient IT solutions.

1.5. Research approach

This study adopted the interpretivist research paradigm. The study was guided by the Neutralisation Theory from the social deviance discipline. The case-study approach was used and suitable for this study because there are few studies on SIT and the researcher needed to gain an in-depth understanding of SIT. The study employed a single case-study approach. In

terms of sampling, the study adopted purposeful and snowball sampling to target employees who were involved with the implementation of SIT.

Data were collected using semi-structured interviews and documentation (IT policy and email). A total of 13 respondents were interviewed. The data were analysed using the thematic analysis approach. The combination of semi-structured interviews and documentation was adopted to improve and strengthen the research findings and to gain a deeper understanding of the concept of SIT (Dubé & Paré, 2003). Due to the limited amount of time available to complete the study, the researcher used cross-sectional studies.

1.6. Identified gaps in literature

Over the years, scholars have adopted theories from other disciplines to enhance the understanding of SIT. The use of theories from other disciplines is a consequence of the interdisciplinary nature of the field of Information System. One of the theories used in the SIT literature is the justifications theory from the social deviance discipline (Haag & Eckhardt, 2015; Haag et al., 2018; Silic, Barlow, & Back, 2017). This study identified and attempted to fill the following research gaps relevant to the justifications for SIT literature.

- *SIT policies.* While previous studies on justifications for SIT examined organisations with strict IT policies for managing SIT (Barlow, & Back, 2017), there was less attention to organisations which permits end-users to implement their own IT solutions. As a consequence, there is little knowledge of how end-users use justification techniques in an environment where end-users are allowed to implement their own IT solutions.
- *Focus on qualitative studies.* Previous studies on justifications for SIT are based on quantitative methods. While quantitative studies were able to identify neutralisation techniques, they were not able to provide details on how they were employed. Qualitative studies are essential because researchers can describe the qualities and characteristics of the phenomenon – which is not easily achievable through the use of quantitative methods (Boyce & Neale, 2006). As a result, a study based qualitative methods bring novelty to the justification of SIT research.

1.7. Research assumptions

Prior to the data collection process, the researcher held the following assumptions regarding SIT at EPZA: The researcher assumed that:

- There is a policy that prevents functional departments from implementing SIT solutions.
- End-users who implemented SIT solutions experienced guilt and shame due to bypassing the IT policy.
- End-users who implemented SIT respected teams or functional departments, which follow the IT department policies.
- End-users who implemented SIT could differentiate between people (teams) who can be victimised and those who cannot be victimised.
- End-users who implemented SIT had a desire to conform to what appeared to be acceptable to wider society at EPZA.

However, some of the assumptions were different from the results, and there are more details in the discussion chapter.

1.8. Summary of research findings

EPZA did not have an IT policy which prevents functional departments from implementing SIT. Instead, the company had a policy which allows functional departments to implement their own IT solutions as long as they informed the IT department to assess the application for potential risks and compatibility with the existing landscape. Consequently, most respondents did not use justifications techniques to justify the implementation of SIT. The respondents who employed justifications techniques used *Denial of responsibility, Denial of injury and Appeal to higher loyalties* to justify SIT.

1.9. Contribution and benefits of the study

The study contributed to the justifications of SIT literature when it explored the concept of SIT using qualitative methods in a corporate company setting – as opposed to earlier studies that used quantitative methods and experiments when exploring the concept of SIT. The study also makes a further contribution to literature by investigating SIT in an environment where functional departments are allowed to implement their own IT solutions – this was not explored by previous studies on Justification of SIT. The study also makes a contribution to

practice where there is a need by IT management to minimise SIT by providing awareness of Neutralisation techniques which may be employed by functional departments to justify SIT. Through the understanding of the Neutralisation techniques, IT managers could make sound decisions when implementing measures to minimise SIT.

1.10. Overview of the chapters

The remainder of the dissertation is structured as follows:

Chapter 2: Reviews existing literature on SIT. The chapter begins with a brief discussion of the definitions and terminologies used in SIT literature. Then the chapter synthesises earlier findings – to find current themes in the existing literature.

Chapter 3: The chapter focuses on the Neutralisation theory; the theory adopted for the study.

Chapter 4: Presents the research design. First, the chapter presents a brief background of the research methodology. Next, it justifies the sampling strategy and sampling technique used in the study. The chapter presents the data-collection technique and data-analysis methods. Finally, the chapter presents issues of reliability and validity related to this study – as well as research access and research ethics.

Chapter 5: Presents the research findings to answer the research question. The chapter identifies and presents emerging themes in the data.

Chapter 6: Discusses the research findings to answer the research question. The chapter presents emerging themes that were identified through the research.

Chapter 7: Concludes the research by reflecting on findings obtained from the study and the contribution made to the body of knowledge and practice. The chapter also presents the limitations of the study and a possible research direction for future studies.

2. Literature Review

This chapter presents a review of the literature review on SIT. The chapter begins with a brief discussion of the definitions and terminologies used in SIT literature. Then the chapter synthesises earlier findings – to find current themes in the existing literature.

2.1. Introduction

IT solutions managed and used by functional departments – outside of the knowledge of the IT department – are a major concern for most organisations. This phenomenon is known as SIT. Usually, end-users implement SIT as workaround solutions to address the limitations and issues related to formally sanctioned systems (Thatte & Grainger, 2010). For instance, most companies use enterprise resource planning (ERP) software to manage their daily operational activities. However, such systems are integrated and have complicated user interfaces (Behrens, 2009; Gorla et al., 2010; Urus et al., 2011). As a result, end-users might implement SIT solutions from third-party vendors to improve the user experience and to introduce additional functionalities not provided by sanctioned systems (Behrens, 2009; Gorla et al., 2010; Urus et al., 2011).

Earlier studies have different perspectives on the implementation of SIT in organisations. Some scholars argue that end-users might implement SIT as a form of resistance to sanctioned systems. Some claim that end-users implement SIT for innovation through process simplification and improved reporting – while others specified that support from management encourages end-users to implement SIT. In this section, these perspectives are observed and classified according to the following themes: causes of SIT, benefits of SIT, risks of SIT, and internal controls to manage the implementation of SIT.

2.2. Defining Shadow IT

Despite the growth of the literature on SIT, scholars have inconsistently defined the term SIT. The use of different terminologies and a different understanding of the concept ‘SIT’ lead to the lack of a precise definition. For example, DV. Kerr et al., (2007) defined Feral systems as “an information system [computerised] that is developed by individuals or groups of employees to help them with their work, but is not condoned by management nor is part of

the corporation's accepted information technology infrastructure …" (p. 142). Behrens (2009) defined Shadow Systems as systems "operating at the fringes of an organization, they covertly replicate the data and functionality of formally sanctioned systems."(p. 124). Spierings et al. (2011) defined Feral information systems as "… any information technology artefact that an End User employs instead of the mandated Information System" (p. 1). Buchwald and Urbach (2012) defined Un-Enacted Projects "as unofficial projects that have never been subject to any official evaluation process but do exist" (p. 2). Zimmermann et al. (2014) defined Shadow IT as "… business processes supporting IT systems, IT services and IT staff. They are deployed autonomously within the business departments by IT users" (p. 1). Myers et al. (2016) defined a shadow IT system "… as those that are not approved or monitored by the IT department" (p. 17).

Although there is some consensus among scientists that a SIT solution is created by end-users without involving the IT department, researchers have not yet found a standard definition for SIT. The inconsistencies in defining SIT result from scholars using different terminologies. In most cases, these terminologies reflect the perspectives of the researcher towards SIT. For instance, scholars who are against SIT solutions usually use negative terminologies such as Rouge IT and Feral systems (Chua et al., 2014; Spierings et al., 2011). Then again, some scholars use more neutral terminologies, such as Shadow systems, Shadow IT and un-enacted projects (Blichfeldt & Eskerod, 2008; Buchwald & Urbach, 2012; Silic, 2015). The lack of consistent use of terminologies is problematic, especially for the new researcher, because they might not be able to build upon existing research (Kopper & Westner, 2016; Lund-Jensen et al., 2016).

For this study, the researcher adopted the term 'Shadow IT', because the latest literature on the subject uses this terminology, as well as the definition by Behrens (2009) – which states that SIT solutions are systems "operating at the fringes of an organization, they covertly replicate the data and functionality of formally sanctioned systems" (p. 124).

2.3. Types of Shadow IT

SIT covers a broad spectrum of unauthorised technologies implemented and used by end-users in companies. These tools or technologies might fall under the following categories, although the list is not exhaustive: utility applications, greynet applications, and un-enacted

projects (Buchwald & Urbach, 2012; Silic & Back, 2014). Utility software helps users to clean and improve the performance of their computers such as codecs and pc cookie cleaners; and greynet applications are installed by end-users who rely on the company's network to operate – for instance, peer-to-peer file sharing software (Silic & Back, 2014). End-users may implement SIT in the form of undercover projects. Such IT projects are not controlled or managed by the in-house IT department, but rather, third-party IT vendors are employed by end users to help with the development and implementation of such software (Behrens, 2009; Buchwald & Urbach, 2012). This study focused on SIT solutions implemented by end-users with assistance from third-party vendors.

2.4. Classification of Shadow IT

SIT solutions are classified according to the criticality and level of risks they exert on the business. The criticality of a SIT system depends on the level of integration of a SIT with the sanctioned system (Fuerstenau & Rothe, 2014). So, the more integrated the SIT solution is with the authorised system, the higher the criticality. SIT solutions are also classified according to the level of risks they exert on the company. For instance, SIT solutions that use the corporate network (e.g. cloud solutions) are considered to have higher security risk than SIT solutions that do not require the network to operate (Silic & Back, 2014).

2.5. Phenomena confounded with Shadow IT

2.5.1. Bring your own device.

Bring your own device (BYOD) is not SIT. Although there is a thin line between SIT and BYOD, the concept of BYOD is limited to employees bringing their mobile devices to the workplace for personal use or work-related activities. It is important to note that employees might bring their devices and then not create SIT solutions (Schalow, Winkler, Repschlaeger, & Zarnekow, 2013). On the other hand, SIT includes undercover IT projects funded and run by the functional departments themselves, without involving the IT department (Buchwald & Urbach, 2012). It may also include IT systems and other IT-related activities deployed by end-users across the organisation – without involving the IT department for support or guidance (Buchwald & Urbach, 2012; Zimmermann & Rentrop, 2014).

2.5.2. End-user computing

SIT is not end-user computing (EUC). EUC deals with empowering the end-users who do not have any form of technical knowledge to implement basic applications. These applications are usually not complicated and are only limited to minor configurations (Chua et al., 2014). Although some scholars have associated SIT with end-user computing, for instance, Friedrich and Julia (2016) – other scholars such as Rentrop and Zimmermann (2012) have argued that EUC should not be confused with SIT. EUC is monitored and managed by the IT department. However, with SIT, the IT department is not aware of IT implementations.

2.6. Reasons for implementing Shadow IT

The literature suggests that if end-users are dissatisfied with sanctioned systems, they are most likely to implement SIT (Behrens, 2009; György & Cleven, 2012; Spierings et al., 2011). Usually, the factor causing dissatisfaction is the misalignment between the IT department's objectives and the functional department's objectives (György & Cleven, 2012). For instance, the implementation of customised functionalities to systems such as ERPs is a costly endeavour which involves the development of a solution, as well as maintenance (Bob-Jones, Newman, & Lyytinen, 2008). IT departments might decide to reduce customisation to drive down costs. Although less customisation on ERP systems might drive down the system upgrade cost, this might be costly to end-users – since the system would not meet their operational requirements due to a lack of functionality needed for their business process (Behrens, 2009; Bob-Jones et al., 2008) For that reason, end-users might explore other options and implement SIT solutions (Chua et al., 2014; Kerr & Houghton, 2008; Spierings et al., 2011).

On the contrary, while sanctioned systems such as ERPs might have the existing functionality necessary to meet the requirements of end-users, these are usually not user-friendly (Behrens, 2009). In most cases, end-users have to navigate different screens to perform a simple task, and this might reduce the productivity of employees (Behrens, 2009). Therefore, end-users might consider implementing additional IT solutions from third-party suppliers to supplement the existing systems to improve productivity and the user-experience (Beimborn & Palitza, 2013; Thatte & Grainger, 2010). Studies indicate that SIT solutions thrive in environments where top management supports the development and implementation of such systems (Spierings et al., 2011). Usually, if management creates an environment that is conducive to

the creation of SIT through rewards systems, end-users might feel empowered to implement such systems (Kerr & Houghton, 2008).

While IT processes and methodologies used by IT departments to deliver IT services are designed to improve software quality – they might also delay the delivery of services to end-users (Behrens, 2009; Buchwald & Urbach, 2012). Usually, end-users perceive these processes as rigid and incapable of meeting changing requirements (Behrens, 2009; Buchwald & Urbach, 2012). Therefore, due to tight deadlines and the need to improve productivity, end-users might decide to implement SIT (Gozman & Willcocks, 2015; Kretzer, 2015; Spierings et al., 2011).

Employees might implement SIT as a form of resistance to sanctioned systems. Usually, sanctioned systems replace legacy systems – which affect the culture and the behaviour of employees (Kerr & Houghton, 2008). During the transition stage to the new system, IT departments might fail to provide adequate change management and training, which could increase resistance from end-users (Kerr & Houghton, 2008). As a result, end-users might choose to implement SIT to cope with the change (Berente, Yoo, & Kalle, 2008; Kerr & Houghton, 2008). Table 2.1 summarises the reasons for adopting SIT.

Table 2.1: Summary of reasons for adopting Shadow IT

Reasons for SIT	Explanation
Data Quality	Inaccurate data, incomplete data, and delay in transaction processing are some of the reasons that could cause end-users to implement SIT solutions.
System Quality	Complex, sanctioned software might cause end-users to implement SIT.
Complex Infrastructure	The integration of multiple systems into a sanctioned software solution might result in slow response times of the system and increase the possibilities of downtimes, which might cause end-users to implement SIT.

2.6.1. Data quality

Good data quality is essential, and without clean data, the company's performance might be impacted (Alshawi, Missi, & Irani, 2011) . Managers and other decision-makers rely on the reports that are based on data generated from sanctioned systems (Gorla et al., 2010). However, some of the challenges linked to data quality are inaccurate data, incomplete data, and delay in transaction processing. These issues are more apparent in highly integrated systems such as ERPs. Incorrect and incomplete data captured by employees could impact on the subsequent business processes in the ERP system and may have negative financial

implications to the company (Urus et al., 2011). To manage the data quality challenges, functional departments may implement SIT.

2.6.2. System quality

System quality is measured regarding user-friendliness, maintainability, and performance (Gorla et al., 2010). Systems such as ERPs have sophisticated user interfaces, which are hard to learn and operate (Behrens, 2009). Due to the complexity of the user interface, employees are most likely to use other software such as spreadsheets to perform transactions such as cashbook entries and to generate reports (Urus et al., 2011). To cope with system quality issues, functional departments may implement SIT.

2.6.3. Complex infrastructure

The complexity of IT infrastructure is also a concern. Systems such as ERPs exist in complex infrastructures that comprise different hardware, software, and networks. The integration of the ERP system with the external system is made possible through interfaces, which might cause slow response times of the system and also downtimes (Urus et al., 2011). To overcome issues relating to complex infrastructure companies may implement SIT.

2.7. Benefits of Shadow IT

Studies indicate that end-users implement SIT to unleash creativity and innovation (Behrens, 2009; Kerr & Houghton, 2008). Innovation is made possible by integrating SIT solutions with sanctioned systems for process simplification and also to improve the user experience (Behrens, 2009; Kerr & Houghton, 2008). The focus on end-user experience is to improve productivity and to meet deadlines by avoiding reworks caused by committing mistakes (Behrens, 2009; György & Cleven, 2012; Silic, 2015; Silic & Back, 2014; Urus et al., 2011). Employee creativity is essential for the company – because more company objectives are met at a low cost (Chua et al., 2014; György & Cleven, 2012; Silic, 2015). Table 2.2 summarises the benefits of SIT:

Table 2.2: Summary of benefits for Shadow IT

Benefits	Explanation
Creativity and Innovation	End-users may implement IT solutions that meet their specific requirements.
Improves Business Performance	SIT may improve the turnaround time for delivering IT services. Thus, end-users may not wait for the IT department to approve their project or allocate to a budget for the project. Instead, they can procure or

	develop the IT services that meet their specific needs, while bypassing red tape.

2.7.1. Benefits on employee's creativity and innovation

Innovation is essential because it enables quick response to the changing requirements of business users (Tambo & Bækgaard, 2013). Innovative companies are more competitive in the market than those that do not focus on innovation (Silic, 2015). Innovation focuses on meeting the strategic and operational needs of a company (Behrens, 2009). The characteristics of an innovative IT solution are relative advantage, compatibility, trialability, complexity, and observability (Behrens, 2009). Relative advantage refers to the ability of a SIT solution to possess unique functionality – which is not available on the systems provided by the internal IT department. Compatibility refers to the ability of a SIT solution to match the user's requirements. Complexity refers to the user-friendliness of a SIT solution. Trialability refers to the freedom to prototype and try a SIT solution, without fully committing the financial resources. This is essential because it enables the company to minimise the overhead costs required by the IT department when developing new solutions (Kretzer & Maedche, 2014). Observability refers to the attractiveness of the functionality offered by the SIT solution.

Furthermore, it is essential that a SIT solution has the innovative characteristics to bridge a gap between the user's requirements and the services offered by the IT department. Users can engage with a third-party service provider and procure only the services they require to meet their specific needs (Behrens, 2009). This procurement method is usually common with cloud-based solutions (Haag, 2015). Technically savvy users may also innovate by developing solutions such as macros and databases to fulfil their requirements (Zimmermann et al., 2014).

2.7.2. Benefits on business performance

SIT solutions improve business performance through continuous alignment, fast delivery of IT services, and nurturing trust between the IT department and users. Continuous alignment is achieved through users developing or procuring IT services that are necessary for their specific requirements and which are not catered for by the internal IT department (Dimmler, 2013). SIT solutions improve the turnaround time for IT service delivery. Thus, users do not have to wait for the IT department to approve their project or allocate to a budget for the project. Instead, they can procure or develop the IT services that meet their specific needs, without going through the red tape (Haag, 2015; Silic & Back, 2014). Trust can be natured

when the IT department discovers the SIT solutions; the IT department might consider new ways to collaborate and communicate with users in respect of the SIT solution (Dimmler, 2013). The IT department can also decide to evaluate and assess the SIT solution to identify whether it meets the strategic objectives that improve business performance (Rentrop & Zimmermann, 2012b).

2.8. Risks associated with Shadow IT

While SIT is considered as a source of creativity and innovation, several scholars have criticised this perception and have indicated that this could introduce risks to a company. For instance, Shumarova and Swatman (2008) and Spierings et al. (2011) argue that the implementation of SIT could compromise the productivity of end-users because much time could be spent exploring technologies – rather than performing the actual work they were hired to perform. Also, most employees consider technology to be a critical factor for achieving a competitive advantage. However, when end-users implement SIT, they are usually interested in a specific functionality and are not considering the complete solution; without conducting a thorough analysis of the SIT, it is unlikely to achieve a competitive edge (Kerr & Houghton, 2008). Furthermore, the lack of documentation of SIT solutions makes it difficult to support and maintain such systems, if something were to go wrong (Behrens, 2009). Fuerstenau and Rothe (2014) argued that managers should be aware of SIT solutions which are integrated with existing IT infrastructure – because the dependency could be risky to the existing infrastructure (Fuerstenau & Rothe, 2014).

Moreover, SIT could affect the security of company data (Chua et al., 2014; György & Cleven, 2012). With the absence of security controls, SIT solutions might jeopardise the privacy and confidentiality of the company's data, since most end-users might not take the necessary precautions to protect company data (Myers et al., 2016; Shumarova & Swatman, 2008). Also, SIT solutions might not have the necessary validations to prevent users from capturing incorrect data – which could result in inaccurate reports (Myers et al., 2016). Data represented on the SIT systems might be inconsistent with the data in sanctioned systems, due to the lack of robust interfaces between the systems. This could lead to employees making incorrect decisions (Kerr & Houghton, 2008; Myers et al., 2016).

SIT solutions are usually implemented to satisfy the needs of a small group of employees, which could be risky because if the original sponsor of the SIT solution resigns and leaves the company – the SIT solution is most likely to fail (Behrens, 2009).

Studies, which indicate that SIT could be beneficial, have been vigorously challenged by other studies, which highlight the risks associated with the implementation of SIT solutions. Table 2.3 displays a summary of risks of using SIT.

Table 2.3: Summary of risks of using Shadow IT

Risks	Explanation
Inadequate Software Maintenance	End-users might lack adequate skills to maintain the SIT solution as it matures over time.
Credibility and Reliability of Reports	The credibility of reports is compromised if there is a lack of robust integration between systems and if there is inadequate testing of SIT.
Financial Risk	Implementation of SIT might result in duplication of functionality - which might have negative implications for the company.
Enterprise IT Architecture Risk	Implementation of SIT solutions might result in complicated interfaces between systems, which then impact on the maintainability of the systems and negatively affect the system architecture.
Data, Information, and Security Risks	SIT might put corporate assets such as data and information at risk – due to the possibility of exposure to malware, viruses, and other external threats, which could compromise the integrity of the data.

2.8.1. Inadequate software maintenance

Over time, SIT solutions become too complicated for a functional department to maintain the software (Chua et al., 2014). Usually, end-users do not have adequate skills to maintain the software as it matures over time. Software documentation is an essential component of software maintenance, but most SIT solutions are poorly documented – which makes them difficult to maintain (Dimmler, 2013). The lack of proper documentation might be risky because the in-house IT department might not be able to assist with routine maintenance. Furthermore, the IT department might also lack the necessary human and IT resources and the capacity to handle any unplanned work, because software maintenance is costly (Fuerstenau & Rothe, 2014). These issues might be calamitous if the SIT solution forms part of a critical business process (Chua et al., 2014; Fuerstenau & Rothe, 2014).

2.8.2. Credibility and reliability of reports

Transactional and analytical reports generated from SIT software applications might be less credible because of a lack of integrated data, and inadequate testing and quality assurance –

which could mislead the decision makers within the organisation. SIT solutions are usually not integrated because they are deployed everywhere in the organisation, which means that each department might have a different version of the SIT solution (Zimmermann & Rentrop, 2014). Decentralised data might be unreliable and may not provide a snapshot of the current state of the company, which might impact on the decision-makers because decisions will be made in silos (Dimmler, 2013; Myers et al., 2016).

Incorrect logic is also a significant concern in relation to the credibility of SIT. Employees might develop macros which contain bugs or install open-source software which contains incorrect logic (Dimmler, 2013). This issue might not be discovered early on, because of a lack of thorough software testing and quality assurance (Fuerstenau & Rothe, 2014).

2.8.3. Financial risk

SIT solutions could have a negative impact on the company's finances. This impact could be a result of the duplication of functionality and fines, as a result of a lawsuit against illegal software installed by users (Behrens, 2009; Mcroberts, 2013). The duplication of existing functionality is costly because different departments might procure different software packages with similar functionalities to the existing software provided by the internal IT department (Fuerstenau & Rothe, 2014).

Furthermore, employees might also install unlicensed software on the company's workstations, which could result in legal issues and fines (Dimmler, 2013). Software licensing management is essential for compliance with audit practices, and improving processes and IT policies (Mcroberts, 2013). Centralised software licensing is necessary because it safeguards the company against wasteful expenditure and duplication of similar software and potential lawsuits (Beimborn & Palitza, 2013). However, through technologies such as cloud computing which enable users to procure and use their cloud solutions, users choose to bypass this governance procedure (Mcroberts, 2013).

2.8.4. Enterprise IT architecture risk

SIT solutions could affect enterprise IT architecture, due to the complex interfaces between the systems and architecture misalignment. The complexity of the interfaces occurs when the employees have identified the benefits of the existing SIT solutions and decide to invest in

even more SIT solutions (Fuerstenau & Rothe, 2014). Not only does this overload the IT architecture – but it also adds more complexity.

Furthermore, the integration of the SIT solution with the existing IT landscape does not follow the appropriate standards, because users might not be cognisant of IT governance best practices and the existing IT landscape (Dimmler, 2013). Also, proper planning in terms of evaluating the SIT is impossible because SIT solutions are not transparent – but only visible when something goes wrong (Rentrop & Zimmermann, 2012b). During that time, the IT department might not have the necessary capacity skill and budget to resolve the problematic issues (Chua et al., 2014).

2.8.5. Data, information, and security risks

SIT solutions could expose the corporate assets (e.g. data and information) to the outside world. When implementing SIT solutions, business users are too focused on acquiring solutions that meet their specific needs – while ignoring the possible threats which could impact on the company's information and data (Silic, 2015). Companies with SIT solutions are more vulnerable to malware, viruses, and other external threats that could compromise the integrity of the company's information and data (Dimmler, 2013; Silic & Back, 2014). Furthermore, data residing in the redundant SIT solutions could be compromised by hackers because of a lack of proper security measures to safeguard the integrity, availability and confidentiality of the data (Myers et al., 2016). When implementing SIT solutions, employees might be opening ports and over-riding the existing security measures in place – which is a threat to the company (Silic & Back, 2014).

2.9. IT controls to reduce Shadow IT

Drawing from these risks, some scholars suggested ways to manage and control SIT. Shumarova and Swatman (2008) indicated that companies have three choices when dealing with SIT. Companies could permit end-users to implement SIT solutions, devise a strategy to restrict the implementation of SIT or regulate SIT through IT policies. Györy and Cleven (2012) argued that IT security policy should be made compulsory because if the users do not comply – it could be catastrophic for the company. Silic and Back (2014) indicated that IT departments should try to identify SIT solutions used by the business units because SIT solutions that are already identified are less risky than the ones that are unknown.

Moreover, Rentrop and Zimmermann (2012) proposed a model for evaluating SIT solutions, by assessing the size, quality and alignment of the SIT solution with the company's strategic objectives. Thatte and Grainger (2010) argued that the IT department should educate the end-users about the limitations associated with the implementation of SIT. Fuerstenau and Rothe (2014) argued that IT departments should pay attention and allocate the necessary resources to SIT solutions that are considered a critical part of the business process.

However, some critics indicated that implementing IT controls could hinder a company from achieving innovation (Silic & Back, 2014). Although business and IT alignment could minimise the rate of SIT implementation – it does not prevent the implementation of SIT (Zimmermann et al., 2014).

Some scholars believe that implementing strict IT controls (e.g. policies) might be an efficient way to prevent the occurrence of SIT within the organisation - but other scholars believe the IT department should be more tolerant (Beimborn & Palitza, 2013; Rentrop & Zimmermann, 2012). Opponents IT controls indicate that the IT department should only focus on identifying ways of anticipating future SIT – rather than preventing users from implementing it (Behrens, 2009). Implementing and ensuring compliance with IT controls on a small organisation might be feasible, but this could be difficult for the large organisation with a small IT department (György & Cleven, 2012). IT departments should instead focus on identifying alternative IT solutions with similar benefits to the SIT solutions, and which the IT department can better control (Beimborn & Palitza, 2013). The IT department should also consider implementing an enterprise application store (app store) that is more controlled by the IT department – as this will protect corporate assets (e.g. data and information) from hackers (Beimborn & Palitza, 2013). SIT might not be bad, and therefore all the identified instances should be assessed to see if they align with company strategy, using criteria such as the relevance of a SIT solution, quality of a SIT solution, and the size of a SIT solution (Rentrop & Zimmermann, 2012).

Other scholars, however, believe that if the IT department wants to minimise the instances of SIT, it should educate end-users about the risks of SIT and also implement strict internal controls to prevent end users from installing third party software application to workstations (Silic & Back, 2014).

2.10. Summary of chapter

Essentially, this chapter reviewed the literature on SIT. Various topics such as the concept of SIT, the enablers of SIT, the benefits of SIT, the risks of SIT, and IT controls were addressed. However, there has been a little discussion about employee justification of SIT in current literature. Therefore, it was necessary to conduct the current study in this area, to fill the gap.

3. Theoretical framework

The selection of an appropriate theory to explore a concept is an essential part of the research process (Grant & Osanloo, 2014). Theoretical frameworks provide clarity and structure to a study, guide the research process, and serve as a blueprint for the study (Grant & Osanloo, 2014). The chapter focuses on the Neutralisation theory; the theory adopted for the study.

3.1. The Neutralization theory: background

Neutralisation theory originated from the social deviance discipline and was developed to explain the behaviour of individuals who break the law. The theory suggests that when people break the law, they always find ways to justify their acts to avoid facing the consequences and to make their behaviour acceptable (Sykes & Matza, 1957). The theory is based on the assumption that individuals who break the law feel guilt and shame for the crimes they have committed. They show respect to people who abide by the law, and who do not commit a crime. They can differentiate between people who can be victimised and those who cannot be victimised, and they have a desire to conform to what appears to be acceptable to wider society. Law-breaking individuals always find ways to justify their behaviour to avoid guilt and shame. They do that to convince themselves that the crime they committed is acceptable. Sykes and Matza (1957) termed the justifications as "*Neutralisation techniques*".

This study employed the Neutralisation theory to assess the deviant behaviour of functional departments who implemented SIT at EPZA. Usually, end-users who implement SIT violate IT policies and procedures. Studies indicate end-users employ the Neutralisation techniques the feeling of guilt and shame of violating the law.

3.2. Neutralisation Techniques

Initially, Sykes and Matza (1957) identified five Neutralisation techniques: denial of responsibility, denial of injury, denial of victim, condemnation of condemners, and appeal to higher loyalties. Table 3.1 lists the summary of Neutralisation techniques.

Table 3.1: Summary of Neutralisation techniques

Technique	Description
Denial of responsibility	Offenders claim that they have no choice but to break the law. In most cases, the offenders shift the blame to the victim and use phrases such as "it wasn't my fault" (Ribeaud & Eisner, 2010).
Denial of injury	The technique is used to nullify the feeling of remorse toward their victim. The offenders justify their behaviour by indicating that "breaking the law is not a big deal, no one got hurt" (Liddick, 2013).
Denial of the victim	Offenders claim that the victim deserved to be harmed and they show no remorse towards the victim (Liddick, 2013; Sykes & Matza, 1957).
Condemnation of the condemners	Offenders who use this technique claim that people who are against the behaviour would have behaved the same way they did if they were in the same situation (Haag et al., 2015).
Appeal to higher loyalties	Offenders believe that the crime they have committed was done for the benefit of the greater part of society (Harris & Dumas, 2009; Liddick, 2013; Sykes & Matza, 1957)

Denial of responsibility is used to shift the blame to the victims. In most cases, the offender claims that they had to commit the crime because it was beyond their control (Sykes & Matza, 1957). An offender might use a phrase such as "*It's not my fault. I commit crime because I had a troubled childhood*" (Liddick, 2013,p623) to justify the crime. In the context of the corporate IT department, service delivery is a challenge, and usually IT departments fail to deliver services according to the end-users expectations. To fulfil their need, end-users may implement IT solutions from third-party suppliers without seeking assistance or approval from the IT department (Silic & Back, 2014).

Denial of injury is used to justify the crime by indicating that it was harmless and did not cause any destruction (Silic & Back, 2014). Offenders might use phrases such as "*maybe what I did was criminal, but no one got hurt*" (Liddick, 2013,p623) to justify the crime. In the context of this study, the implementation of SIT in a company may result in negative financial, legal and IT security implications. However, end-users may neutralise their behaviour by only highlighting the benefits of implementing SIT and avoiding the negative implications for the company (Chua et al., 2014; Dimmler, 2013; Silic & Back, 2014).

Denial of the victim is used to justify the crime by indicating that the victim deserved to be harmed and they show no remorse toward the victim (Sykes & Matza, 1957). Offenders may use phrase such as "*yes, I committed the crime, but he deserved i*t" (Liddick, 2013,p623) to justify the deviant action. In the context of this study, due to the poor service delivery received

from the IT department, end-users may seek alternative IT suppliers without consulting the IT department and show no remorse to the IT department for bypassing IT policies and procedures (Behrens, 2009; Dimmler, 2013; Silic & Back, 2014).

Condemnation of the condemners is used to justify the crime by indicating that people who are against the behaviour would have behaved the same way if they were in the same situation (Sykes & Matza, 1957). Offenders might use phrases such as "*I'm not the bad guy, the abusive and corrupt criminal justice system is where you find the real crooks*" (Liddick, 2013,p623) to justify the deviant behaviour. Usually, IT departments can enforce strict IT controls thorough IT policies as a way to prevent end-users from implementing IT solutions from third-party suppliers, and end-users may see these as unreasonable and indicate that if the IT was in a similar situation, they would also have considered other IT service providers (Silic & Back, 2014).

Appeal to higher loyalties: used to justify the crime. This Neutralisation technique is evident when respondents believe that the crime they have committed was done for the benefit of the greater part of society (Sykes & Matza, 1957). Offenders might use phrases such as "*the gang is my family—I sell drugs to support my family*" (Liddick, 2013,p623) to justify the crime. In the context of this study, end-users may justify the implementation of SIT by indicating that they had to meet the key performance target of the department, and may also state that if they had not done so they would not have been able to achieve the targets they have achieved (Behrens, 2009; Dimmler, 2013; Silic & Back, 2014).

3.3. The justification for the choice of theory

The Neutralisation theory is ideal for assessing the justifications for SIT. The theory holds the view that law-breaking individuals use different techniques of Neutralisation to justify their behaviour in an effort to minimise the feeling of guilt and shame. While the theory was originally developed in the field of criminology to assess the behaviour of criminals, recent studies have applied it to assess IS-related topics such as online consumer misbehaviour (Harris & Dumas, 2009), information systems' security policy violations (Barlow et al., 2013), and justification of SIT. Table 3.2. Shows earlier studies that applied the Neutralisation Theory to explore Justification of SIT.

Table 3.2: Studies which applied the Neutralisation theory to explore Shadow IT

Title	Key findings	Author(s)
Justifying Shadow IT Usage	Researchers used the Neutralisation Theory to develop a research model for evaluating the factor that might influence the creation of SIT. The study indicated that denial of necessity, denial of injury and condemnation of the condemner Neutralisation techniques might influence the creation of SIT in a company.	Haag and Eckhardt (2015)
A new perspective on Neutralisation and deterrence: Predicting Shadow IT usage	The findings from the study highlighted that Neutralisation technique which could predict the intention of end users implementing SIT.	Silic et al. (2017)
The Acceptance of justifications among Shadow IT Users and Nonusers – An Empirical Analysis	The study investigated the usage patterns of "Shadow IT users" versus "Shadow IT non-users". The findings indicate that SIT non-users will only be convinced to accept SIT solutions if they believe that it would be beneficial to use SIT solutions.	Haag et al., (2018)

In the context of this study, Neutralisation Theory looks at evaluating Neutralisation techniques used by end-users (functional departments) to justify the implementation of SIT in a company.

Moreover, there are only a few studies that have used the Neutralisation Theory to explore the concept of SIT. To the best of the researcher's knowledge, the studies that used the Neutralisation Theory did not use a qualitative approach, but rather a quantitative approach to collect and analyse data. Qualitative studies are however essential because they provide details that cannot easily be captured by surveys and other quantitative methods (Boyce & Neale, 2006). This study aims to close that gap by collecting and analysing data using qualitative methods.

3.4. Research propositions

Neutralisation theory identified five techniques used to justify criminal behaviour: (i) denial of responsibility, (ii) denial of injury, (iii) denial of victim, (iv) condemnation of condemners, and (v) appeal to higher loyalties (Sykes & Matza, 1957). Based on the literature review, the researcher made propositions listed in Table 3.3:

Table 3.3: Summary of propositions

Proposition	Technique	Evidence
1	**Denial of responsibility**	Employees may use the "*Denial of Responsibility*" Neutralisation technique to justify the implementation of SIT. Denial of responsibility manifests itself when the respondents blame others for their deviant action (Sykes & Matza, 1957).

2	**Denial of injury**	Employees may use the "*Denial of Injury*" Neutralisation technique to justify the implementation of SIT. Denial of injury manifests itself when the respondents indicate their criminal activity was harmless and did not cause any destruction (Sykes & Matza, 1957).
3	**Denial of the victim**	Employees may use the "Denial of the Victim" Neutralisation technique to justify the implementation of SIT. Denial of the victim is evident if respondents indicate that the victim deserved the immoral behaviour implemented against them (Sykes & Matza, 1957).
4	**Condemnation of the condemners**	Employees may use the "*Condemnation of the Condemners*" Neutralisation technique to justify the implementation of SIT. Condemnation of the condemners is evident if the respondents fail to take responsibility for their crimes, but instead indicate that the people condemning the deviant behaviour are hypocrites (Sykes & Matza, 1957).
5	**Appeal to higher loyalties**	Employees may use the "*Appeal to Higher Loyalties*" Neutralisation technique to justify the implementation of SIT. Appeal to higher loyalties is evident if the respondent believes that the crime was committed to benefit others (Sykes & Matza, 1957).

3.5. Summary of chapter

This chapter discussed the theoretical background of the study. Neutralisation Theory was selected as an appropriate theory for this study because it is in line with the study objective, which is to evaluate justifications used by end-users (functional departments) who have implemented SIT in a company. While the Neutralisation Theory originates from the field of criminology, it has gained wider acceptance in the field of IS – and scholars have used it to explore IS topics. The chapter gave some background on the Neutralisation Theory, explained Neutralisation techniques, gave justification for the choice of theory, and closed with a discussion of the application of the Neutralisation Theory in IS research.

4. Research Methodology

This chapter presents a brief background of the research methodology. Next, it justifies the sampling strategy and sampling technique used in the study. The chapter presents the data-collection technique and data-analysis methods. Finally, the chapter presents issues of reliability and validity related to this study – as well as research access and research ethics

4.1. Research paradigm

A paradigm or worldview is an assumption made by an individual about a particular phenomenon (Tien, 2009). In research, I influence the way in which knowledge is created (Bhattacherjee, 2012; Tien, 2009). The two common research paradigms in IS are positivism and constructivism (interpretivist). Their ontological and epistemological stances characterise these paradigms.

Ontology is the researcher's perception of reality and how it exists (Krauss & Putra, 2005; Rehman, 2016). The positivists believe that knowledge is already available and is produced when the researcher is objective and independent from the social context (Tien, 2009). On the other hand, interpretivists believe that reality does not exist, to understand the social phenomenon the researcher has to interact with respondents (Klein & Myers, 1999).

Epistemology is the researcher's perception of knowledge discovery. These perceptions are influenced by the ontological stance adopted by a researcher. The positivist's researchers believe in independence and objectivity. Thus, when conducting a study, a researcher remains objective and detach from the social actors (Bhattacherjee, 2012; Rehman, 2016). On the other hand, the constructivists believe that knowledge cannot be created if the researcher is independent of the social actors, and therefore mixing with the respondents enables the researcher to attain a deeper insight of the context of the subject studied (Klein & Myers, 1999; Tien, 2009).

The primary objective of this research was to assess the justifications used by end-users who bypass IT policies and procedures to implement SIT solutions. The researcher adopted the interpretivist research paradigm to gain a deeper understanding of the concept of SIT.

4.2. Research strategy

While there are many research strategies, this study adopted the case-study approach to examine the concept of SIT. Merriam (2002) defined a case study as "…*an intensive description and analysis of a phenomenon or social unit such as an individual, group, institution, or community*" (p. 8). The case-study research strategy was suitable for this study because this research examined the concept of SIT, which is exploratory and also asked the "*how?*" and "*why?*" questions (Yin, 2009).

There are different types of case-study research strategies case study can be either a single case or multiple cases. A single case is suitable if there is only one instance of the phenomenon and multiple cases are suitable when there is a possibility of replication of the scenarios (Zainal, 2007). The primary concern for the case-study research approach is the generalisation of the results. For a single case study, it could be difficult since the phenomenon cannot be replicated. However, the researcher might triangulate the findings with existing studies. On the other hand, multiple case studies might be advantageous, because the researchers might be able to generalise their conclusions. This study adopted the single case-study research approach to examine the concept of SIT within the real-world context (EPZA) (Merriam, 2002; Yin, 2009).

4.3. Sampling strategy

Selecting a sample that can be generalised to the entire population is an essential step of the research project (Marshall, 1996). Samples are necessary because it could be impractical or inefficient to study the entire population (Marshall, 1996; Saunders et al., 2009). Some of the constraints that prevent the researcher from studying the entire population are related to the availability of resources such as money and time (Saunders et al., 2009). Figure 4.1 illustrates the sampling process. This process involves three stages – identification of the population, selecting a sampling frame, and determining the sample (Bhattacherjee, 2012).

The target population (unit of observation) could be a person or group that the researcher would like to make inferences about (Bhattacherjee, 2012). The researcher determined the unit of analysis by answering the following questions: "*do I want to "analyse" the individual? Do I want to "analyse" a program? Do I want to "analyse" the process? Do I want to*

"analyse" the difference between organisations? " (Baxter & Jack, 2008, p. 545). The research question and the unit of analysis considered in this research are as follows:

Research question

How do functional departments (end-users) justify the implementation of Shadow IT solutions?

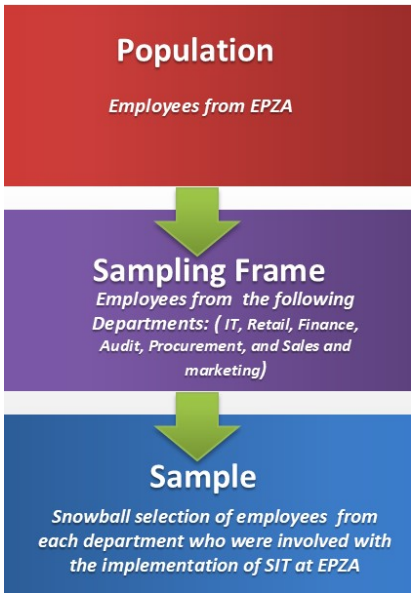
Unit of analysis

The researcher interviewed employees from different functional departments to assess if they have used the Neutralisation techniques to justify the implementation of SIT.

The choice of the sampling frame was based on two factors:

1. The availability of respondents to conduct the interview.
2. The respondents who are a subject matter expert on the topic investigated (Bhattacherjee, 2012).

Figure 4.1: The sampling process



The sampling frame for this study comprised of employees from different business units – as well as the managers from the IT department. The last step was to determine the sample of the study. There are two types of sampling techniques: probability and non-probability (Bhattacherjee, 2012; Saunders et al., 2009). Probability sampling or (representative sampling) indicates that every case or element in a population might be selected to form part of the sample. Usually, probability samples are associated with the survey data-collection technique (Saunders et al., 2009). There are different types of probability samples such as

simple random sampling, systematic sampling, stratified sampling, and cluster sampling (Bhattacherjee, 2012).

On the other hand, non-probability samples indicate that some of the units in the population might not be considered as part of the sample. In this case, the respondents might be selected based on their knowledge of a particular subject area (Bhattacherjee, 2012). Some examples of non-probability sampling are convenience sampling, quota sampling, snowball sampling, and purposeful sampling (Bhattacherjee, 2012).

The study adopted purposive sampling and snowball sampling. The purposeful sampling technique was suitable because the researcher was unaware of the exact number of SIT instances available in the company, as well as the employees who were involved with the implementation of SIT (Bhattacherjee, 2012). To identify the SIT instances and the key stakeholders involved in the implementation SIT solutions, the snowball sampling strategy was used. The snowball technique involves making contact with cases in the population who will make necessary recommendations to another member of the population (Saunders et al., 2009; Shakir, 2002). The snowball sampling strategy was useful because the researcher could get a subject matter expert who was involved with the implementation of SIT based on the referral from earlier respondents. Table 4.1 lists respondents who took part in the study:

Table 4.1: Respondents' profile

Respondent ID	Respondent Role	Department
ISR1	Solution Specialist	IS Department
ISR2	Solution Analyst	IS Department
ISR3	Solution Analyst	IS Department
ISR4	Change Manager	IS Department
ISR5	IT Manager	IS Department
BUR1	Key Accounts Team Leader	Retail Department
BUR2	Finance Manager	Finance Department
BUR3	IT Audit Manager	Audit Department
BUR4	IT Auditor	Auditing Department
BUR5	Procurement Specialist	Procurement Department
BUR6	Procurement Manager	Procurement Department
BUR7	Procurement Analyst	Procurement Department
BUR8	Project Specialist	Sales and Marketing Department

Thirteen respondents were interviewed for this study. The sample comprises employees from the IT department – as well as employees from other functional departments such as finance, internal auditing, procurement and sales and marketing.

The size of the sample is based on Guest et al. (2006), who indicated that for a qualitative study, a saturation point is achieved if a researcher interviews at least 12 respondents as representing a homogeneous sample. However, if the saturation point is not met after 12 respondents are interviewed, the researcher will continue collecting the data until the saturation point is met (Marshall, 1996).

4.4. Time-frame

Researchers can choose to complete their studies within different time-frames depending on the scope and availability of resources for the study (Saunders et al., 2009). The research time-frame is not dependent on the research strategy selected by the researcher. There are types of research time frames – such as cross-sectional and longitudinal. A longitudinal study is conducted over a period, during which time the researcher can study a phenomenon and see how it changes over a period (Saunders et al., 2009). On the other hand, a cross-sectional study is conducted at a specific period, and the study only captures a snapshot of a particular phenomenon during a specific period. Cross-sectional studies are helpful, especially if the researcher has a limited amount of time to complete the study (Saunders et al., 2009). Due to the limited amount of time available to complete this thesis, the researcher selected the cross-sectional time-frame.

4.5. Data collection techniques

The study adopted two techniques – documentation analysis and semi-structured interviews. The combination of these data-collection techniques improved the strength of the research finding, by enabling the researcher to gain a deeper understanding of the concept of SIT (Dubé & Paré, 2003).

4.5.1. Semi-structured interviews

Interviews can be unstructured, semi-structured and highly structured. Structured interviews involve researchers preparing the interview questions well ahead of time; the questions may not be changed during the interview (Merriam, 2002). Unstructured interviews involve not preparing the questions before the interview – but using the research area or topic of interest to ask and probe for more answers (Merriam, 2002). Semi-structured interviews involve the researcher preparing a list of questions before the interview; however, during the interview, the participant's responses may prompt the interviewer to probe further to gain deeper insight into a phenomenon (Merriam, 2002). This study employed the semi-structured interview

technique to analyse the availability of SIT policy and justifications for SIT by functional departments in a company.

The advantage of interviews is that they provide detailed information that cannot be easily captured by the surveys (Boyce & Neale, 2006). However, interviews have some disadvantages such as bias, time-intensive, poor interviewing skills, and a lack of generalisation (Boyce & Neale, 2006). To mitigate these issues, the researcher considered the following suggestions by Boyce and Neale (2006):

- The researcher identified a list of stakeholders to be interviewed ahead of time.
- Research instruments such as the interview protocol were used during the interview process (see *Appendix A*).
- The researcher took notes during the interview and audiotaped each interview.
- Immediately after the interview was complete, the researcher began the transcription process.

4.5.2. Document analysis

Documentary data were used as secondary data. Documentation is essential to gain a deeper insight of the concept being studied (Merriam, 2002). The researcher collected supporting documents such as policy documents and emails, which aided with understanding the context of SIT in EPZA. Through documentation, the researcher could triangulate the findings of the primary data collected (Saunders et al., 2009).

During data collection, the researcher followed three fundamental principles: triangulation, case-study database and chain of evidence (Rowley, 2002). The data collected from multiple sources such as policies and semi-structured interviews were compared against each other to substantiate the findings (Rowley, 2002). To improve the transparency and reliability of the study, the researcher documented and safely kept all the interview transcripts and any other field notes (Rowley, 2002).

4.5.3. Research instrument

The researcher used semi-structured interviews as a primary research instrument for collecting data in this study. The interview questions (Appendix B) were crafted with the aim of eliciting data relating the five techniques of Neutralization from the Neutralization theory which are the denial of responsibility, denial of injury, denial of victim, condemnation of condemners and appeal to higher loyalties. The interview document had six sections, the first of the

interview section collected data relating to the respondent job title, level of experience on the role and the details of the policy for SIT at EPZA. The second section of the interview sheet consisted of questions relating to the Neutralization techniques.

A pilot study was conducted in preparation for the complete study (van Teijlingen & Hundley, 1998). Two employees from the IT department at EPZA were interviewed. The feedback received from the respondents assisted with refining the interview questions and assessing the effectiveness of recruiting the respondents to participate in the study (van Teijlingen & Hundley, 1998).

4.6. Data analysis

The study adopted the thematic analysis approach. Thematic analysis is *"... a method for identifying, analysing, and reporting patterns (themes) within data*" (Braun & Clarke, 2006,p6). Through thematic analysis, the researcher could describe the data in detail. The researcher used Microsoft excel to code , organise, and analyse the data thematically (Bree & Gallagher, 2016). Figure 4.2. Illustrates the phases of Thematic Analysis.

Figure 4.2: Phases of thematic analysis (Braun & Clarke, 2006).

Phase	Description of the process
1. Familiarising yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
2. Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.
4. Reviewing themes:	Checking in the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
5. Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells; generating clear definitions and names for each theme.
6. Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

1. The researcher transcribed all the interviews and also familiarised himself with the data; during this stage, the researcher immersed himself in the data to gain an in-depth understanding and meaning of the data (Braun & Clarke, 2006). The researcher achieved that by listening to the audio recordings and reading the interview transcripts several times. Data analysis began soon after the first interview was completed – which allowed the researcher to make the necessary adjustments and to improve on the subsequent interviews (Merriam, 2002).
2. The researcher documented the codes. The researcher created the codes by reading the transcripts; these codes represent the interesting themes identified from the interviews (Braun & Clarke, 2006). The researcher worked systematically through the transcripts to make sure that no data items were missed.
3. The researcher began to search for themes (Braun & Clarke, 2006), went through the long list of codes derived from phase 2, and begin sorting them and constructing a theme for each group of codes.
4. The themes were reviewed and refined (Braun & Clarke, 2006). If the themes were too vague and there was not enough data to support them, the researcher revised them and broke them into sub-themes.
5. The research defined all the themes and explained the characteristics of data captured (Braun & Clarke, 2006).
6. The researcher began the write-up process.

4.7. Research validity and reliability

4.7.1. Reliability

Reliability measures the consistency of the data collected for a study (Bhattacherjee, 2012). The consistency of the research refers to the ability of the study to yield similar results if it was conducted on a different occasion. Three issues were taken into account by the researcher to avoid threats to reliability – participant error, participant bias, and the researcher's error (Saunders et al., 2009):

Participant error - To mitigate this issue, the researcher scheduled interview sessions at the time convenient for participants. The research considered factors such as day of the week, time of the day, and time when they were less occupied.

Participant bias – To mitigate participant bias, the researcher conducted one-on-one interviews in a meeting room away from all forms of distraction. The respondents were made aware that all information – including participant names – will be treated confidentially.

Researcher error – The interview questions were structured, and the researcher asked the questions in a consistent manner.

4.7.2. Validity

There are two types of validity – internal and external (Saunders et al., 2009). Internal validity measures whether the study is measuring what it was supposed to measure (Bhattacherjee, 2012). The issues relating to the design of the research mostly affect internal validity. Some of the internal validity issues include the size of the population, history, and time taken to complete the study (Saunders et al., 2009). On the other hand, external validity is concerned about the extent to which the study could be generalised to the entire population (Bhattacherjee, 2012).

4.8. Research access and ethics

4.8.1. Access and permission

Academic research may involve invading the company's or respondents' privacy, and therefore obtaining the necessary permission is essential (Stake, 1995). Before the commencement of data collection, the researcher understood the roles of the departments. The familiarisation process included understanding the organisational structure and the different top managers within each department. Existing contacts within the departments were used to ensure that entry to the organisation was easy (Saunders et al., 2009). Also, a formal email stating the purpose and the type of access required was sent to relevant stakeholders. Permission to conduct this study was authorised by the project sponsor EPZA and a formal letter detailing acceptance of the study was drafted and signed by the CIO of EPZA (*See Appendix E*).

4.8.2. Research ethics

Ethics is defined as "… the appropriateness of your behaviour in relation to the rights of those who become the subject of your work or are affected by it" (Saunders et al., 2009, p. 183). The issue of privacy is essential, and the details of respondents, including their names and the names of the company, were kept confidential. The researcher also assured anonymity and

confidentiality to the respondents, and an email was sent to the respondents before the interview (see *Appendix C*). Data collection did not commence until the ethics approval certificate was obtained from the University of Cape Town.

4.9. Summary of chapter

This chapter began with a brief description of the philosophical considerations; the researcher adopted the interpretivist research approach. The researcher considered a case study to be an appropriate research strategy for understanding the concept of justification of SIT by functional departments within a company. The study used a purposeful sampling strategy and the snowball sampling technique, because the number of cases and respondents was not known – they were discovered in the field during data collection. The time-frame selected was cross-sectional due to the time limit in terms of completing the study. Data collection and analysis techniques were interviews, documentation, and thematic analysis – because they enabled the researcher to conduct an in-depth exploration of the phenomenon of SIT. Finally, the reliability and validity of the study – as well as the research access and ethics – were discussed.

5. Case description

This chapter describes the company chosen for this study (EPZA). The chapter outlines the SIT policy and historical background of SIT at EPZA and how the company attempted to deal with such implementations.

5.1. Description of the organisation

The research was conducted in a multinational petroleum company based in Cape Town, South Africa; for ethical reasons, the organisation is anonymised as EPZA. EPZA specialises in manufacturing and refining downstream petroleum products. The company has a presence in over 18 countries and ships petroleum products to more than 30 countries worldwide. EPZA employs more than 3000 employees across the primary and support activities of the value chain.

The primary activities of the value chain comprise of sourcing and manufacturing products, storage and distribution of products to the customers and marketing the products to the customers. The support service enables the primary activities (*the business*) to deliver quality services to customers, and comprise of the following departments: Finance, Human Resources, Legal and Corporate. Figure 5.1 illustrates the value chain for EPZA.

Figure 5.1: EPZA value chain

The Finance department is one of the largest support department at EPZA, and it aims to meet the needs of the business by performing activities relating to treasury, taxation, credit management, accounting and IT. The finance department consists of eight functional departments namely, Accounting department, Treasury Department, Risk department, Credit department, Tax department, Procurement department, IT department, and Document and knowledge management department.

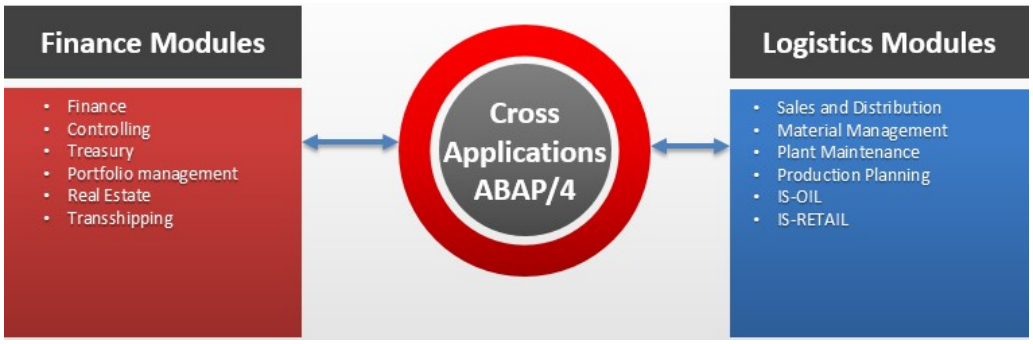
5.2. The IT department at EPZA

EPZA has an in-house IT department that functions as an enabler for the company to meet strategic objectives. The focus of the IT department at EPZA is to understand the needs of the functional departments and to deliver cost-effective IT solutions to meet departmental and organisational strategic objectives. The IT department consists of the following teams; SAP Core Applications, End-user computing, Information Security, and Architecture and governance team.

- *SAP core applications (SCA)* – The SCA team is the largest within the IT department and concentrates on three main areas: Finance, Logistics and Cross Applications. The Finance area focus on the following SAP modules: Finance, Controlling, Treasury, Project portfolio management, Finance supply chain, Real estate, and Transhipping. The Logistics area focuses on the following: Sales and Distribution, Material Management, Plant Maintenance, Production Planning, Quality Management, IS-Retail, and IS-OIL. The Cross Application area focuses on the following: SAP ABAP Development, Solution Manager and Fiori Development. Each SAP modules consist of functional consultants and developers responsible for eliciting the requirements from the functional departments, designing the solutions, implementing solutions through SAP development or system configuration, testing, and post-delivery maintenance. Figure 5.2 illustrates a list of SAP modules supported at EPZA.

- *End-user computing (EUC)* – The EUC team focuses on two main areas, Application Development (.Net development) and End-user training. The Application development team is responsible for the development of software applications, licencing and upgrading all Microsoft products used across the company such as office package applications. The end–user training team develops training manuals and train users from the different functional department on all applications developed by the IT department, SAP and.Net applications.
- *Information security team*– The Information security team, ensures that information across all applications supported by the IT department is preserved through safeguarding confidentiality, integrity and availability of information. The information security team consist of IT security consultants responsible for developing IT controls and to grant authorisation to end-users with the aim of safeguarding and protecting the company's assets.
- *Architecture and governance* – The Architecture and governance is responsible for reviewing all technology solutions and provides the conceptual and technical architecture which aligns with the EPZA's strategies. It also promotes reusing of common applications to ensure that the software portfolio is simplified and validates the technology solutions that support the functional departments

Figure 5.2: SAP modules at EPZA



In the organisational structure, the IT department falls under the Finance Department from which it receives most of the operational budget. The budget is allocated so that the IT department can maintain and support the existing legacy applications – and also create IT services for functional departments across the company. Due to budget constraints, usually, the IT department is not able to meet the demands of the functional departments. In addition, to budget constraints, the IT department at EPZA experienced many challenges, and they are listed in Table 5.1.

Table 5.1: Challenges experienced by the IT department at EPZA

Challenge	Comment
Poor communication - The IT department at EPZA operates in silos. Several factors contribute to the existence of silos such as poor communication between different teams within the IT department, communication between the management and employees at an operational level.	"We don't know what the function of our IT division is - if you got an internal division in IT as the business you expect to get everything that you require from that division. So, maybe if they - if it does not make any business sense then maybe the business can be told what the reason is then we can understand and have a more productive relationship with our IT division."- **[BUR2].** "The managers will tend to say yes we can do it, but eventually when it hits the ground with the developers, it is a bit of a stumbling block to say they cannot do it" – **[BUR1].** "To have architects that do not know the system end to end and that does not know integration makes it very difficult – because business runs to them for a solution. They can sign the solution, and they do not bother comm... I will not say always, but they do not normally contact the consultants. They would try to build up their own solutions and just fish for little bits and pieces but eventually they might have been a solution that the consultant could have put ahead and then architect went and said – ok really there is a third-party system out there – Which is incorrect because first of all you can only go third-party if your baseline is correct" – **[ISR1].**
IT is too slow - IT department is to slow to deliver solutions to the functional departments due to red tape.	"Is just in IS, there is too much red tape. We are short-staffed, there is too much complaining, we don't have the staff, and we don't have the capacity to do this. So the business, a lot of the time, has to seek third-party solutions" – **[BUR8].** "It (the process for requesting a new development) is very tedious, it is a long process. We do understand I mean they have to plan and make sure that all the resources are properly utilised, but it does sometime impact the way the business operating" – **[BUR2]**
Lack of capacity to deliver IT services- the IT department at EPZA lacks the capacity (shortage of staff) to manage the demand from the functional department.	"The challenge now was full potential to say now depending on how quickly you want the solution if you have to have it now you would have to go to the external vendor or if you can wait till November then she would then be able to help. So, I suppose it just depends on the available resources internally" – **[BUR3].** "… We don't have the staff, we don't have the capacity to do this – so the business, a lot of the time, has to seek for third-party solutions." – **[BUR8].**

5.3. Shadow IT at EPZA

Most functional departments at EPZA do not inform the IT Department prior to the implementation of unsanctioned IT solutions. In most cases, the IT Department is only aware of a SIT when a functional department requires to integrate their software with existing sanctioned software such as SAP, or when they needed to upgrade their software. The following statements demonstrate the presence of SIT at EPZA.

> "*So basically, we (the functional department) just did research the guys came through and did a pilot for the tool, we did one file I think, we piloted one audit file and then we bought the tool*" – [**BUR3]**.
>
> "*…we (the functional department) do implement applications without going through the architecture process. There is no way really for EPZA to pick up if the third-party application has been implemented and has not gone through the architecture process*" – [**BUR4**].

In instances were a SIT solution has to be integrated with existing sanctioned software, it has to go through the formal IT architecture review process, and, depending on the outcome of the architecture review, the IT department may agree or refuse to implement the software application. One respondent made an example of a SIT solution which was not implemented because of security risks and stated that:

> "*We (the functional department) purely focused on what we needed without necessarily keeping the potential risks in mind. So, we had the vendor that provided us with the tool that we wanted and then only when we hit the implementation stage then the guys from IS, …wanted a conversation with the vendor to get an understanding of how the tool extract EPZA's information and how does it interact and who's got access to that information...they decided that no, security is too high - the risk is too high, then we couldn't implement it…*" – [**BUR3**].

Lack of applications architecture review of an arm's length application by the IT department meant that the software application introduced by the functional department was not assessed to determine whether it aligned with the company's policies and standards – and the company lost money due to increased duplicate IT solutions across the company.

> *"…we gave them the redesign document, but at the stage, EPZA had already paid R 3 million for the other software. So the slid it under the table just before we closed the IS gap. We basically got excluded from all meeting after that - after we have told them that they have to redesign.*" – **[ISR1].**
>
> "*If it's bought already then they would have to go through an architecture review. So, they would be an architecture review in hindsight as to they have bought this thing, they have spent*

the money there is nothing we can do about it – we can educate them that they don't do it again…" **– [ISR4]**

To express concerns around the issues of relating to the implementation of SIT, the CIO sent an email to different stakeholders in the company outlining the impact of SIT on the productivity and profitability of the company. The CIO informed the stakeholders about the policy introduced to clean up duplicate IT solutions in the company:

"*The policy aims to reduce/remove any duplicate and inefficient IT-related activities and costs across divisions and the affiliates, and thereby contributes to the full potential battlefields of 'drive down cost to serve' and 'optimise across the value chain*'" – [**Source: email from CIO**].

5.4. Summary of chapter

This chapter introduced the company chosen for the study. The chapter began by explaining the organisational structure and outlined the different departments within the company's value chain and the core business performed by the company. Furthermore, the chapter explained the role of the IT department at EPZA. Finally, the chapter outlined the instances of SIT solutions at EPZA and the implications for the profitability of the company.

6. Findings

This chapter presents the research findings gathered from the analyses of interviews and documents. Themes found in the literature are presented and backed up with the actual responses from the interviews and documentation (IT policy). To begin with, the chapter identifies the availability of IT policy or IT control to manage or to prevent the implementation of SIT by functional departments at EPZA. Then the chapter classifies the Neutralisation techniques used by end-users to justify the implementation of SIT at EPZA. Finally, the chapter highlights the emerging concepts from this study.

6.1. IT controls for Shadow IT at EPZA

To establish whether there is a policy for managing SIT solutions at EPZA, the respondents were asked to indicate whether the organisation had an IT policy that prevents end-users from implementing unsanctioned software from third-party vendors. Most respondents were unaware of the policy. One of the respondents stated that:

> "*I haven't heard of a policy that says thou shall not implement (SIT)*" – [**BUR3**].

Some respondents mentioned that there was a policy used by the IT department to manage new software implementations across the company. However, they felt the policy does not prevent them from implementing their own software applications. The policy they were referring to was the Application Management Element (AME) policy.

> "*It is allowed. The proposal is that it goes through the architecture and governance process and the service acceptance process. So, there is a policy which states that you get arms-length applications, partnership applications, and the third one is [an] IT-owned type of application.*" – **[BUR4].**

The AME policy was established to manage the process of implementing new IT solutions at EPZA. The policy outlines the responsibilities of the IT department and the functional departments when implementing a new software application. This policy focuses on topics such as software budget allocation, software licence management, maintenance and support, software support, information security, end-user training, software testing, application capacity management, data governance, IT service continuity, and backup and recovery.

The AME policy offers functional departments three options through which they can implement IT solutions – dedicated, partnership and arms-length. In the *dedicated* option, the

IT department is responsible for the implementation and support of the software. *Partnership* software applications are managed by both the IT department and the functional department – which means that the IT Department and a functional department agree to share responsibilities relating to the topics stated in the AME policy. However, in the arms-length option, the functional department takes full responsibility for the software application; it is responsible for implementing and supporting it. While the arms-length option allows the functional department to implement IT solutions without assistance from the IT department, the policy states that the functional department has a responsibility for "*ensuring that the Information Services Department has a line of sight of all applications used by the Business*" **[AME Policy, p. 6]**. Table 5.1. Summarises the application management policy used at EPZA:

Table 6.1: Summary of the Application Management Elements policy at EPZA

Mode	IT Department responsible	Functional Department Responsible
Dedicated	• Facilitating communication with external vendors regarding software licenses. • Ensuring that the eternal vendor delivers the software, as stipulated in the contract. • Installation and integrating the third-party software to the existing landscape. • Managing the software development lifecycle such as designing, development and implementing the software applications. • Ensuring that confidentiality, integrity and availability are maintained at all times. • Developing and providing ongoing support for the software implemented. • Documenting the test case/test scripts and ensuring that all test scenarios are covered prior to implementation of the software. • Documenting policies for mitigating IT security risks and setting the strategy according to the company's strategy. • Alignment between the IT and business units, in terms of the security plans and business continuity plans.	• Not applicable
Partnership	• The IT department, in partnership with a business unit, are responsible for the licensing cost of the software and full support of the software.	• The business unit is responsible for first-line support of the software

	• The IS department is responsible for offering the necessary infrastructure and for installing the software.	• The business units are responsible for building and implementing the software. • The business unit is responsible for managing all security-related issues • The business unit is responsible for end-user training. • The business unit in consultation with the IS department consults the external vendor in terms of obtaining licensing costs. • The business unit is responsible for renewing the contract with the external vendor and for managing all contractual obligations. • The business unit is responsible for configuring the systems obtained from the external vendor or for seeking assistance from the external vendors
Arms-Length	• Not applicable	• Software licensing costs. • Software license management. • Engaging with vendors in terms of maintenance and support of the software. • Technical and functional support of the software. • Building, implementing and installation of the software. • Protection of information and securing the systems from external threats. • Testing the software (unit test, integration testing and user acceptance testing). • Notifying the IS department when planning to introduce a new software application/the IS department assesses the application for potential risks and compatibility with the existing landscape.

Some respondents felt the AME policy gave the functional department too many responsibilities in terms of implementing the software and that there was less support from the IT department – especially if the functional department chose the partnership or arms-length option. One of the respondents stated that:

> "*I think our biggest risk sits between the arms-length and partnership applications because you are giving the business a huge responsibility from a governance perspective and the business is not necessarily as technically savvy to ensure compliance to the governance*." **– [BUR4]**

In addition, one respondent mentioned that the reason end-user bypass the IT department especially with the arms-length application is because there is no formal guideline in the AME policy. The respondent made the following comments regarding the arms-length applications:

> "*…I think that on its own it's an indication that the business can be exposed because it's not clear as to what are the difference like the steps that need to be followed*" – **[BUR3]**

6.2. Neutralisation techniques

Neutralisation techniques allow the delinquents to justify their deviant behaviour by using phrases that make the situation morally acceptable – with the main objective of protecting their self-image and minimising the feeling of guilt and shame (Sykes & Matza, 1957). The primary objective of this study was to identify whether end-users at EPZA used Neutralisation techniques to justify the implementation of SIT. Analysis of interview transcripts revealed that end-users use Neutralisation techniques to justify the implementation of SIT. While there are many Neutralisation techniques in the literature, the three Neutralisation techniques identified in this study were: denial of responsibility, denial of injury, and appeal to higher loyalties.

The Neutralisation Theory is grounded on the assumption that individuals who break the law feel guilt and shame in relation to the crimes they have committed. In this study, however, only few instances of individuals expressing guilt and shame were evident. For instance, one respondent said that:

> "*You are IS – you have heard that we are doing this. Yes, we didn't go through the right channels and you don't even ask enough questions to see if there is anything you can do or to improve…yes, probably when the business implemented the solution they should have started there – but nevertheless it is done*" – **[BUR8].**

This statement indicates that the end-users are aware that they did not follow the correct process when implementing a SIT solution. However, they continued to defend their actions to minimise the guilt and shame. An example which indicates that business is aware of the IT process was evident when the one respondents made the following statement:

"*We have to do it (implement 3rd party solution) in consultation with our IS division. We cannot just – business units cannot go by themselves and seek third-party vendor without our internal IT division*" – **[BUR2].**

Table 6.2: Summary of the Neutralization techniques

Neutralization Technique	List of sample response
Denial of responsibility	*"So, I suppose it just depends on the available resources internally and then also – well I suppose the resources will affect the timing how quickly can you get it done. Cause then if you don't have sufficient people to do it as quickly as you want it to you either then go outside or you wait" – [BUR3].*
Denial of Injury	*"I also believe that you need to understand the criticality or the context of the problem or the issue, because if it stops business from operating then you need to be able to come up with a solution pretty fast, and sometimes the solution that it works 80% or 50% is ok. However, once that solution is implemented you need to then sit back and say ok – let's now formally do something to resolve the issue"* – **[BUR4].**
Appeal to higher loyalties	*"They needed a mobile application, and they needed it at a specific time and knowing IS/IT you would have to log something ...if you are going to follow the business processes it's going to take you a year or even to just get the personnel and the people to do that"* – **[BUR8].**

6.2.1. Denial of responsibility

The most frequently used technique of Neutralisation in this study was denial of responsibility. While end-users acknowledge that implementing SIT is wrong, they denied the responsibility for implementing IT solutions without informing the IT department – by blaming the IT department for not being able to deliver IT solutions on time. For instance, one respondent stated that:

"*They needed a mobile application and they needed it at a specific time and knowing IS/IT you would have to log something ...if you are going to follow the business processes it's going to take you a year or even to just get the personnel and the people to do that*" – **[BUR8].**

However, the AME policy states that all arms-length applications should be formally declared to the IT department even though the IT department would not provide support.

In general, end-users at EPZA are not satisfied with the service they receive from the IT department – which could lead to the implementation of SIT. For instance, one respondent made the following comment:

"*I mean it might be just an opinion but we don't feel that they've got the necessary expertise which our third-party vendors are having and this is just an opinion, personal opinion. Within the company, people tend to stay here for quite a long time. So, it is possible that maybe they don't keep abreast with what is happening out there and hence the difficulty or it might also*

just be a case of the company does to not have does not see an appetite in investing in a service that can be optimally resourceful." – **[BUR2].**

Another example of denial of responsibility was identified when the end-user indicated that the reason they implemented SIT was that the in-house IT department did not have enough employees to manage the demand from the functional department:

"*So, I suppose it just depends on the available resources internally and then also – well I suppose the resources will affect the timing how quickly can you get it done. Cause then if you don't have sufficient people to do it as quickly as you want it to you either then go outside or you wait*" – **[BUR3].**

For all the scenarios, the IT department was not informed about the IT solutions and only found out when the functional department needed to integrate the software with sanctioned systems or if they needed assistance with upgrading software.

6.2.2. Denial of injury

Another Neutralisation technique that was identified was denial of injury. While the respondents acknowledged the risks of implementing IT solutions without informing the IT department, they denied that the IT solutions they implemented could be risky to the company. One of the respondents stated that:

"*I also believe that you need to understand the criticality or the context of the problem or the issue, because if it stops business from operating then you need to be able to come up with a solution pretty fast, and sometimes the solution that it works 80% or 50% is ok. However, once that solution is implemented you need to then sit back and say ok – let's now formally do something to resolve the issue*" – **[BUR4].**

6.2.3. Appeal to higher loyalties

Another Neutralisation technique that was identified was 'appeal to higher loyalties'. This was evident when one respondent indicated that they implemented SIT for benefit of the greater part of the society (managers). For instance, one respondent stated that:

"*They needed a mobile application, and they needed it at a specific time and knowing IS/IT you would have to log something ...if you are going to follow the business processes it's going to take you a year or even to just get the personnel and the people to do that*" – **[BUR8].**

6.3. Other findings: Risk of Shadow IT

Most respondents highlighted the risks of implementing SIT. Some of the risks mentioned during the interviews were lack of business continuity strategy. When some of the respondents were asked to comment on whether there is a strategy used to ensure business continuity, it

was noted that the functional department did not focus on implementing the continuity strategy. This was evident when one of the respondents stated that:

> "*Being honest, there is not much strategy. There is someone, a colleague of mine, who once worked here and he sort of handed over his projects to me and the only thing that helped me was the emails and the documentation that he has. Other than that [laughter] you work your own way. You find out what's happening yourself because handover is not enough*" – **[BUR8]**

Another risk was that when functional department obtains a SIT solution, all they focus on is the functionality and they do not focus on whether the software would be able to integrate with the existing sanctioned systems – which in turn delays the delivery of the desired solution. One respondent stated that:

> "*Let's take the one scenario that failed - the financial model tool we purely focused on what we needed without necessarily keeping the potential risks in mind."* – **[BUR3].**

It also emerged that by not following the correct processes and procedures for implementing IT solutions, the company lost money. This was evident when one of the respondents made the following comment:

> "*Where we gave them the redesign documents but at the stage of that happened EPZA had already paid R 3 million for the other software. So, the slid it under the table just before we closed the IS gap. We basically got excluded from all meeting after that after we have told them that they have to redesign."* – **[ISR1]**

6.4. Summary of chapter

The study findings indicate that EPZA faces challenges despite the company having IT policy (Application Management Elements) to manage the implementation of new software applications. While the AME policy does not prevent the functional department from implementing their own IT solutions, functional departments are expected to inform the IT department of any IT solution they intend to implement prior to purchasing the software – so that IT can perform an architecture review to mitigate the risk. The findings also revealed that even though it is a requirement of the IT department that business units inform the IT department of all arms-length solutions, they continued to implement them without informing the IT Department. The respondents also used some Neutralisation techniques to justify the implementation of SIT and highlighted the risks and reasons for implementing SIT solutions.

7. Discussion of findings

This chapter provides a discussion of the research findings – with the aim of answering the research question and research objectives. The chapter also focuses on the emerging concepts identified in the research findings.

7.1. Summary of the research objectives

The main objective of this study was to assess the Neutralisations techniques used by end-users to justify the implementation of SIT and to investigate whether the IT department had implemented IT policies to prevent the implementation of SIT. The study was conducted in a multinational petroleum company – for ethical reasons the organisation was anonymised as EPZA. The literature on SIT suggests that end-users use Neutralisation techniques to justify the implementation of SIT (Haag & Eckhardt, 2015; Silic et al., 2017). However, the studies were based on the quantitative approach and less attention was given to the qualitative approach. This study attempted to close the gap by using the qualitative approach.

7.2. The context of Shadow IT at EPZA

The findings indicate that EPZA faces challenges despite the company having IT policy (Application Management Elements) to manage the implementation of new software applications. One of the major challenges that EPZA faces is "*... duplicate and inefficient IT-related activities ...*" [**email, CIO**] that are spread across the company. As a result, the company lost money. The finding concurs with previous studies that indicate that SIT is a significant challenge for most organisations and has major financial, legal and security implications (Chua et al., 2014; György & Cleven, 2012).

Some of the reasons for end-users bypassing the IT department were based on the previous experience with the IT department. Some end-users felt the AME policy gave them too many responsibilities to implement and manage IT solutions – even though they do not have the necessary ICT skills. This finding differs from previous studies, which indicated that end-users implement SIT solutions because of improved technical knowledge and accessibility to cloud-based solutions (Gozman & Willcocks, 2015; Zimmermann & Rentrop, 2014). In the case of EPZA, end-users felt that the circumstances in the company (e.g. lack of capacity from the IT department) contributed to them implementing SIT, even though they do not have the necessary technical skills to do so.

7.3. Revisiting assumptions

In the first chapter, the researcher made assumptions, and in this section, the researcher revisits these assumptions. The assumptions made in the first chapter were based on the knowledge acquired from reviewing the literature. The assumptions identified in the first chapter are discussed considering the research finding of this study. The summary of assumptions and findings are listed in table 7.1.

Table 7.1: Research assumptions and findings

Assumptions	Findings (Realities)
There is a policy that prevents functional departments from implementing SIT solutions.	This assumption turned out to be partially true. There is no policy which prevented functional departments from implementing their own IT solutions. However, the policy gave functional departments their own IT solutions through the arms-length agreement.
End-users who implemented SIT solutions experienced guilt and shame due to bypassing IT policy.	Most respondents did not feel guilt and shame, because they believed there was no policy that prevented them from implementing their own IT solutions.
End-users that implemented SIT respected teams or departments that follow IT department policies.	The assumption was incorrect. There was no evidence in the findings to support this assumption.
End-users who implemented SIT were able to differentiate between people (teams) who can be victimised and those who cannot be victimised.	The assumption was correct. The functional department blamed the IT department for not delivering IT solutions which met their specific needs.
End-users who implemented SIT had a desire to conform to what appeared to be acceptable to wider society at EPZA.	The assumption was correct. End-users implemented SIT to meet the needs (KPI) of the managers.

7.3.1. **Assumption 1: There is a policy that prevents functional departments from implementing SIT solutions**. This assumption turned out to be partially true. While the respondents indicated there was an IT policy for managing software applications at EPZA, the policy did not prevent end-users from implementing their own IT solutions. According to the Application Managed Element policy, end-users are encouraged to implement software using the arms-length agreement – however, all arms-length software should be declared to the IT department so that the IT department can conduct the architecture review. Nevertheless, the findings indicated that some end-users were implementing arms-length software without informing the IT department at all.

Some of the reasons for the IT department creating a policy that encourages end-users to implement their own IT could be linked to shortfalls experienced by the IT department, such

as bureaucracy and red tape that delay the delivery of IT services to the business (Behrens, 2009; Buchwald & Urbach, 2012). Also, in some instances, the IT department does not have enough human resources to manage the demand from the functional department. One end-user stated that"

> *"…if you don't have sufficient people to do it as quickly as you want it to you either then go outside or you wait*" – [**BUR3**].

So, to avoid the misalignment between the IT department's objectives and the functional department's objectives (György & Cleven, 2012) , the IT department at EPZA allowed end-users to implement their own IT solutions – provided they ask the IT department to do the architecture review to ensure that the IT solution acquired from the third-party vendor aligns with the company's strategy and security policies. This finding is in line with previous studies that indicate that SIT should be accepted because it improves end-user creativity and innovation and business performance (Haag & Eckhardt, 2015; Silic & Back, 2014; Tambo & Bækgaard, 2013).

Assumptions 2 through 5 are based on the study by Sykes and Matza (1957), who indicated that for an offender to use the Neutralisation technique to justify their behaviour, they should meet the following criteria: Firstly, the offenders should demonstrate guilt and shame about the crime they have committed. The offender should show respect and admiration toward people who abide by the law and who do not commit a crime. The offender should be able to differentiate between those who can be victimised and those who cannot be victimised. The offender should also have the desire to conform to what seems to be acceptable to wider society.

7.3.2. **Assumption 2: End-users who implemented SIT solutions experienced guilt and shame due to bypassing IT policy**. This assumption is incorrect. The findings indicated that end-users did not feel guilty for implementing SIT solutions – because they felt that the policy allowed them to implement their own IT solutions. The findings also indicated that end-users did not trust the IT department to deliver IT services on time. One of the respondents indicated that:

> "*is just in IS there is too much red tape, we are short-staffed there, [there] is too much complaining, we don't have the staff, we don't have the capacity to do this – so the business a lot of the time has to seek third-party solutions*" – [**BUR8**].

This finding is in line with that of previous studies, which suggest that the motivation behind the implementation of SIT is lack of trust and satisfaction sanctioned IT systems (Mallmann & Maçada, 2016).

It was also noted that end-users were generally unhappy with the services provided by the IT department at EPZA. Some respondents indicated that they felt that the IT department was not providing enough software options to choose from. This was evident when one of the respondents indicated that:

> "*You are tied to one specific partner where you are buying all the technology from, you leave yourself open to flexibility to be able to meet a business need, so having one specific big business partner, Lumira and SAP as an example*" – [**BUR5**].

The dissatisfaction and lack of trust in the IT department contributed to removing the guilt and shame from implementing IT solutions. Furthermore, end-users did not see the need to inform the IT department about arms-length applications, because they felt that the IT department did not provide enough support. This gave the users more responsibility to implement and manage the IT solution, even though they do not have the necessary technical skills.

7.3.3. **Assumption 3: End-users who implemented SIT respected teams or departments that follow IT department policies.** This assumption is incorrect. There was no evidence to support this finding in this study.

7.3.4. **Assumption 4: End-users who implemented SIT were able to differentiate between people (teams) who can be victimised and those who cannot be victimised**. This assumption is correct. The findings indicate that end-users felt the need to bypass the IT department because of poor IT service delivery. This is in line with previous studies, which suggested that if end-users are dissatisfied with sanctioned systems, they are most likely to implement SIT (Behrens, 2009; Györy & Cleven, 2012; Spierings et al., 2011). Usually, the dissatisfaction is caused by misalignment between the IT department's objectives and the functional department's objectives (Györy & Cleven, 2012). In this study, it also emerged that different teams in the IT department at EPZA operated in silos, the IT department deliver IT services too slowly due to red tape, the IT department lacked capacity (human resources) to manage the demand from the functional department, and there was a lack of focus on business needs. As a result, end-users didn't feel the need to inform the IT department when they implemented arms-length applications – even though it was a requirement of AME policy to

inform the IT department about all software introduced by the business for architecture review purposes. In essence, end-users blamed the IT department due to its poor service delivery.

7.3.5. **Assumption 5: End-users who implemented SIT had a desire to conform to what appeared to be acceptable to wider society at EPZA**. This assumption was correct. The findings indicated that the main focus for most end-users when they implemented SIT, was to meet the key performance indicators required by the business. So, to prevent the IT department from discontinuing software that does not conform to the IT department's policy, end-users did not inform the IT department – unless they really needed assistance from them. One respondent from the IT department indicated that:

> "*We basically got excluded from all meeting after that after we have told them that they have to redesign. So, in short, they were chasing KPIs. We have to have it in by this time even if it is not gonna work really – that is just the case it has to go in*" – [**ISR1**].

For end-users, meeting the KPIs enables them to conform to company objectives – one respondent made the following comment:

> "*the challenge now was full potential to say now depending on how quickly you want the solution if you have to have it now you would have to go to the external vendor or if you can wait till November, then she would then be able to help. So, I suppose it just depends on the available resources internally*"- [**BUR3**].

Through SIT they can achieve the objective because the business does not have to wait for the IT department to approve their project or allocate to a budget for the project. Instead, they can procure or seek assistance from external IT consultants or third-party solutions to develop the IT services that meet their specific needs – without going through red tape in the IT department (Haag, 2015; Silic & Back, 2014).

7.4. Guilt and shame

Respondents did not feel guilty for not informing the IT department about arms-length applications. Usually, the respondents felt that the IT department did not support them when they implemented arms-length applications, and hence there was no need for them to inform the IT department if they managed to successfully implement an IT solution. In most cases, end-users blamed the IT department for not delivering IT services on time. Some of the themes identified, which contributed to poor service delivery, were that the IT department operated in silos, the IT department was too slow, the IT department did not have the capacity to handle the request from the functional departments, and that the IT department did not focus on the

needs of functional departments. Accordingly, end-users did not demonstrate guilt and shame for not following the process – as stated in the AME policy.

7.5. The Neutralisation techniques

The primary objective of this study was to establish whether end-users who implement SIT used Neutralisation techniques. Of the five Neutralisation techniques identified in this study, only two were used by respondents. Most respondents did not use Neutralisation techniques to justify the implementation of SIT – because they indicated there is an IT policy that allows them to implement their own IT solutions through the arms-length agreement. While this is true, the AME policy required all end-users to notify the IT department of all arms-length IT solutions, so that the IT department can perform the architecture review to assess the security of the software and functionality of the software, in line with what is currently available in the company – to avoid duplicate functionality.

7.5.1. Denial of responsibility

End-users use the *denial of responsibility* Neutralisation technique to justify the implementation of SIT. With this technique, end-users indicated they were forced to implement SIT solutions because of poor IT service delivery by the in-house IT department. One way in which end-users used the denial of responsibility technique, was to blame the IT department for poor service delivery. Poor IT service delivery was linked to the IT department operating in silos, being too slow to deliver IT solutions, and the IT department not having enough capacity to handle requests from different functional departments.

7.5.2. Denial of injury

Another Neutralisation technique used was the *denial of injury*. With this Neutralisation technique, end-users felt that implementing a SIT solution would not create harm to the company. One way that respondents used the denial of injury Neutralisation technique was when they ignored the risk a SIT solution can pose to the company. This was evident when one of the respondents indicated that *"*sometimes the solution that works 80% or 50% is ok*"* **- BUR4.**

7.5.3. Appeal to higher loyalties

Another Neutralisation technique used was *Appeal to higher loyalties*. With this Neutralisation technique, end-users indicated that they implemented SIT to meet the KPI of the company set by the management. This was evident when one of the respondents indicated that

"They needed a mobile application, and they needed it at a specific time and knowing IS/IT you would have to log something" – [**BUR8**].

7.6. Revisiting the research question and objectives

This study inquired *"How do functional departments (end-users) justify the implementation of Shadow IT solutions?"*

The objective of this study was to investigate the justifications used by end-users who have employed SIT. The sub-objectives of this study were to:

- Investigate whether the IT department has implemented any form of IT policy or any IT control – to prevent functional departments from implementing SIT solutions.
- Assess Neutralisation techniques used by end-users to justify the implementation of SIT.

This study revealed that EPZA has a policy that allows end-users to implement their own IT solutions through the arms-length agreement – but at the same time the policy states that end-users should inform the IT department about all arms-length applications so that the IT department can perform the architecture review. The study found that most end-users did not see the need to inform the IT department about software applications implemented through the arms-length agreement because they felt they were allowed to implement their own IT solutions – thus removing guilt and shame. This finding was contrary to the assumption made by Sykes and Matza (1957), who indicated that for delinquents to use the Neutralisation techniques, they have to feel guilt and shame about the deviant action they have committed. As a result of the lack of guilt and shame, most respondents did not use Neutralisation techniques to justify the implementation of SIT. The AME policy was only revealed to the researcher during the data-collection process. Therefore, there is a need for more qualitative studies on SIT – which should investigate companies with IT policies that forbid the implementation of SIT.

7.7. Summary of chapter

This chapter portrayed the experiences of a sample of IT employees and end-users from different functional departments at EPZA. The assumptions made in the first chapter, which were based on the literature, were compared with the actual findings of this study. The Neutralisation techniques used by the end-users are revisited. The researcher also revisited

the research questions and objectives. It was found that most end-users did not feel guilt and shame about implementing SIT, and they did not use Neutralisation techniques to justify the implementation of SIT.

8. Conclusion

SIT continues to be a major challenge for most organisations and could result in financial, legal and security implications (Chua et al., 2014; György & Cleven, 2012). Earlier studies on Justification of SIT mainly used the quantitative methods to explore SIT. While quantitative studies are essential for the identification of neutralisation techniques, they are not capable of providing details on how the neutralisation techniques were employed (Boyce & Neale, 2006). Without in-depth understanding the justifications, it may be difficult to devise effective mechanisms to minimise the implementation of SIT solutions in organisations. Furthermore, previous studies examined organisations with strict IT policies for managing SIT (Silic et al., 2017). However, there was less attention to organisations which permits end-users to implement their own IT solutions. To address the research gaps, this study investigated the justifications used by end-users who had employed SIT in a multinational petroleum organisation, through the use of qualitative methods.
Conclusions drawn from this study are presented in the following section.

8.1. Summary of key findings

To situate the study, it was necessary to investigate whether the IT department at EPZA had implemented any form of IT policy or any IT control to prevent functional departments from implementing SIT solutions. The findings showed that EPZA does not have an IT policy which prevents functional departments from implementing SIT. Instead, the company has a policy which allows functional departments to implement their own IT solutions as long as they inform the IT department to assess the application for potential risks and compatibility of a SIT application with the existing landscape. The policy minimised the guilt and shame in functional departments who implemented SIT, and they felt there was no need to inform the IT department about the arms-length application since they do not receive support from IT department. The study also assessed the Neutralisation techniques used by end-users to justify the implementation of SIT.

Consequently, most respondents did not justify the implementation of SIT due to the policy which allowed them to implement their own IT solutions. Nevertheless, respondents who employed Neutralisation techniques used *Denial of responsibility, Denial of injury and Appeal to higher loyalties* to justify SIT.

8.2. Implications of the study

8.2.1. Implications for theory

This study made an empirical contribution to the Neutralisation Theory when it explored the concept of SIT using qualitative methods in a corporate setting – as opposed to earlier studies that used quantitative methods and experiments when exploring the concept of SIT (Haag & Eckhardt, 2015; Silic, Barlow, & Back, 2017). The study supports findings from earlier studies which indicated that end-users might use Neutralisation techniques to justify the implementation of SIT.

The study also made a unique discovery through the identification of the IT policy that allows end-users to implement their own IT solutions through the arms-length agreement. This policy significantly minimised the guilt and shame in end-users who implemented SIT, and they felt there was no need to inform the IT department about the arms-length application. This was since there was no support received from IT during the implementation process – even though the policy required end-users to inform the IT department about all software applications implemented through the arms-length process.

As a result, three techniques – denial of responsibility, denial of injury and appeal to higher loyalties were used by the respondents to justify the implementation of SIT. Therefore, there is a need for future studies in this domain to investigate companies with IT policies that forbid the implementation of SIT and compare these with companies with policies that allow the implementation of SIT – and see how they influence end-users to use Neutralisation techniques.

8.2.2. Implications for practice

This study found that when an organisation has an IT policy that permits end-users to implement their own IT solutions through an arms-length policy, guilt and shame are minimised – which increases the creation of SIT solutions. If the company has a policy like the AME policy that allows end-users to implement their own IT solutions through arms-length options, the IT department should regularly educate end-user about the dangers of implementing IT solutions that do not go through the architecture process. Another option would be to add a function to the procurement process to proactively discover the IT solutions

before they are implemented in the company – so that the architecture review can be conducted.

8.3. Limitations of the study

This study had several challenges and limitations. First, the researcher experienced challenges in terms of recruiting the participant. Most participants were not willing to participate due to busy work schedules. This challenge was mitigated through organising interviews during the most convenient times of the respondents (Saunders et al., 2009). Secondly, at the time when the study was conducted, the researcher was part of the IT department at EPZA – which might have influenced the way in which respondents gave their responses. The researcher also acknowledges that because this was a qualitative study, it was subject to bias in terms of data collection and interpretation. Finally, the study was conducted in a multinational oil and gas company, and, therefore, the results might not be generalisable with other industries.

8.4. Future work

The objective of this study was to investigate justifications used by functional departments which employed SIT. Based on the research findings, there is a need to examine the different IT policies for managing SIT from different organisations and how they influence the usage of Neutralisation techniques. Future studies may also focus on unpacking the reasons why end-users choose not to declare IT solutions even though there is an IT policy which states that SITs must be declared.

8.5. Final word

This study unpacked the Neutralisation techniques used by end-users who implemented SIT solutions at EPZA. The study focused on a multinational oil and gas company. The key findings of this study suggest that end-users may use “denial of responsibility” and “denial of injury” Neutralisation techniques to justify the implementation of SIT. The study informs theory and practice about the possible ways in which employees might defend the implementation SIT solutions in companies.

REFERENCES

Alshawi, S., Missi, F., & Irani, Z. (2011). Organisational, technical and data quality factors in CRM adoption - SMEs perspective. *Industrial Marketing Management*, 1–8.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers and Security*, *39*, 145–159.

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*, *13*(4), 544–559.

Behrens, S. (2009). Shadow systems : The good , The bad and The ugly. *Communications of the ACM*, *52*(2), 124–129.

Beimborn, D., & Palitza, M. (2013). Enterprise App Stores for Mobile Applications Development of a Benefits Framework. In *Proceedings of the Nineteenth Americas Conference on Information Systems* (pp. 1–11). Chicago, Illinois.

Berente, N., Yoo, Y., & Kalle, L. (2008). Alignment or Drift? Loose Coupling over Time in NASA' s ERP Implementation. In *International Conference on Information Systems (ICIS)* (pp. 1–17).

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. *Textbooks collection*.

Blichfeldt, B. S., & Eskerod, P. (2008). Project portfolio management – There's more to it than what management enacts. *International Journal of Project Management*, *26*(4), 357–365.

Bob-Jones, B., Newman, M., & Lyytinen, K. (2008). Picking Up the Pieces After a "Successful" Implementation: Networks, Coalitions and ERP Systems. In *Proceedings of the Fourteenth Americas Conference on Information Systems* (pp. 1–12).

Boyce, C., & Neale, P. (2006). Conducting In-depth Interviews: A Guide for Designing and Conducting In-Depth Interviews for Evaluation Input. *Monitoring and Evaluation*, 1–12.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Bree, R., & Gallagher, G. (2016). Using Microsoft Excel to code and thematically analyse qualitative data: a simple, cost-effective approach. *AISH-J*, *8*(2), 2811–2814.

Buchwald, A., & Urbach, N. (2012). Exploring the Role of Un-Enacted Projects in IT Project Portfolio Management. In *Thirty Third International Conference on Information Systems* (pp. 1–10).

Chua, C. E. H., Storey, V. C., & Chen, L. (2014). Central IT or Shadow IT ? Factors Shaping Users ' Decision To Go Rogue With IT. In *Thirty Fifth International Conference on Information Systems* (pp. 1–14).

Dimmler, M. (2013). *Towards a scientifically founded understanding of the shadow IT phenomenon*. University of Amsterdam.

Dubé, L., & Paré, G. (2003). Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations. *MIS Quarterly*, *27*(4), 597–635.

Friedrich, B., & Julia, K. (2016). Deviant cloud usage in public institutions - a matter of peronal innovativeness? In *Twenty-Fourth European Conference on Information Systems* (pp. 1–10).

Fuerstenau, D., & Rothe, H. (2014). Shadow IT Systems: Discerning the Good and the Evil. In *Twenty Second European Conference on Information Systems* (pp. 1–14).

Gorla, N., Somers, T. M., & Wong, B. (2010). Organizational impact of system quality, information quality, and service quality. *Journal of Strategic Information Systems*, *19*(3), 207–228.

Gozman, D., & Willcocks, L. (2015). Crocodiles in the Regulatory Swamp: Navigating the Dangers of Outsourcing, SaaS and Shadow IT. In *Thirty Sixth International Conference on Information Systems* (pp. 1–20).

Grant, C., & Osanloo, A. (2014). Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your "House." *Administrative Issues Journal Education Practice and Research*, 12–26.

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough ? An Experiment with Data Saturation and Variability. *Family Health International*, *18*(1), 59–82.

Györy, A., & Cleven, A. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. In *European Conference on Information Systems* (pp. 1–13).

Haag, S. (2015). Appearance of Dark Clouds? – An Empirical Analysis of Users ' Shadow Sourcing of Cloud Services. In *Proceedings der 12. Wirtschaftsinformatik* (pp. 1438–1452).

Haag, S., & Eckhardt, A. (2015). Justifying Shadow IT Usage. In *Proceedings of the 19th Pacific Asia Conference on Information Systems* (pp. 1–11).

Haag, S., Eckhardt, A., & Bozoyan, C. (2015). Are Shadow System Users the Better IS Users? – Insights of a Lab Experiment. *Thirty Sixth International Conference on Information Systems*, 1–20.

Haag, S., Eckhardt, A., & Schwarz, A. (2018). Information & Management The Acceptance of Justi fi cations among Shadow IT Users and Nonusers – An Empirical Analysis. *Information & Management*, (November), 1–11.

Harris, L. C., & Dumas, A. (2009). Online consumer misbehaviour: an application of neutralization theory. *Marketing Theory*, *9*(4), 379–402.

Kerr, D., & Houghton, L. (2008). Feral Systems: The Likely Effects on Business Analytics Functions in an Enterprise Resource Planning System Environment. In *ACIS 2008 Proceedings* (pp. 484–491).

Klein, H., & Myers, M. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, *23*(1), 67–94.

Kopper, A., & Westner, M. (2016). Towards a Taxonomy for Shadow IT. In *Twenty-second Americas Conference on Information Systems* (pp. 1–10).

Krauss, S. E., & Putra, U. (2005). Research Paradigms and Meaning Making : A Primer. *The Qualitative Report*, *10*(4), 758–770.

Kretzer, M. (2015). Linking Report Individualization and Report Standardization : A

Configurational Perspective. In *Twenty-Third European Conference on Information Systems (ECIS)* (pp. 1–18).

Kretzer, M., & Maedche, A. (2014). Generativity of Business Intelligence Platforms : A Research Agenda Guided by Lessons from Shadow IT. *Multikonferenz Wirtschaftsinformatik*, 207–220.

Liddick, D. (2013). Techniques of Neutralization and Animal Rights Activists. *Deviant Behavior*, *34*(8), 618–634.

Lund-Jensen, R., Azaria, C., Permien, F. H., Sawari, J., & Bækgaard, L. (2016). Feral Information Systems, Shadow Systems, and Workarounds – A Drift in IS Terminology. *Procedia Computer Science*, *100*(2016), 1056–1063.

Mallmann, G. L., & Maçada, A. C. G. (2016). Behavioral Drivers Behind Shadow IT and Its Outcomes in Terms of Individual Performance. In *Twenty-second Americas Conference on Information Systems, San Diego* (pp. 1–5).

Marshall, M. N. (1996). Sampling for qualitative research Sample size. *Family Practice*, *13*(6), 522–525.

Mcroberts, M. (2013). Software Licensing in the Cloud Age Solving the Impact of Cloud Computing on Software Licensing Models. *The International Journal of Soft Computing and Software Engineering*, *3*(3), 395–402.

Merriam, S. B. (2002). Introduction to qualitative research. In *Qualitative research in practice: Examples for discussion and analysis* (pp. 3–17). Jossey-Bass.

Myers, N., Starliper, M., Summers, S. L., & Wood, D. A. (2016). The Impact of Shadow IT Systems on Perceived Information Credibility and Managerial Decision Making. *Social Science Research Network*, *305*(801), 357–383.

Rehman, A. A. (2016). An introduction to research paradigms An Introduction to Research Paradigms. *International Journal of Educational Investigations*, *3*(8), 51–59.

Rentrop, C., & Zimmermann, S. (2012a). Shadow IT : Management and Control of unofficial IT. In *The Sixth International Conference on Digital Society Reference* (pp. 98–102).

Rentrop, C., & Zimmermann, S. (2012b). Shadow IT evaluation model. In *Proceedings of the Federated Conference on Computer Science and Information Systems* (pp. 1023–1027).

Ribeaud, D., & Eisner, M. (2010). Are Moral Disengagement, Neutralization Techniques, and Self-Serving Cognitive Distortions the Same? Developing a Unified Scale of Moral Neutralization of Aggression. *International Journal of Conflict and Violence*, *4*(2), 298–315.

Rowley, J. (2002). Using case studies in research. *Management Research News*, *25*(1), 16–27.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*. *Research methods for business students* (5th ed.). Pearson Professional Limited.

Schalow, P. S. ., Winkler, T. J., Repschlaeger, J., & Zarnekow, R. (2013). The Blurring Boundaries Of Work-Related And Personal Media Use : A Grounded Theory Study On The Employee ' s Perspective. In *Proceedings of the 21st European Conference on Information Systems* (pp. 1–12).

Shakir, M. (2002). The selection of case studies: Strategies and their applications to IS implementation cases studies. *Research Letters in the Information and Mathematical Sciences*, (3), 191–198.

Shumarova, E., & Swatman, P. A. (2008). Informal eCollaboration Channels: Shedding Light on" Shadow CIT. In *BLED 2008 Proceedings* (p. 18).

Silic, M. (2015). Shadow it – Steroids for Innovation. In *28th International Conference on Advanced Information Systems Engineering* (pp. 1–17).

Silic, M., & Back, A. (2014). Shadow IT - A view from behind the curtain. *Computers & Security*, *45*, 274–283.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & Management*, (2016), 1–15.

Spierings, A., Kerr, D., & Houghton, L. (2011). Feral Information Systems viewed through the lens of stracturation theory. In *The 11th International DSI and the 16th*

APDSI Joint Meeting (pp. 1–11).

Stake, R. (1995). The Art of Case Study Research. In *Thousand Oaks, CA: Sage* (pp. 49–68).

Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: a Theory of Delinquency. *American Sociological Review*.

Tambo, T., & Bækgaard, L. (2013). Dilemmas in Enterprise Architecture Research and Practice from a Perspective of Feral Information Systems. In *17th IEEE International Enterprise Distributed Object Computing Conference Workshops* (pp. 289–295).

Thatte, S., & Grainger, N. (2010). Feral systems : why users write them and how they add value. In *Firth pre-ICIS workshop on ES Research* (pp. 1–10).

Tien, C.-C. (2009). What Is the Truth in Market Research? Being a Truth Teller. *Asian Journal of Management and Humanity Sciences*, *4*(4), 241–258.

Urus, T., Molla, S., & Teoh, S. (2011). Post ERP Feral System and use of ' Feral System as Coping Mechanism. *World Academy of Science, Engineering and Technology*, *60*, 1050–1057.

van Teijlingen, E., & Hundley, V. (1998). The importance of pilot studies. *Nursing Standard : Official Newspaper of the Royal College of Nursing*, *16*(40), 33–36.

Yin, R. K. (2009). *Case study research : design and methods*. *Applied social research methods series* (Vol. 5.).

Zainal, Z. (2007). Case study as a research method. *Jurnal Kemanusiaan*, *5*(2), 1–6.

Zimmermann, S., Felden, C., & Rentrop, C. (2014). Managing Shadow IT Instances – A Method to Control Autonomous IT Solutions in the Business Departments. In *Twentieth Americas Conference on Information Systems, Savannah* (pp. 1–12).

Zimmermann, S., & Rentrop, C. (2014). On the emergence of shadow IT - A transaction cost-based approach. In *Twenty Second European Conference on Information Systems* (pp. 1–17).

APPENDIX A: INTERVIEW PROCEDURE

- The researcher will set up the interviews with the stakeholder – considering their most convenient time.
- On the day of the interview, the researcher will seek informed consent from the interviewee (it will be read to the respondent).
- The interviewer will only proceed with the interview, if the respondent has agreed to have the interview.
- Immediately after the interview, the researcher will summarise all the key data.
- All the data collected will also be verified.

APPENDIX B: RESEARCH INSTRUMENT

Sample Interview Guideline	
	Opening Question
	1. Which department do you work for and what is your role and responsibilities? 2. How long have been in your current role? 3. Are you aware of an IT policy which prevents functional departments from implementing 3rd party IT solutions on their own?
Denial of Responsibility	
	4. I understand that you were involved with the implementation of *SIT x*? o Which process did you follow when implementing *SITx*? o Did you consult the IT department when implementing or upgrading SITx?
Denial of Injury	
	5. How do you ensure business continuity of SITx? 6. How do you manage to keep the information on SITx accurate and up to date? 7. How did you ensure proper testing when implementing SITx?
Denial of victim	
	8. Did you consult the IT department when implementing SITx? Please explain the process?
Condemnation of condemners	
	9. How would you feel if the IS department had a policy which prevents the implementation of Shadow IT solutions?
Appeal to higher Loyalties	
	10. What were the reasons for implementing SIT x?
	Closing Questions
	11. Would you like to add anything else? *Thank you very much for your time!*

APPENDIX C: INTRODUCTORY LETTER

UNIVERSITY OF CAPE TOWN
Leslie Commerce Building
Upper Campus
Or Private Bag, Rondebosch 77001
Cape Town

Fax No: (021) 650-2280

Introductory Letter

Justification for Shadow IT by functional departments in a company

Good day

My name is Joshua Magunduni, a Master's student at the University of Cape Town. I would like to request for permission to conduct a research on the justifications for shadow IT by functional departments within a company. The main objective of this study is to assess how different functional departments justify the implementation of Shadow IT solutions.

As part of my research, I need to conduct interviews and also analyse the documents. Data collections will involve identification of Shadow IT solutions and interviewing the stakeholders associated with that. Participation to this study will be voluntary and the all data will be used for academic purposes only. The data collection process will begin in January,2017 and end March, 2017.

If you have any questions, please contact me or my Supervisor. The contact details are listed below.

Signature_____ Date _____

For questions, please contact
Joshua Magunduni
Cell phone Number: 0791819169

APPENDIX D: INTERVIEW CONSENT FORM

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

04 April 2017

Request to conduct research and interview participation consent form

Dear Sir/Madam,

In terms of the requirements for completing a Master's Degree in Information Systems at the University of Cape Town a research study is required.

The researcher, in this case Joshua Magunduni has chosen to conduct a case study entitled Justifications for Shadow IT by functional departments in a company. The objective of the research is to unpack the reasons behind the implementations IT solutions from 3rd Party Vendors by functional department.

Your participation in this research is voluntary. All information will be treated in a confidential manner and used exclusively for the purpose of this study. No individual names will be recorded or published. You will not be requested to supply any identifiable information, ensuring anonymity of your responses. You can choose to withdraw from the research at any time for whatever reason, in accordance with ethical research requirements.

The data collection method will be one-on-one interview. The interview will last maximum of 1 hour. If you are willing to participate in this study, kindly sign the attached form and return to me at your earliest convenience.

Should you have any questions regarding this research, please feel free to contact me on 0791819169 or email: mgnjos002@myuct.ac.za

Your participation in this study would be greatly appreciated, but is entirely voluntary.

Sincerely,

Joshua Magunduni
Researcher M.Com Student, (UCT)
Department of Information Systems
University of Cape Town
Email: mgnjos002@myuct.ac.za

Prof Wallace Chigona
Research Supervisor
Department of Information Systems
University of Cape Town
Email: Walace.chigona@uct.ac.za

APPENDIX E: AUTHORISATION TO CODUCT REASEARCH

To whom it may concern,

This confirms that Joshua Magunduni is employed by and works within the Information Services division as a SAP Developer.

hereby approves that Joshua completes a case study on F towards his Master's degree in Information Systems.

Our understanding s that the research will focus on Shadow IT and the reasons for the creation of Shadow IT in various departments across an organisation. I am sure that the research will be of benefit to especially in unpacking Shadow IT and also making recommendaticns on how large corporates should ceal with and structure for Shadow IT, if at all. We have been informed that data collection will be through interviews and will cover those impacted by, or initiating Shadow IT.

We understand that all information will be treated confidentially and will be used exclusively for the purpose of this study. Further, the company name will not be referenced in the study to maintain confidentiality. The company has the right to withdraw from this study should it deem it necessary.

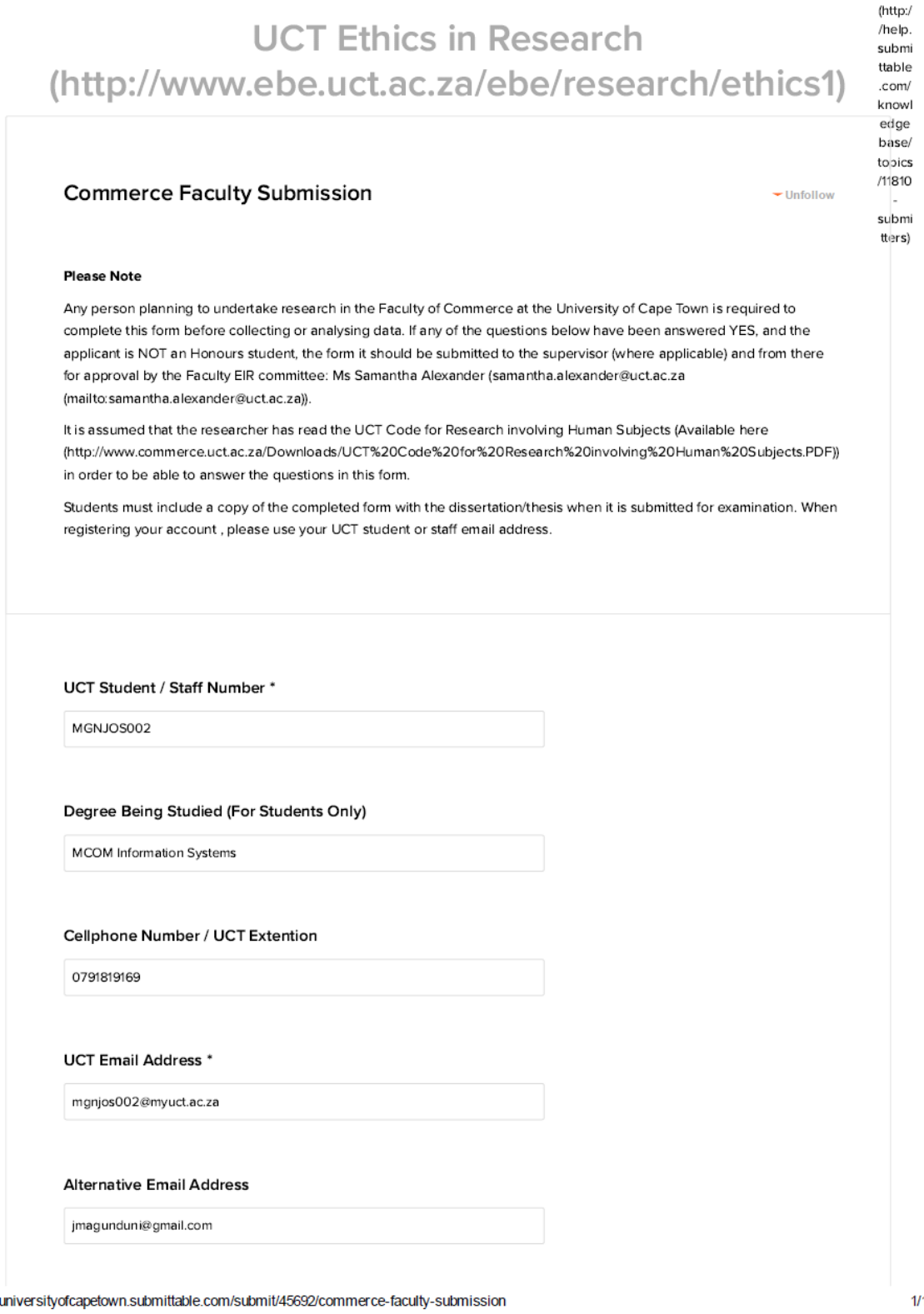
Joshua is a proactive employee and adds value to the F Information Services team. I wish him well in his studies and look forward to reading his research repcrt on completion. I am sure that completing this degree will result in personal growth and also add to his contribution to F

Regards,

Signature Removed

Chief Information Officer

APPENDIX F: UCT ETHICS APPROVAL



UCT Ethics in Research (http://www.ebe.uct.ac.za/ebe/research/ethics1)

(http://help.submittable.com/knowledgebase/topics/11810-submitters)

Commerce Faculty Submission

Unfollow

Please Note

Any person planning to undertake research in the Faculty of Commerce at the University of Cape Town is required to complete this form before collecting or analysing data. If any of the questions below have been answered YES, and the applicant is NOT an Honours student, the form it should be submitted to the supervisor (where applicable) and from there for approval by the Faculty EIR committee: Ms Samantha Alexander (samantha.alexander@uct.ac.za (mailto:samantha.alexander@uct.ac.za)).

It is assumed that the researcher has read the UCT Code for Research involving Human Subjects (Available here (http://www.commerce.uct.ac.za/Downloads/UCT%20Code%20for%20Research%20involving%20Human%20Subjects.PDF)) in order to be able to answer the questions in this form.

Students must include a copy of the completed form with the dissertation/thesis when it is submitted for examination. When registering your account , please use your UCT student or staff email address.

UCT Student / Staff Number *

MGNJOS002

Degree Being Studied (For Students Only)

MCOM Information Systems

Cellphone Number / UCT Extention

0791819169

UCT Email Address *

mgnjos002@myuct.ac.za

Alternative Email Address

jmagunduni@gmail.com

https://universityofcapetown.submittable.com/submit/45692/commerce-faculty-submission 1/10

1. PROJECT DETAILS

Project title: *

Justification for Shadow IT by Functional Departments in a Company

Enter a title for your submission

Principal Researcher/s: *

Joshua Magunduni

Enter Email address(es): * If providing more than one email address please separate the email addresses using a semicolon (;)

Status of Applicant *

- ○ Member of Academic Staff
- ○ Researcher
- ○ PhD Student
- ◉ Master Student
- ○ Other

Supervisor Name (For Students Only) :

Prof Wallace Chigona

Supervisor email address

wallace.chigona@uct.ac.za

Enter Email address(es):

Department: *

Department of Information Systems

Co-researcher(s) Names:

If providing more than one name please separate the email addresses using a semicolon (;)

Co-researcher(s) Email Addresses:

Enter Email address(es): * If providing more than one email address please separate the email addresses using a semicolon (;)

Review Track *

- ◉ Normal
- ○ Expedited

Brief description of the research project *

The main aim of this study is to unpack the rationalizations behind the implementations of Shadow IT within a company.Shadow IT is any IT solution implemented by the end-users without seeking approval from the IT department.

Please describe in 500 words the purpose of this research project

Limit: 500 words

Data collection: (please select) *

- [x] Interviews
- [ ] Questionnaire
- [x] Secondary data
- [ ] Observation
- [ ] Other*

File Upload

Acceptable file types: **pdf, doc, docx, txt, rtf, jpg, gif, png, wpf, odt, wpd.**

Upload the following files:
a. Research proposal or Literature review (no more than 10 pages)
b. Questionnaire, survey, topic guide or other relevant documentation
c. Letter of consent for participants
d. Any other relevant documentation that helps the Ethics Committee to understand the study and the ethical implications

Select up to 20 files to attach.
You have attached 5 files (827.21 KB total). You may add up to 15 more.

Introduction_Letter.docx	Attached	REMOVE FILE (/SUBMIT/REMOVEFILE?UID=465E68D3-ABB8-455F-8741-867260F675F9&PID=4
Letter_of_consent.docx	Attached	REMOVE FILE (/SUBMIT/REMOVEFILE?UID=465E68D3-ABB8-455F-8741-867260F675F9&PID=4
Literature_Review.docx	Attached	REMOVE FILE (/SUBMIT/REMOVEFILE?UID=465E68D3-ABB8-455F-8741-867260F675F9&PID=4
Research_Methodology.docx	Attached	REMOVE FILE (/SUBMIT/REMOVEFILE?UID=465E68D3-ABB8-455F-8741-867260F675F9&PID=4
Semi_structured_Interview.docx	Attached	REMOVE FILE (/SUBMIT/REMOVEFILE?UID=465E68D3-ABB8-455F-8741-867260F675F9&PID=4

Choose Files

Have you attached a research proposal with research methodology? *

- ( ) Yes
- (•) No

The research proposal may not be more than 10 pages

2. PARTICIPANTS

2.1 Please indicate below the affiliations of participants from the list below : *

- [x] Company employees
- [ ] Health sector
- [ ] General public
- [ ] Military
- [ ] Agricultural sector
- [ ] Students / Learners
- [ ] Education sector / Academic sector
- [ ] Other*

2.2 Please describe how you plan to protect the participants *

The issue of privacy is important, all respondents including their names and the names of the company will be kept confidential.

Describe how you will protect participants during and after the research. 500 Words

Limit: 500 words

2.3 Does the research discriminate against participation by individuals, or differentiate between participants, on the grounds of gender, race or ethnic group, age range, religion, income, handicap, illness or any similar classification? *

○ Yes ◉ No

2.4 Does the research require the participation of socially or physically vulnerable people (children, aged, disabled, etc.) or legally restricted groups? *

○ Yes ◉ No

2.5 Will you be able to secure the informed consent of all participants in the research? (In the case of children, will you be able to obtain the consent of their guardians or parents?) *

◉ Yes ○ No

2.6 Will any confidential data be collected or will identifiable records of individuals be kept? *

◉ Yes ○ No

2.7 In reporting on this research is there any possibility that you will not be able to keep the identities of the individuals involved anonymous? *

○ Yes ◉ No

2.8 Are there any foreseeable risks of physical, psychological or social harm to participants that might occur in the course of the research? *

○ Yes ◉ No

2.9 Does the research include making payments or giving gifts to any participants? *

○ Yes ◉ No

2.10 Race / Ethnicity - Are you asking a question about race/ethnicity in your questionnaire? *

○ Yes ◉ No

2.13 Gender - Are you asking a question about gender in your questionnaire?

○ Yes ◉ No

2.14 If you answered Yes to 2.13 - Have you included the option: "Prefer not to answer" as part of your gender question?

○ Yes ◉ No*

*** If you have selected "No" in 2.14, please explain why**

Not applicable

Maximum 300 words

Limit 300 words

3. PROVISION OF SERVICES

3.1 Does your research involve the provision of services to communities? *

Yes* No

*** If your answer is YES, please provide a brief description below:**

200 words

Limit 200 words

3.2 Is the community expected to make decisions for, during or based on the research? *

Yes* No

***If your answer is YES, please provide a brief description below:**

200 words

Limit 200 words

3.3 At the end of the research will any economic or social process be terminated or left unsupported, or equipment or facilities used in the research be recovered from the participants or community? *

Yes* No

***If your answer is YES, please provide a brief description below**

Limit 200 words

3.4 Will any service be provided at a level below the generally accepted standards?

Yes*

No

***If your answer is YES, please provide a brief description**

200 words

Limit 200 words

4. ORGANISATIONAL PERMISSION

4.1 If your research is being conducted within a specific organisation, please state how organisational permission has been/will be obtained:

A formal email was sent to the Cheif Information Officer

4.2 Have you attached the letter from the organisation granting permission? (please select) *

- (•) Yes
- ( ) No but it will be obtained before commencing the research
- ( ) Not applicable

4.2.1 If you have selected "Yes" in the question above please upload a the letter granting permission.

Acceptable file types: **pdf, doc, docx, txt, rtf, wpf, odt, wpd**.

Upload letter from the organisation granting permission

Permission_to_conduct_study.pdf Attached

REMOVE FILE (/SUBMIT/REMOVEFILE?UID=465E68D3-AB88-455F-8741-867260F675F9&PID=4

You have attached 1 file (338.35 KB). You cannot attach any more files here.

4.3 Are you making use of UCT students as respondents for your research? *

- ( ) Yes
- (•) No

4.4 Was approval granted?

- ( ) Yes
- ( ) No
- ( ) Awaiting a response

4.4.1 If you have selected "Yes" in the question above please upload a copy of the approval letter.

Acceptable file types: **pdf, doc, docx, txt, rtf, wpf, odt, wpd**.

Upload UCT Students Approval Letter

Choose Files

No files have been attached yet.

4.5 Are you making use of UCT staff as respondents for your research? *

- ( ) Yes
- (•) No

4.6 If yes, have you contacted Executive Director: Human Resources for permission ?

- ( ) Yes
- ( ) No
- ( ) Awaiting response

4.7 Was approval granted?

- ( ) Yes
- ( ) No

Contact Details

Executive Director: Human Resources - Miriam.Hoosain@uct.ac.za (mailto:Miriam.Hoosain@uct.ac.za)
Executive Director: Student Affairs - Moonira.Khan@uct.ac.za (mailto:Moonira.Khan@uct.ac.za)

5. INFORMED CONSENT

5.1 What type of consent will be obtained from study participants? *

- ☐ Oral Consent
- ☑ Written Consent
- ☐ Anonymous survey questionnaire (covering letter required and no consent form needed))
- ☐ Other (please specify)

5.2 How and where will consent/permission be recorded?

Recommended 400 words

Limit: 400 words

6. CONFLICT OF INTEREST

6.1 Is there any existing or potential conflict of interest between a research sponsor, academic supervisor, other researchers or participants?

○ Yes ◉ No

6.2 Will information that reveals the identity of participants be supplied to a research sponsor, other than with the permission of the individuals? *

◉ Yes ○ No

6.3 Does the proposed research potentially conflict with the research of any other individual or group within the University? *

○ Yes ◉ No

6.4 Are you aware of any other conflict of interest that you would like to declare ? *

○ Yes ◉ No

If you have answered YES to any of these questions, please describe how you plan to address these issues (Questions 6.1 - 6.4)

500 words

Limit: 500 words

7. RISK TO PARTICIPANTS

7.1 Does the proposed research pose any physical, psychological, social, legal, economic, or other risks to study participants you can foresee, both immediate and long range? (please select) *

○ Yes* ◉ No

*** If YES, please answer the following questions:**

7.2 Describe in detail the nature and extent of the risk and provide the rationale for the necessity of such risks

300 words

Limit 300 words

7.3 Outline any alternative approaches that were or will be considered and why alternatives may not be feasible in the study

300 words

Limit 300 words

7.4. Outline whether and why you feel that the value of information to be gained outweighs the risks

300 words

Limit 300 words

☑ **I certify that I have read the the Commerce Faculty Ethics in Research policy (http://www.commerce.uct.ac.za/Pages/ComFac-Downloads) ***

I hereby undertake to carry out my research in such a way that

* there is no apparent legal objection to the nature or the method of research; and
* the research will not compromise staff or students or the other responsibilities of the University;
* the stated objective will be achieved, and the findings will have a high degree of validity;
* limitations and alternative interpretations will be considered;
* the findings could be subject to peer review and publicly available; and
* I will comply with the conventions of copyright and avoid any practice that would constitute plagiarism.

☐ **Supervisor has seen the application**

If you are a student, you need to show your application to the supervisor prior to having it signed.
Please save your application as draft (at the bottom of this page), download it (right click on the application under the "saved draft folder" and download the linked file). Please send the file via email to your supervisor.
A second option is to click on your browser (left top corner of this window) and click on "print" and save as a pdf. Or you can export it to pdf, if your browser provides for that.

You can send at the same time the signature file (see below) so that your supervisor can sign it off

Signature *

Acceptable file types: **pdf, doc, docx, txt, rtf, jpg, gif, tiff, png, wpf, odt, wpd.**

Choose Files

Download the signature page from: here (http://www.commerce.uct.ac.za/Downloads/COM%20Ethics%20Signatories%202016.pdf)
Fill it in and have it signed. Once signed, please scan the document and upload it here.
When the application has been submitted, reviewed and approved, the Chair of the Ethics Review Committee of the Commerce Faculty will sign the document and return it to you.

No files have been attached yet.

8. CHECKLIST - Please complete the section below.

☑ **A full copy of a research proposal or a literature review with methodology is attached**

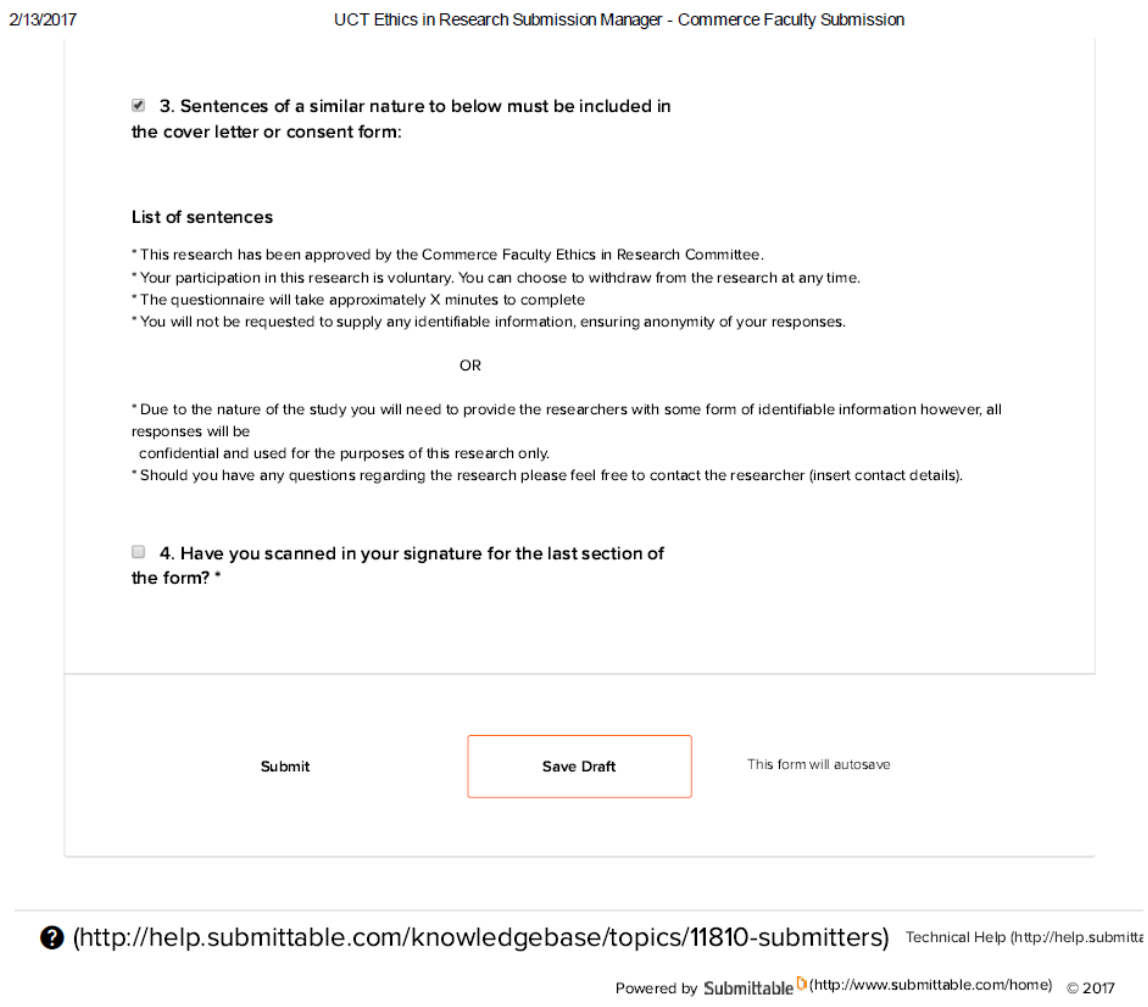
☑ **Interview schedules / cover letters / questionnaires / forms and other materials used**

☑ **Organisational consent letter / UCT student or staff approval letter**

On your cover letter to your questionnaire have you included the following?

☐ **1. The circular UCT Logo - Please see http://www.uct.ac.za/images/uct.ac.za/about/intro/logo/logocircles.gif**

☐ **2. A sentence explaining the aim of the research**



2/13/2017 UCT Ethics in Research Submission Manager - Commerce Faculty Submission

☑ **3. Sentences of a similar nature to below must be included in the cover letter or consent form:**

List of sentences

* This research has been approved by the Commerce Faculty Ethics in Research Committee.
* Your participation in this research is voluntary. You can choose to withdraw from the research at any time.
* The questionnaire will take approximately X minutes to complete
* You will not be requested to supply any identifiable information, ensuring anonymity of your responses.

OR

* Due to the nature of the study you will need to provide the researchers with some form of identifiable information however, all responses will be
confidential and used for the purposes of this research only.
* Should you have any questions regarding the research please feel free to contact the researcher (insert contact details).

☐ **4. Have you scanned in your signature for the last section of the form? ***

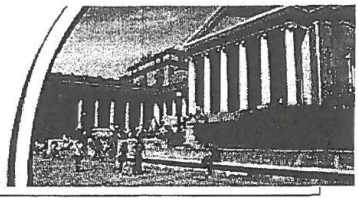
Submit | Save Draft | This form will autosave

(http://help.submittable.com/knowledgebase/topics/11810-submitters) Technical Help (http://help.submitta

Powered by Submittable (http://www.submittable.com/home) © 2017

https://universityofcapetown.submittable.com/submit/45692/commerce-faculty-submission 10/10

UNIVERSITY OF CAPE TOWN
FACULTY OF COMMERCE
Igniting Knowledge and Opportunity



Ethics Approval Request for the Study entitled: Justification for Shadow IT by functional departments in a company

Signed by:

	Full name and signature	Date
Principal Researcher/Student:	Joshua mugurduni Signature Removed	13/12/2017

This application is approved by:

Supervisor	WALLACE CHIGONA	17/12/2017
Co- Supervisor	Signature Removed	