



Cape Peninsula
University of Technology

**MANAGING INFRASTRUCTURE RISKS IN INFORMATION COMMUNICATION
TECHNOLOGY OUTSOURCED PROJECTS: A CASE STUDY AT TRANSNET,
SOUTH AFRICA**

by

DELTON JADE BASSON

Thesis submitted in fulfilment of the requirements for the degree

Magister Technologiae: Information Technology

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

Supervisor: Dr AC De La Harpe

Cape Town Campus

May 2017

CPUT copyright information

The thesis may not be published either in part (in scholarly, scientific or technical journals), or as a whole (as a monograph), unless permission has been obtained from the University

DECLARATION

I, Delton Jade Basson, declare that the contents of this thesis represent my own unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.



Signature

25 May 2017

Date

ABSTRACT

The balance between the dependency on Information and Communications Technology (ICT) and reducing costs has led to an increase in ICT outsourcing in many organisations. ICT outsourcing has benefits, but organisations have limited knowledge on information security and risks when outsourcing these functions. A lack of information security knowledge or a poor organisational risk culture carries the risk of project failure and security breaches. It is unclear how to manage information risks through the usage of ICT infrastructure risk management when outsourcing ICT projects, and this exposes organisations to ICT security risks. The aim of the study is to explore how a selected transport organisation can manage information risks through the usage of infrastructure risk management when outsourcing ICT projects.

Two primary research questions are posed namely, “what information risks does the ICT department manage when outsourcing ICT projects?”, and “how can the ICT department protect their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT?” To answer these two questions, a study was conducted at a transport organisation in South Africa. A subjective ontological and interpretivist epistemological stance has been adopted and an inductive research approach was followed. The research strategy was a case study. Data for this study was gathered through interviews (17 in total) using semi-structured questionnaires. Data collected were transcribed, summarised, and categorised to provide a clear understanding of the data.

For this study, forty findings and eight themes were identified. The themes are ICT outsourcing, information risks, costs, ICT vendor dependency, vendor access and management, risk management, user awareness, and frameworks. Guidelines are proposed, comprising six primary components.

The results point to gaps that need to be addressed to ensure that information is protected when outsourcing ICT projects. Measures need to be put in place and communication has to be improved among operating divisions. The findings lead to questions such as, “how does business create an ICT security culture to ensure that information is protected at all times”, and “does vendor access management really get the necessary attention it requires?” Further studies on human behaviour towards ICT security is needed to ensure the protection of organisations against security risks.

Keywords: Information risks, ICT outsourcing, ICT projects, ICT security, ICT vendors, ICT governance, ICT services, ICT frameworks, ICT costs, ICT infrastructure, COBIT, ISO, Risk management

TABLE OF CONTENTS

DECLARATION	II
ABSTRACT	III
TABLE OF CONTENTS	IV
LIST OF FIGURES	VIII
LIST OF TABLES	IX
GLOSSARY	X
DEFINITIONS	XII
CHAPTER 1: INTRODUCTION	1
1.1 Introduction	1
1.2 Background to research problem	1
1.3 Problem statement	2
1.4 Research questions	2
1.5 Research aim.....	4
1.6 Research methodology	4
1.6.1 Research philosophy.....	4
1.6.2 Research approach.....	4
1.6.3 Research strategy.....	4
1.6.4 Data collection	5
1.6.5 Data analysis	5
1.7 Ethics.....	5
1.8 Headline findings.....	6
1.9 Delineation of research	7
1.10 Contribution.....	7
1.11 Summary.....	7
CHAPTER 2: LITERATURE REVIEW	9
2.1 Introduction	9
2.2 Outsourcing.....	11
2.2.1 ICT outsourcing.....	11
2.2.2 ICT outsourcing: Core and non-core functions	13
2.2.3 ICT contracts and selection.....	13
2.2.4 Relationship and alignment between the outsourcing business and ICT vendor.....	14
2.3 Risks.....	16
2.3.1 ICT outsourcing risks	17
2.3.2 Outsourcing contract risks.....	18

2.3.3	Offshore outsourcing risks.....	18
2.3.4	Infrastructure risks.....	18
2.3.5	ICT security risks.....	19
2.4	ICT governance.....	20
2.5	Risk management	22
2.6	ICT outsourcing frameworks.....	26
2.7	User awareness	33
2.8	Conclusion	34
CHAPTER 3: RESEARCH METHODOLOGY		37
3.1	Introduction	37
3.2	Research philosophy.....	38
3.2.1	Ontology	39
3.2.2	Epistemology	40
3.3	Research approach.....	41
3.4	Research strategy	42
3.4.1	Case study	43
3.4.2	Sampling	43
3.4.3	Unit of analysis.....	44
3.5	Data collection	44
3.6	Data analysis	45
3.7	Ethics	46
3.8	Summary.....	47
CHAPTER 4: ANALYSIS AND FINDINGS.....		49
4.1	Introduction	49
4.2	The case	49
4.3	The participants.....	50
4.4	Findings	53
4.4.1	Interviews.....	53
4.4.2	Summary of the findings.....	72
4.4.3	Summary of findings and theme development.....	76
4.5	Themes.....	79
4.6	Summary.....	81
CHAPTER 5: DISCUSSION		83
5.1	Introduction	83
5.2	The themes	84

5.2.1	Theme 1: ICT outsourcing.....	84
5.2.2	Theme 2: Information risks.....	85
5.2.3	Theme 3: Costs.....	87
5.2.4	Theme 4: ICT vendor dependency	88
5.2.5	Theme 5: Vendor access and management.....	89
5.2.6	Theme 6: Risk management	91
5.2.7	Theme 7: User awareness	94
5.2.8	Theme 8: Frameworks	95
5.3	The proposed guidelines	96
5.4	Answering the research questions	99
5.5	The aim.....	100
5.6	Conclusion	100
 CHAPTER 6: RECOMMENDATIONS, REFLECTION AND CONTRIBUTIONS.....		102
6.1	Recommendations	102
6.2	Reflection	103
6.3	Contribution to research	103
6.4	Contribution to Information Technology.....	104
6.5	Contribution to law and compliance.....	104
6.6	Limitations of research	104
 REFERENCES		106
 APPENDIX A: INTERVIEW GUIDE TEMPLATE.....		121
APPENDIX B1: INTERVIEW ANSWERS OF PARTICIPANT 1.....		125
APPENDIX B2: INTERVIEW ANSWERS OF PARTICIPANT 2.....		130
APPENDIX B3: INTERVIEW ANSWERS OF PARTICIPANT 3.....		135
APPENDIX B4: INTERVIEW ANSWERS OF PARTICIPANT 4.....		140
APPENDIX B5: INTERVIEW ANSWERS OF PARTICIPANT 5.....		145
APPENDIX B6: INTERVIEW ANSWERS OF PARTICIPANT 6.....		150
APPENDIX B7: INTERVIEW ANSWERS OF PARTICIPANT 7.....		155
APPENDIX B8: INTERVIEW ANSWERS OF PARTICIPANT 8.....		161
APPENDIX B9: INTERVIEW ANSWERS OF PARTICIPANT 9.....		165
APPENDIX B10: INTERVIEW ANSWERS OF PARTICIPANT 10.....		170
APPENDIX B11: INTERVIEW ANSWERS OF PARTICIPANT 11.....		176
APPENDIX B12: INTERVIEW ANSWERS OF PARTICIPANT 12.....		181
APPENDIX B13: INTERVIEW ANSWERS OF PARTICIPANT 13.....		185
APPENDIX B14: INTERVIEW ANSWERS OF PARTICIPANT 14.....		190

APPENDIX B15: INTERVIEW ANSWERS OF PARTICIPANT 15.....	195
APPENDIX B16: INTERVIEW ANSWERS OF PARTICIPANT 16.....	201
APPENDIX B17: INTERVIEW ANSWERS OF PARTICIPANT 17.....	205
APPENDIX C: CONSENT LETTER OF COMPANY TO CONDUCT RESEARCH	210
APPENDIX D: EXAMPLE OF ANALYSIS OF INTERVIEW DATA.....	213
APPENDIX E: SUMMARY OF INTERVIEW RESPONSES	215

LIST OF FIGURES

Figure 2.1: The ICT outsourcing process	14
Figure 2.2: First Assessment Framework Analysis (FMEA).....	29
Figure 2.4: Framework for service configurations decisions	31
Figure 2.3: Risk Measurement Outsourcing Framework	32
Figure 2.5: FARM outsourcing matrix.....	33
Figure 3.1: The research process	37
Figure 3.2: Graphical presentation of how ontologies, epistemologies, methodologies, methods, and data sources fit together	39
Figure 3.3: Nature of social sciences	40

LIST OF TABLES

Table 1.1: Research Question 1 and research sub-questions	3
Table 1.2: Research Question 2 and research sub-questions	3
Table 2.1: Failures/gaps within FMEA phases	30
Table 4.1: Job title, years of experience, and work specification of participants	51
Table 4.2: Findings of SRQ 1.1	73
Table 4.3: Findings of SRQ 1.2	73
Table 4.4: Findings of SRQ 1.3	73
Table 4.5: Findings of SRQ 1.4	74
Table 4.6: Findings of SRQ 2.1	74
Table 4.7: Findings of SRQ 2.2	75
Table 4.8: Findings of SRQ 2.3	75
Table 4.9: Findings of SRQ 2.4	76
Table 4.10: Findings and related themes for RQ 1	76
Table 4.11: Findings and related themes for RQ 2	77
Table 4.12: Themes developed based on RQ 1 and research sub-questions	80
Table 4.13: Themes developed based on RQ 2 and research sub-questions	80

GLOSSARY

Abbreviation	Full Word / Term
AD	Active Directory
APN	Access Point Name
BEE	Black Economic Empowerment
CCTV	Closed-Circuit Television
COBIT	Control Objective for Information Related Technology
DC	Domain Controllers
DRP	Disaster Recovery Plan
EIMS	Enterprise Information Management Systems
FARM	Flexibility Absorptive Capacity, Relationship and Monitoring
FMEA	First Assessment Framework Analysis
FIPS	Federal Information Processing Standards
HQ	Headquarters
ICT	Information and Communications Technology
IP	Internet Protocol
IS	Information Systems
ISO	International Standardisation Organisation
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
MCS	Monte Carlo Simulation
MIT	Massachusetts Institute of Technology
OD	Operating Division
SME	Small and Medium enterprises
SMME	Small, Medium and Micro-sized enterprises
SLA	Service Level Agreement
SOP	Standard Operating Procedure
TFR	Transnet Freight Rail
TIA	Transnet Internal Audit

Abbreviation	Full Word / Term
TP	Transnet Pipelines
TPT	Transnet Port Terminals
TNPA	Transnet National Port Authority
TRE	Transnet Rail Engineering
VPN	Virtual Private Network

DEFINITIONS

Word/Term	Definition
Frameworks	“Conceptual structures used to solve or address complex issues” (Gulla & Gupta, 2012:30)
Governance	“Is the way something is controlled and management as the act of controlling” (O’Neill, 2014:343)
ICT outsourcing	Handover of ICT functions to a third party or company that is within the country or outside, with the aim of achieving strategic advantages (Samantra, Datta & Mahapatra, 2014)
Information security	“Activities, processes, controls and efforts that aim to protect information and data; and their underlying infrastructures” (Khidzir, Mohamed & Arshad, 2013a)
Outsourcing	The process of assigning work that was previously done internally to an external organisation (Sohail, 2011:370)
Risk	Any unexpected problem or threat that needs attention in order to prevent dissatisfaction of a project (Saetang & Haider, 2014)
Risk management	“Strategies, methods and supporting tools to identify, control risk to an acceptable level” (Talet, Mat-zin & Houari, 2014:2).
Security	Lockdown of a system or putting measures in place to reduce or deny abuse (Nunes-Vaz & Lord, 2013)

CHAPTER 1: INTRODUCTION

1.1 Introduction

In the corporate environment, more and more organisations become dependent on Information and Communications Technology (ICT) (Coertze & Von Solms, 2013b). Many organisations outsource their ICT functions to achieve their objectives and to prepare for changes that may occur in the corporate environment (Talet et al., 2014; Abdullah & Verner, 2012). According to Sohail (2011), ICT outsourcing dates back to the early 1960's when Perot's electronic data systems were sourced by Frito-Lay and Blue Cross to process their data. Since then, outsourcing has become popular and numerous large and small organisations are outsourcing their ICT activities. Several factors have led to the popularity of outsourcing ICT such as cost, quality, flexibility, and skills (Nassimbeni, Sartor & Dus, 2012; Sohail, 2011).

Even though ICT outsourcing has become popular, the management of information risks is still problematic within organisations. Information risks increase when outsourcing ICT technologies to other organisations. In a South African transport organisation several ICT technologies and functions are outsourced, but certain information risks associated with the outsourcing process are not identified and managed properly.

To identify the information risks and determine how these information risks can be managed, research are conducted within a transport organisation by means of interviews with the aim of exploring how the transport organisation can manage information risks by using infrastructure risk management when outsourcing ICT projects.

1.2 Background to research problem

The balance between the dependency on ICT and reducing costs has led to an increase in ICT outsourcing in many organisations (Yap, Lim & Jalaludin, 2016; Mohammad & Jafari, 2014; Hamlen & Thuraisingham, 2013). According to Yap et al. (2016) and Wickramasinghe (2015), one of the strategies followed by business to reduce costs and skill shortages for ICT services is to outsource ICT functions. Yap et al. (2016) support Patil and Wongsurawat (2015) and explain that literature reports mention ICT outsourcing as a method to reduce ICT costs. Hamlen and Thuraisingham (2013) as well as Murthy, Karim and Ahmadi (2015) go a step further and identify dependency on ICT, cuttings of cost, and globalisation as reasons for the increase in ICT outsourcing.

Although ICT outsourcing has its benefits, organisations have limited knowledge of information security and risks that should be considered when outsourcing ICT functions (Hamlen & Thuraisingham, 2013; Urbach & Würz, 2012; Herath & Kishore, 2009). Hamlen and Thuraisingham (2013) as well as Mubarak (2016) agree that when outsourcing ICT services there is an increase in security vulnerabilities, because most organisations have limited knowledge of the ICT outsourcing risks. Urbach and Würz (2012) elaborate on this issue and state that organisations with little outsourcing experience will face problems when outsourcing ICT projects.

As a result of a lack of information security knowledge or a poor organisational risk culture, organisations carry the risk of project failures and security breaches such as hacking, which could lead to unauthorised access of information (Mubarak, 2016; Talet et al., 2014; Marabelli, Newell & Zang, 2013; Khidzir, Mohamed & Arshad, 2013b). Khidzir et al. (2013a) and Marabelli et al. (2013) highlight a number of ICT security risks that can be associated with ICT outsourcing, including leakage of information and data theft. Talet et al. (2014) and Karlsson, Kolkowska and Prenkert (2016) also identify other ICT risks at a higher level, including security breaches, ICT financial problems, failure of ICT projects, and unstable business. Aundhe and Mathew (2009) as well as Hamlen and Thuraisingham (2013) state that there is a gap in literature on security needs for outsourcing ICT.

1.3 Problem statement

It is unclear how to manage information risks through the usage of ICT infrastructure risk management when outsourcing ICT projects, and this exposes organisations to ICT security risks.

1.4 Research questions

To address the research problem, two primary research questions are asked. Firstly, “what information risks does the ICT department manage when outsourcing ICT projects?”, and secondly, “how can the ICT department protect their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT?” From these primary research questions, research sub-questions are created. Tables 1.1 and Table 1.2 indicate the research questions, research sub-questions, methodology used to answer the research questions, and the objective of each research question.

Table 1.1: Research Question 1 and research sub-questions

Research Questions	Methodology	Objective
RQ 1: What information risks does the ICT department manage when outsourcing ICT projects?	Case study using semi-structured questions/interviews	To determine what information risks the ICT department manages when outsourcing ICT projects
SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?	Case study using semi-structured questions/interviews	To establish what type of access ICT vendors have to Transnet's information and systems
SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?	Case study using semi-structured questions/interviews	To determine the highest information risk of outsourcing ICT projects at Transnet
SRQ 1.3: What strategies do the ICT department have in place to manage information risks associated with ICT outsourcing?	Case study using semi-structured questions/interviews	To establish what strategies the ICT department has in place to manage information risks associated with ICT outsourcing
SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?	Case study using semi-structured questions/interviews	To determine what the ICT department does to ensure that ICT vendors adhere to the strategies that are put in place

Table 1.2: Research Question 2 and research sub-questions

Research Questions	Methodology	Objective
RQ 2: How can the ICT department protect their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT?	Case study using semi-structured questions/interviews	To determine how the ICT department protects their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT functions
SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks / threats from inside and outside Transnet?	Case study using semi-structured questions/interviews	To determine how the ICT department deals with ICT infrastructure security risks/threats from inside and outside Transnet
SRQ 2.2: How does the ICT department ensure that they do not become dependent on their ICT service providers?	Case study using semi-structured questions/interviews	To establish how the ICT department ensures that they do not become dependent on their ICT service providers
SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet information against ICT infrastructure security threats when outsourcing ICT functions?	Case study using semi-structured questions/interviews	To examine how the ICT department uses ICT frameworks to protect their information against ICT infrastructure security threats when outsourcing ICT functions
SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?	Case study using semi-structured questions/interviews	To investigate how the ICT department ensures that ICT vendors adhere to their security and compliance requirements

1.5 Research aim

Researchers conduct research with different aims, namely to explore, describe, explain, evaluate, or predict phenomena (Neuman, 2010). The aim of this study is to explore how the transport organisation can manage information risks through the usage of infrastructure risk management when outsourcing ICT projects.

1.6 Research methodology

1.6.1 Research philosophy

Ontology: Ontology can be defined as “an explicit specification of a conceptualisation” (Moreira, Martimiano, Brandão & Bernardes, 2008:154) or “the study of the kinds of things that exist” (Chandrasekaran, Josephson & Benjamins, 1999:20). Neuman (2010:92) identifies two ontology positions: realists and nominalists. Realists (objective ontology) assume that the “real world” is not dependent on humans and their understanding thereof to exist. Nominalists (subjective ontology) assume that humans have their own view of reality. For this study, a **subjective ontological stance** is followed as the researcher sees himself within the real world and is part of the case used for the research.

Epistemology: Neuman (2010:93) describes epistemology as “the issue of how we know the world around us or what makes a claim about it true”. Neuman (2010) recognises three epistemology approaches: positivism that adopts a realist position, interpretivism or phenomenology that explains there are multiple ways of looking at things in reality, and the critical theory tradition that is a combination of positivism and interpretivism. The research adopted an **interpretivist** epistemological stance since the researcher is interpreting the data collected from the interviewees to make claims about the truth.

1.6.2 Research approach

When conducting research, the investigator can follow one of two research approaches known as inductive and deductive research (Neuman, 2010). The researcher conducted an investigation to formulate a theory; therefore, an inductive approach was followed to explore how Transnet can manage information risk via ICT infrastructure risk management when outsourcing their ICT projects.

1.6.3 Research strategy

To answer the research questions and sub-questions a case study was done on a transport organisation. According to Yin (2009), the purpose of a case study is to formulate a theory, hence the reason for an inductive approach. For the case study,

the unit of analysis has been identified as ICT professionals and the unit of observation as ICT managers and ICT security experts.

1.6.4 Data collection

Neuman (2010) identifies several methods to collect data, including the analysis of existing documents, observations, interviews, and questionnaires. For this investigation, data collection was done by means of interviews with semi-structured questionnaires using an interview guide.

1.6.5 Data analysis

Neuman (2010) identifies two data analytical techniques, known as qualitative and quantitative data analysis. This research made use of qualitative data analysis techniques. Once the data collection process was completed, the data collected were summarised, organised, and categorised. The summarised and categorised data were then further put through a thematic analysis process.

1.7 Ethics

Ethics: Resnik (2011:1) defines ethics as “norms for conduct that distinguish between acceptable and unacceptable behavior”. According to Resnik (2011), ethical norms are learned at home, school, church, or any other social environment. Throughout the research process, the researcher adhered to ethical norms.

The researcher obtained a consent letter from Transnet to collect data from participants. Participants who were unable to give informed consent had not been considered during the data collection process. Although the researcher obtained a consent letter, the researcher also adhered to the conditions as stipulated in an agreement between the researcher and Transnet.

Data collected during the literature review and data collection process were not fabricated or falsified. All contributors to the literature review were acknowledged and no form of unpublished data was used without permission. During the interview process, the interviewee had the right to walk out at any time if he/she felt uncomfortable with the questions asked.

The confidentiality of data collected during the interview process was protected and not discussed with colleagues. Data collected will not be published without consent of Transnet. The researcher ensured that the results of the research are honest and research data will be kept for any enquiries that may arise in future. The research

paper will only be submitted to one institution with the goal of advancing research and knowledge.

1.8 Headline findings

Forty findings are formulated in Chapter 5 based on the analysis of interview answers collected during the research process. From these 40 findings, ten (10) headline findings are identified, of which the following four (4) are the primary headline findings.

Headline finding 1: Vendor access and management

The management of vendor access requires more attention when outsourcing ICT functions. From the research, it can be said that processes for ICT vendor access management are not enforced or reviewed frequently as required and that access restriction is not always specific. This could be because of key suppliers having full access to the systems and network infrastructure as core systems are hosted by an ICT vendor, or the disagreement among participants on how levels of access to systems and networks are or should be granted to ICT vendors.

Headline finding 2: Risk management

There is no specific definition for information risks within the organisation where the study has been conducted. What makes it worse, is that several participants are not aware of methods used to determine the impact of information risks when outsourcing ICT projects, even though it has been found that exploiting or disclosure of confidential information to third parties is seen as the highest information risk when outsourcing ICT.

No direct mechanisms exist to deal with the risks of infrastructure outsourcing within the organisation where the study has been performed, and those risks are managed through *ad-hoc* security assessments.

The ICT department is highly dependent on the ICT service provider; they do not have any plans in place to replace ICT vendors immediately if anything goes wrong. This is seen as a risk that needs to be address by business when deciding to outsource ICT functions.

Headline finding 3: Vendor compliance

Compliance to ICT security is seen as an important factor when outsourcing ICT. Compliance issues are not addressed immediately when picked up by the outsourcing business and most participants are not even aware of criteria used to

measure the ICT security success rates of ICT vendors. Another issue that has been identified under vendor compliance is that primary vendors do not convey rules to secondary vendors. This causes information security challenges as primary contracts of the outsourcing business stipulate that secondary vendors must adhere to the same rules as the primary vendor.

Headline finding 4: User awareness

The human factor remains an issue when it comes to ICT security issues. From the research, it is found that the ICT department does have ICT training programmes in place, but it does not cover infrastructure security risks associated with ICT outsourcing. There is minimal awareness training on infrastructure security risks because of cost cuts.

Due to user unawareness of ICT security and information risks associated with ICT outsourcing, end-users sometimes deal directly with ICT vendors, bypassing security controls; this opens the gate to more ICT security challenges. Further studies on human behavior towards ICT security is needed to ensure that organisations and information are protected.

1.9 Delineation of research

There are several risks that need to be managed when outsourcing ICT projects, such as financial, technology, security, and information risks as indicated in the literature review. This research only focused on managing information risks through the usage of infrastructure risk management when outsourcing ICT projects.

1.10 Contribution

Guidelines are proposed to assist business in managing information risks through the usage of infrastructure risk management when outsourcing ICT projects, as well as exposing risks and presenting ways to manage the risk and add knowledge to the research area. The research contributes towards information technology as well as law and compliance as discussed in Chapter 6.

1.11 Summary

The management of information risks remains a challenge to organisations that outsource their ICT functions. In Chapter 1, the author provides the reader with a broad overview of the problem statement, followed by the research questions. The main research questions are expanded on by formulating research sub-questions as well as the methodology used to answer each question. The objective of each question is also presented. The aim of the study is to explore how the transport

organisation can manage information risks through the usage of infrastructure risk management when outsourcing ICT projects.

For the research methodology, a subjectivist stance with an interpretivist approach has been adopted. A case study research strategy at a transport organisation in South Africa was used. The data were collected using semi-structured questionnaires followed by the data analysis methods of summarising, categorising, and a thematic analysis. An explanation of the ethics that were applied throughout the research process followed. Four headline findings are presented and the chapter concludes with the delineation and contribution of the research.

In Chapter 2, the literature review is done by identifying keywords from the title, problem statement, research questions, and aim of the study. The keywords are then used to explore the literature.

Chapter 3 provides details of the research methodology used in the research, which includes the research philosophy, research approach, research strategy, data collection techniques, and how the data were analysed.

In Chapter 4, information of the case used in the research is discussed. In this chapter, the interviews conducted during the research process are analysed and findings are formulated based on the analysis of the interview answers from the 17 participants.

Chapter 5 provides the reader with a discussion on the findings, and guidelines are proposed to solve the phenomena under investigation.

Chapter 6 concludes the research with recommendations, a reflection, and contributions of the research.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

ICT plays a vital role in industrial and service delivery organisations, as it helps to reduce costs and decrease supply time (Safari & Yu, 2014). According to Mohammad and Jafari (2014), the investment in ICT increased from 32% to 52% in 2012. Despite the increase in ICT expenditure, ICT projects have a reputation to fail (Talet et al., 2014). The failure of ICT projects is a major risk since many organisations are dependent on ICT to run their daily tasks (Borghoff, 2014). Mohammad and Jafari (2014) explain that the cost of ICT services and information systems (IS) development is increasing and has become a concern for management (Mohammad & Jafari, 2014). As a result of the increased cost, more organisations are turning to external vendors to manage their ICT functionalities (Lee, Lim & Yap, 2013; Ceazer, Cavusogly & Srinivasan, 2010).

The outsourcing of ICT by businesses is an important strategy many organisations apply to lower ICT risks. The management of information risk through the usage of ICT infrastructure when outsourcing ICT projects exposes organisations to even greater ICT security risks. It is unclear how to manage information risks through ICT infrastructure risk management when outsourcing ICT projects, which exposes organisations to ICT security risks. As a result, the aim of this study is to explore how organisations can manage information risks through the usage of infrastructure risk management when outsourcing ICT projects.

The literature review was done by identifying keywords from the title, problem statement, research questions, and aim of the study. The keywords were then used to explore the literature. The exploration of the literature was done through accessing the CPUT library's electronic databases such as Google Scholar, Emerald, EBSCOhost, Scopus, Science Direct, and Springer Link.

More and more organisations are considering the adoption and usage of ICT as an important factor in their business (Shaikh & Karjaluto, 2015). ICT as a tool is integrated into processes, procedures, and products within entire organisations, governments, and communities (Schware, 2013). Bahl and Wali (2014) explain that business has become critically dependent on the use of ICT. According to Bayrak (2013), organisations are using ICT to make informed decisions and develop competitive advantages in order stay ahead in the market. In addition to this, more small and medium enterprises (SMEs) are inventing new methods to benefit and

improve ICT usage in the business, and at the same time limit their investments in ICT to fit the company's needs. Bahl and Wali (2014) support Bayrak (2013) by stating that in most organisations, ICT is treated as a support service and therefore business needs to understand how ICT can provide them with a sustainable competitive advantage. It is also pointed out that business still manages ICT in such a way to minimise costs and not to maximise the contribution ICT offers the business. Shaikh and Karjaluto (2015) provide a shorter description by explaining that ICT is used by individuals to accomplish their goals and needs while Schenkl, Sauer and Mörtl (2014:296) define technology in ICT as "knowledge for solving technical problems". For an organisation to be successful, ICT must be seen as an integral part and not as an option to business (Bayrak, 2013).

Shaikh and Karjaluto (2015:2) explain that "computers have been considered as one of the most important inventions in the 20th century and the future technology trends exclusively emphasise enhancement in human-computer interaction". Kilubi (2015) support Shaikh and Karjaluto (2015) by stating that over the last half century, technology has improved the life quality of people enormously. ICT has developed in such a way that physical presence of manpower is not needed to perform an activity, since individuals are able to perform these activities or task remotely through ICT (Pawlak, Polak & Sivakumar, 2014). Singh and Karn (2012:273) explain that we live in the information age where technology allows us to send information easily and quickly around the world without any difficulties. Information that is being send, is collected, processed, and stored in ICT systems, which makes information a valuable and critical asset to the organisation to survive; therefore information must be kept safe and protected at all times (Bahl & Wali, 2014). Silva, de Gusmão, Poletto, Silva and Costa (2014) support Bahl and Wali (2014) by saying that information can be seen as the most important asset to the business and threatened by several risks. To protect the organisation's information assets, the implementation of proper governance and risk management is the key to successful information protection (Humphreys, 2008). The management of risks and governance will be discussed in detail at a later stage in this chapter.

Traditionally, information products and services are the responsibility of the internal ICT department; this, however, is changing as ICT outsourcing becomes an alternative (Narasimhaiah & Somers, 2014). Information products and services can include ICT projects such as the development of software, communications, and security infrastructure. In an attempt to sustain competitive advantages, as

mentioned at the beginning of this chapter, organisations, small and large, are outsourcing some or even all their ICT activities (Sohail, 2011).

2.2 Outsourcing

The outsourcing of ICT has become a strategy that is widely accepted and continues to grow as it has the ability to satisfy the needs of vendors and clients by creating a business model that is attractive for both parties on the universal business playground (George, Hirschheim & Von Stetten, 2014:107). Outsourcing is the process of assigning work that was previously done internally to an external organisation (Sohail, 2011:370). Nassimbeni et al. (2012:406) provide a broader description by referring to outsourcing as the relocation of activities and processes to an external organisation or service provider regardless of their location, while offshore outsourcing refers to relocation of activities and processes to a country other than where the business or service provider is situated. Outsourcing has become a strategy that does not only perform certain functions of a department, but also could include an entire department as it is seen as a required component to obtain a competitive advantage in the new millennium (Pratap, 2014). The outsourcing strategy is used by several industries, from manufacturing to ICT services (Zhu, 2015). Lee, Yeung and Hong (2012) suggest that outsourcing of functions should be part of a business's long-term strategy and not just a short-term benefit. It is also suggested that business needs to have measures in place to ensure that outsourcing strategies are implemented effectively (Kang, Wu, Hong, Park & Park (a), 2014).

2.2.1 ICT outsourcing

ICT outsourcing refers to the handover of ICT functions with the aim of achieving strategic advantages. These functions include IT assets, the hosting of websites, ICT infrastructures, training of staff, auditing of ICT security, and application development to a third party or company within or outside of the country (Samantra et al., 2014; Sá-soares, Soares & Arnaud, 2014; Lee et al., 2013; Khidzir et al., 2013a; Urbach & Würz, 2012; Narasimhaiah & Chiravuri, 2011). Bachlechner, Thalmann and Maier (2014:39) state the following: "ICT outsourcing mean[s] that a client organisation, called service user, delegates the continuous responsibility for the provision of a specific IT service under a contract that includes a service level agreement (SLA) to a third party, called service vendor". These ICT activities or ICT services can include help desks, network support, management of applications/systems (Vorontsova & Rusu, 2014), as well as development of software (Patil & Wongsurawat, 2015).

ICT outsourcing always consists of agreements between at least two participants; on the one hand is the outsourcing recipient, referred to as the “outsourcing business” or “client”, and on the other hand is the outsourcing provider known as the “ICT vendor” (Murthy et al., 2015; Vorontsova & Rusu, 2014; Sá-soares et al., 2014). ICT outsourcing is still regarded as an important ICT strategy for many outsourcing organisations (Schmidt, Müller & Rosenkranz, 2015) and seen as common practice in business (Samantra et al., 2014). Mann, Folch, Kauffman and Anselin (2015) explain that the ICT outsourcing strategy seems to be an option for many organisations, but the implementation is complex since business needs to find vendors that suit their needs, interview the prospective vendors, and perform cost-benefit analyses. Several studies on ICT outsourcing have been conducted over the past 20 years (Mann et al., 2015; Gonzalez, Gasco & Llopis, 2015; Narasimhaiah & Somers, 2014; Gonzalez, Llopis & Gasco, 2013; Deng, Mao & Wang, 2013; Kite, 2012; Lacity, Willcocks & Khan, 2011; Fink, 2010; Chou & Chou, 2009; Crow & Muthuswamy, 2003; Willcocks & Choi, 1995; Willcocks, Fitzgerald & Feeny, 1995; Altinkemer, Chaturvedi & Gulati, 1994; Martinsons, 1993; Takac, 1993). For example, a study done by Narasimhaiah and Somers (2014) shows that the satisfaction level for ICT outsourcing is only 33%, while it is between 70-80% for non-ICT outsourced activities. The authors also report that out of 164 outsourced ICT projects only 70 were successful or continued until the end of the lifecycle. The existing 94 projects were either given to new ICT vendors or discontinued.

According to Narasimhaiah and Somers (2014), the ICT outsourcing market makes out 67% of all international outsourcing deals. Patil and Wongsurawat (2015) indicate that ICT outsourcing has become a worldwide industry worth \$536 billion. Numerous reasons are mentioned in literature for the outsourcing of ICT, such as allowing the outsourcing business to cut costs, focus on core functions, and at the same time improve efficiency (Murthy et al., 2015; Patil & Wongsurawat, 2015; Teo & Bhattacharjee, 2014; Yildiz & Demirel, 2014; Kang et al., 2014; Samantra et al., 2014). Although most of the organisations outsource their ICT for cost cutting reasons, a study on more than 100 organisations that outsourced their information technology processes shows that there are various hidden costs revealed over time after agreements are signed (Pratap, 2014). Bahli and Rivard (2013) support Pratap (2014) by stating that many organisations have cancelled their ICT outsourcing contract due to hidden or higher costs than expected. Samantra et al. (2014) go a step further and explain that even though ICT outsourcing is seen as beneficial to the company, these benefits are accompanied by risks that are not always easy to handle or manage, such as hidden costs and unexpected output. ICT managers are

still trying to convince executives that the outsourcing of ICT is not always cost effective or a strategy for cutting costs (Bahli & Rivard, 2013). Other problems identified with outsourcing of ICT include the outsourcing business that runs the risk of becoming dependent on the vendor (Yildiz & Demirel, 2014), poor service delivery, opportunistic vendor behaviors, and a lack of capabilities of the vendors to provide service (Nassimbeni et al., 2012). According to Schwarz (2014), a study conducted by KPMG found that 72% of their customers do not have criteria for measuring the success rate of ICT outsourcing, as it is difficult to determine the success rate of ICT outsourcing.

When outsourcing ICT services, organisations should look at several factors such as security compliance, risk management, and financial matters (Bahl & Wali, 2013). Selecting the wrong vendor could lead to negative consequences for the ICT projects that are outsourced by business (Watjatrakul, 2014).

2.2.2 ICT outsourcing: Core and non-core functions

Once business decides that outsourcing is part of their strategy, they need to define their core and non-core functions in order to decide which ICT services will be outsourced (Tafti, 2005). Many organisations outsource their non-core functions to focus on their core functions or core competencies (Zhang, 2015). Bayrak (2013) explains that an organisation needs to determine which applications support the core functions of the business in order for business to decide which applications they need to insource or outsource. Once this process is completed, business can start with the vendor selection and contract processes.

2.2.3 ICT contracts and selection

One factor that could influence the ICT outsourcing strategy is the contract and selection process of ICT vendors (Samantra et al., 2014). Li and Wan (2014) state that it is a complex process to select an ICT vendor. ICT vendors could lie about their knowledge and capabilities just to get a contract (Bahli & Rivard, 2013). It is therefore important that the outsourcing business looks at vendor qualifications and has an evaluation process in place when selecting a vendor. Li and Wan (2014) suggest a self-explanatory process of seven phases that guides the outsourcing business when considering an ICT outsourcing strategy, as illustrated in figure 2.1.

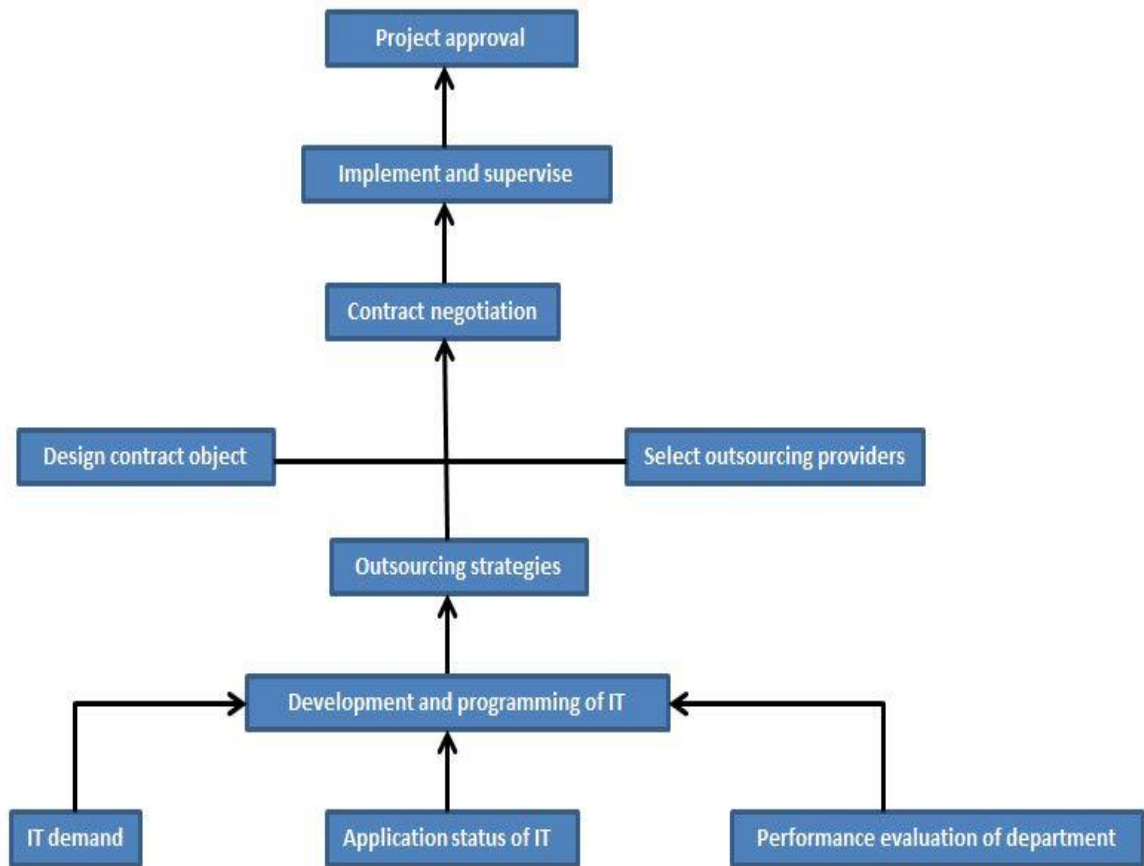


Figure 2.1: The ICT outsourcing process
(Li & Wan, 2014:72)

Usually when business decides on a vendor, there is a SLA in place that can be used for various reasons such as reward/penalty agreements and identifying the responsibilities of both parties (Petri, Rana, Regzui & Silaghi, 2012). Tafti (2005) suggests that outsourcing business includes a reversible clause in the contract that could provide them with the option of buying back essential services and equipment; for example, human reversibility may allow business to hire individuals that were employed by the ICT vendor to acquire their services and skills. According to Pratap (2014), there is still a gap in terms of effectively managing the outsourcing agreement.

2.2.4 Relationship and alignment between the outsourcing business and ICT vendor

The dependency on ICT by business has grown (Tøndel, Line & Jaatun, 2014) in such a way that when developing strategic ICT systems, many organisations depend on ICT vendor resources, capabilities, and processes (Abdullah & Verner,

2012). Coertze and von Solms (2013b) explain that the dependence on ICT by business has increased and ICT is present in almost every business process, which makes it a requirement for the business to operate effectively and efficiently. Bayrak (2013) elaborates that a major disadvantage of outsourcing is that the business can become heavily dependent on a vendor delivering critical functions to the business, and as a result, loses control over the processes. Sometimes the outsourcing businesses are locked in the ICT relationship in such a way that they cannot get out without incurring costs or losing assets (Bahli & Rivard, 2013). It is also true that the outsourcing of relationships does not stay the same, but changes over time (Kutsikos & Sakas, 2014); therefore, it is important that vendor relationships are managed properly to ensure that both parties are happy with contractual agreements (Bachlechner et al., 2014). Tate and Ellram (2009) state that poor alignment occurs between ICT vendors and the outsourcing business due to a lack of change management.

For an ICT outsourcing relationship to be successful, mutual trust and sharing of knowledge are important factors (Teo & Bhattacharjee, 2014). These factors include flow of information, brainstorming ideas to improve processes, and sharing of experiences gained over time (Duhamel, Gutierrez-Martinez, Picazo-Vela & Luna-Reyes, 2014). Lee et al. (2012) advise that businesses have a strong long-term relationship with a single vendor, but then again, having more than one vendor for a function opens the doors to negotiation. Karyda, Mitrou and Quirchmayr (2006) state that having a single vendor for the total outsourcing of ICT functions can be seen as a high risk.

Vendors can also be under pressure because of contractual agreements to deliver and therefore outsource some of their ICT functions to other vendors who specialise in a specific area; this makes the whole process difficult to manage (Bachlechner et al., 2014). Furthermore, Narasimhaiah and Somers (2014) identify vendor commitments, effectiveness, slow implementation, and the ability to understand information needs and poor service as problems associated with the ICT outsourcing relationship. It has been found that only 40% of vendor-client relationships work out effectively or can be seen as successful (George et al., 2014). According to Vorontsova and Rusu (2014), a good relationship between the outsourcing business and ICT vendor will always contribute to the success of the ICT outsourcing relationship or agreement. Sá-soares et al. (2014) add to factors influencing a good relationship by saying that in order for vendor-client relationships to be successful, risks need to be managed.

2.3 Risks

Saetang and Haider (2014) describe a risk as any unexpected problem or threat that needs attention to prevent dissatisfaction of a project. In order to be classified as a risk two features must be present in projects, namely uncertainty and loss (Talet et al., 2014). Business must consider the various risks related to ICT outsourcing before they make their final decision (Tafti, 2005). Talet et al. (2014) identify the top five ICT risks in projects as i) shortage of personnel, ii) unreasonable schedules and budgets, iii) incomplete requirements, iv) unrealistic expectations, and v) software not delivered on time. Other risks that can be associated with ICT outsourcing include contracts that are incomplete, vendors knowing the processes better than the clients, unrealistic expectations, and failure to develop in-house skills (Karyda et al., 2006). Qi, Qingling, Wei and Zhu (2012) add long-term hidden costs, dependency on service providers, and service levels not met as risks associated with ICT outsourcing. Abdullah and Verner (2012) explain that risks seen as potentially critical by business must be highlighted, as it can contribute to the failure of projects.

It is also important that managers understand the possible risks each outsourced project holds so that they can attempt to minimise the impact of risks and ensure that outsourced ICT projects are implemented successfully (Talet et al., 2014). Risks associated with ICT outsourcing are viewed as an important factor that needs to be considered when outsourcing ICT activities (Sá-soares et al., 2014). When outsourcing ICT services or systems to a third party there are various risks involved (Patil & Wongsurawat, 2015; Kumar, Sharma & Chauhan, 2014). According to Kang et al. (2014), risks in outsourcing agreements can arise because of a lack of control over ICT vendors.

According to Nassimbeni et al. (2012), external security risks increase as a result of outsourcing, for example, access of sensible data given to service providers and sub-contractors. Security risks can be caused by internal as well as external factors and are sometimes seen as a challenging task due to complex environments (Feng, Wang & Li, 2014). Bayrak (2013) highlights the fact that at corporate level of the organisation, directors and investors care more about how the applications can help increase revenue and decrease costs. Smaller amounts are invested into ICT security as they believe the risks of ICT security are not high (Silva et al., 2014). Business needs to determine the cost of security to ensure that the ICT strategies they want to implement will be effective (Leszczyna, 2013).

2.3.1 ICT outsourcing risks

Narasimhaiah and Chiravuri (2011) predict that ICT outsourcing will continue to grow in the international market even though ICT projects are associated with so many risks. Risks of ICT outsourcing include the loss of innovation and dependency on ICT vendors (Gulla & Gupta, 2012). This means that the relationship between the client and ICT service provider may have grown in such a way that the service provider ends up knowing the business processes and ICT services better than the client, ensuring a dependency on the ICT service provider (Aundhe & Mathew, 2009). Other risks include security breaches, project failures, disputes in courts, and costs that were not expected (Talet et al., 2014). Narasimhaiah and Chiravuri (2011) also refer to poor services, vendors that are not committed, and slow implementation processes as problems that can be associated with ICT outsourcing.

There are different factors leading to these risks. Elitzur, Gavius and Wensley (2012) explain that it is not always easy to determine if ICT service providers act in the best interest of their clients, and business cannot always monitor the suppliers' behavior (Chakravarty, Grewal, Sarker & Sambamurthy, 2014). For example, unauthorised personnel may have access to the systems from outside and use their access to perform attacks such as installing viruses (Hamlen & Thuraisingham, 2013).

Another issue that makes the ICT outsourcing process vulnerable is that organisations outsource their ICT functions to more than one vendor, which makes it difficult to manage their ICT infrastructure (Bachlechner et al., 2014). For this reason, it is important that security issues of ICT outsourcing should be examined and addressed by business and all the suppliers involved (Hamlen & Thuraisingham, 2013). Cheng (2012) states that ICT security risks associated with ICT outsourcing are only investigated by a few researchers. This is ironic since vulnerabilities to malware attacks and risks increase when ICT functions are outsourced (Hamlen & Thuraisingham, 2013).

Failure of ICT outsourcing will not only affect the service provider but also the client (Aundhe & Mathew, 2009). One ideal example is the outsourcing of firewalls and virtual private network (VPN) management. Firewalls and VPN management are seen as the most popular ICT security functions that are outsourced. These functions are viewed as important as it helps to detect intrusions and monitor security (Ceazer et al., 2010). The failure of the firewalls and VPN could lead to security breaches and disputes in courts, as mentioned previously.

2.3.2 Outsourcing contract risks

Two types of contract risks can be identified when it comes to outsourcing. Firstly, pre-contract risks can be found when selecting an unsuitable vendor due to unawareness of the level of expertise required from the vendor to perform the activities. Secondly, the post-contract period when vendors make decisions on behalf of the business is a hazard as the business cannot always deal with or monitor unsatisfactory actions and performances of the vendor (Narasimhaiah & Somers, 2014). Several organisations do not have any methods in place to determine if they should make or buy services. It has been found that many organisations base their decision on cost cutting and reduction of staff, and not on what makes long term business sense (McIvor, 2000).

2.3.3 Offshore outsourcing risks

As mentioned in section 2, offshore outsourcing refers to ICT work being performed by a service provider situated in a country other than the client. Due to geographical differences, various risks can be identified as a result of time zone differences, legislations, or security and privacy problems (Gonzalez, Llopis & Gasco, 2013; Kumar et al., 2014). It is also true that ICT vendors can employ employees who are not fully qualified as requested by the outsourcing business to perform certain activities, or the ICT vendor can make changes to technologies and processes of the outsourcing business without the knowledge of the client (Kumar et al., 2014). Nassimbeni et al. (2012) explain that geographical factors can become an issue when business uses offshore outsourcing, especially when it comes to providing 24/7 support service as well as infrastructure and laws that can have an impact on contractual agreements.

2.3.4 Infrastructure risks

Various sectors depend on information infrastructures to conduct their daily activities and achieve business goals (Chatzipoulidis, 2015). By outsourcing technology and applications, organisations are able to save on ICT investments and still get the required data, infrastructure, and software they need (Bayrak, 2013); but outsourcing the information system architecture and activities that go hand-in-hand for a long period can cause problems for the business as it is difficult and costly to rebuild their own ICT infrastructure. Onyeji, Bazilian and Bronk (2014) agree with Bayrak (2013) and elaborate that dependence on ICT infrastructure and systems to business has opened the door to several threats and risks, which could have devastating consequences on various parts of the organisation and systems. Furthermore, vendors may be sharing facilities that are used for processing with

other business competitors, which can also be seen as a risk (Fink, 1994). Górnjak-Kocikowska (2008:13) points out that in some organisations, the “infrastructure is not able to change quickly enough in response to the challenges posed by computer-based ICT”.

2.3.5 ICT security risks

Security has always to do with the lockdown of a system or putting measures in place to reduce or deny abuse (Nunes-Vaz & Lord, 2013). When talking about information and computer security, security can be seen as different ways in which computer resources are set up to be accessed and utilised, and is also known as availability, confidentiality, and integrity of resources (Webb, Ahmad, Maynard & Shanks, 2014; Khidzir et al., 2013a; Von Solms & Van Niekerk, 2013). Albrechtsen (2015) refers to computational security as the process of preventing and detecting unauthorised personnel and activities attempting to access a system unlawfully. For the purpose of this research attention is given to information risks and security, referred to as ICT security or information security. Khidzir et al. (2013a:2018) define information security as “activities, processes, controls and efforts that aim to protect information and data, and their underlying infrastructures”. According to Onyeji et al. (2014), ICT security is on the top-10 list of concerns for businesses in 2013. It is therefore important that business identifies information security requirements to ensure that information assets of the organisation are secured when it comes to information security risks (Khidzir, Mohamed & Arshad, 2013b). ICT security is usually associated with technology, while risks are viewed as a “human characteristic” (Munteanu & Fotache, 2015:415). When it comes to information security, humans are identified as the weakest link (Tsohou, Karyda & Kokolakis, 2015) as they have access to most of the organisation’s information (Shropshire, Warkentin & Sharma, 2015). AlHogail (2015) agrees that information security must be seen as both a technological and human issue, since security will only work if employees understand and adhere to the policies and procedures put in place by business.

Due to the dependency on ICT by business, ICT security has become an important factor when managing risks (Feng et al., 2014). It is clear that at some stage, an organisation will face some kind of incident related to information security (Tøndel et al., 2014). Nazareth and Choi (2015) indicate that the management of information security to protect assets is critical for business and is still seen as a challenging task as security incidents increase. Silva et al. (2014) state that there are still managers not having the necessary knowledge to put controls in place in order to

deal with ICT security abuse. This could be seen as a huge risk, since ICT managers and information security personnel must be able to identify and understand ICT related issues to be able to address the sources of the threat properly (Shropshire et al., 2015).

Although there are many ways to protect information and prevent information security incidents, business will not be able to protect all their ICT systems as it is not always economically feasible (Nazareth & Choi, 2015). Barham (2014) proposes that information security cover various media types and not only electronic formats. Regarding information security incidents occurring in the organisation, employees are still seen as the largest contributors (as mentioned earlier) (Veiga & Martins, 2015). For this reason, when developing information security policies, procedures, and awareness programmes, it is important that the outsourcing business and ICT vendor do not only focus on controls in terms of technology and processes, but also include human elements such as norms, beliefs, and attitudes (Veiga & Martins, 2015; Rocha Flores, Antonsen & Ekstedt, 2014). Rastogi and von Solms (2012), however, state that information security is still seen as a technical issue and is the responsibility of technical staff in most organisations. Then again, the success of information security is not always only dependent on technical aspects put in place, but also on user behavior while using ICT systems (Montesdioca & Maçada, 2015). Albrechtsen (2015:86) makes the statement that “if you think technology can solve your security problems, then you do not understand the problems and you do not understand the technology”.

Furthermore, when it boils down to selecting an ICT outsourcing vendor, Bahl and Wali (2014:3) point out that “information security assurance along with corporate governance, risk management, quality and other factors” must be taken into consideration. Although this may be important, managers and developers do not make any effort to understand how the end-users see information security, but rather use their own interpretation of how end-users view information security (Rastogi & Von Solms, 2012). Information security is driven by information security governance, which forms part of corporate governance (Bahl & Wali, 2014).

2.4 ICT governance

According to O'Neill (2014:343), “governance is the way something is controlled and management as the act of controlling” and implementing good governance enables business to have a decision making process that is clear and ensures transparency. Good governance should also include ICT governance, which consists of

leadership, structures of the organisation, and processes that will allow business to manage, control, and extend their strategies and objectives (Juiz, Guerrero & Lera, 2014). Mesquida and Mas (2014) explain that since the mid-nineties, ICT organisations began showing interest in best practices in terms of implementing and managing the various services to meet the needs of customers. One of the standards for best practices that are mostly implemented is ISO 9001, which has to do with system quality management. In the past years, a few other standards have appeared to improve processes, including ISO 27001 and COBIT as discussed in Chapter 1.

ICT governance focuses on how secure, effective, and legal information is handled by business. Several developing countries have started implementing various ICT tools to solve the age-old problem of the absence of/poor ICT governance which includes technical, legal, and organisational protection tools (Barham, 2014). Technical tools refer to hardware and software that can be used to protect the business against intentional or unintentional attacks. These tools can include firewalls, antivirus software, password protection mechanisms, and digital signatures when performing activities. Legal protection tools consist of contracts and IP rights allocated to the organisation. Contracts assist both parties to ensure that data and knowledge produced are protected and not exploited. The registration of IP rights ensures that IP violations do not occur in certain countries that may have a weak legal system. Organisational protection tools include policies, procedures, and controls used by the organisation for managing recovery plans and threat prevention. These tools can be in the form of assigning responsibilities to individuals and description of processes (Singh & Karn, 2012).

Many organisations consider ICT risks and governance to be an ICT problem, but it should be seen as a business governance matter (Everett, 2011). Misuraca, Broster and Centeno (2012) make it clear that governance cannot be change because of new ICT opportunities, but Singh and Karn (2012) argue that all areas of governance can be penetrated using the capabilities of ICT. This means that service delivery, information, and knowledge management will be more efficient and effective if ICT is used properly.

According to Bahl and Wali (2014:4), over the past years several organisations experienced losses and failures due to “inadequate security, privacy, and governance” of information. For this reason, it is suggested that corporate governance, ICT governance, and security governance need to be aligned so that

business does not only see security as a technology issue. In an ideal world, the individuals responsible for the information security tasks report to the board or the corporate governance department. This is not always possible, but information security professionals should at least ensure that the information risks identified are included in the risk register of the business (Everett, 2011). Although the board of directors may have realised how critical ICT is for the business and may increase their involvement in the governance of ICT, they do not have full control over ICT. This may be as a result of a lack of ICT expertise or knowledge at board level (Coertze & Von Solms, 2013b).

Ayogu and Bayat (2010) explain that in South Africa, it is not really the lack of oversight when it comes to ICT governance being the problem, but the willpower of business to drive the oversight. To implement ICT governance standards, there are various ICT governance frameworks (Juiz et al., 2014). Frameworks can be referred to as a graphical presentation of things that need to be done (Soni & Kodali, 2013). Everett (2011) states that it can vary from months to years for an organisation to become fully compliant to a framework, as policies, procedures, and controls need to be implemented and enforced throughout the organisation in order to be audited.

Implementing and enforcing policies, procedures, and controls usually takes time, which contributes to the compliancy factor. Information security controls have an impact on how employees view information, systems, and processes (Veiga & Martins, 2015). The effectiveness of policies, procedures, and controls for ICT functions remains the responsibility of the client; thus, the client needs to make sure the controls that are put in place are evaluated and sufficient (Mazza, Azzali & Fornaciari, 2014).

2.5 Risk management

Risk management focuses on risk identification, determining the acceptable level of tolerance, formulating strategies for risk mitigations, and putting action plans in place should a predicted risk occur (O'Neill, 2014). Risk management usually consist of two parts: firstly, reducing the circumstances of the risk before it happens, and secondly, dealing with a risk after it occurred (Ghosh, Boswell, Kwak & Skibniewski, 2011). Talet et al. (2014:02) define risk management as “strategies, methods, and supporting tools to identify, control risk to an acceptable level”. Various domains such as management, operations, and economics have studied risk and risk management as well as addressed each risk in a certain way based on its object of analysis. The management of risk can be seen as one of the primary

objectives of an organisation, especially if business is conducted globally (Tate & Ellram, 2009). Although business may know which risks impact on a project, it is more important to know what risks are common as these are difficult to mitigate (Abdullah & Verner, 2012). Risk assessments cannot not be done in a single phase; it needs to be an iterative process when formulating a risk management plan (Lee et al., 2012). When risk assessment is performed on information security, more attention is given to technical factors than social and cultural factors (Munteanu & Fotache, 2015). According to Qi et al. (2012), it is difficult to determine the effectiveness of a risk treatment plan. Once the risk assessment is completed, business should ensure that implemented actions (risk treatments) enable them to secure the organisation.

The main goal of ICT risk management is to secure the information systems responsible for retrieving, processing, exporting, and storing the organisation's information in such a way that business can make informed management decisions that justify the investment into ICT expenditures (Talet et al., 2014). To manage ICT projects effectively, business needs to adopt and implement the various risk management principles, tools, and techniques. Business must also consider other aspects when implementing risk management methods, including technology, market, financial, and operational factors which must be tied into the project life cycle (Ghosh et al., 2011). Humphreys (2008) suggests that once a risk has been identified, it needs to be captured in a risk register. The risk register should include the severity, impact, and type of risk in order to develop a risk profile of the business; secondly, management needs to measure the cost vs benefit factor of having controls in place to mitigate identified risks against not having any controls in place. Once business decides on the controls to put in place, they need to provide training to staff, showing employees how the controls work and allocating security-related responsibilities and roles to individuals.

Lee et al. (2012) go a step further and identify five stages/phases for formulating a risk management plan. Stage 1 identifies the risk events when outsourcing and stage 2 determines the probability, impact, and detection of the risk/s identified in stage 1. In stage 3, business should state the consequences of each risk and have an understanding of the impact of the risk/s. In stage 4, it is important to understand the cost and benefit factors of any outsourcing decisions, and statistical techniques can be used as a method for determination these factor impacts. In stage 5, business should develop an action plan for each risk and lastly repeat the process, as solving the one risk could have various consequences on other risks.

ICT projects are not free of risks. In addition, the risks encountered during the implementation of ICT projects are not simply due to financial factors. It is the responsibility of ICT project managers to take an overall look of the risks and not simply focus on financial risks. Other risks that can be identified during ICT projects include employee risks, technology risks, and business process management risks (Talet et al., 2014). According to Sterlicchi (1996), most security breach threats stem from within the organisation. Security breaches are usually associated with failures due to technical issues, vulnerabilities in the systems not being addressed, behavior of humans towards security, and fraud by various stakeholders (Silva et al., 2014). Many organisations suffer major losses and have to pay huge fines due to system breaches, attacks, and poor procedure and policy process controls (O'Neill, 2014).

Khidzir et al. (2013a) state that information security risks are viewed as the highest risks when outsourcing ICT projects; the management of information security with processes and systems is also seen as a critical issue (Sommestad, Hallberg, Lundholm & Bengtsson, 2014; Marabelli et al., 2013). Information security risks can include leakage of information, theft of employee data, and utilisation of intellectual property (Khidzir et al., 2013a). Previous studies have proven that few organisations invest in information security (Marabelli et al., 2013). Coertze and von Solms (2013a) support these statements and explain that due to a lack of resources and expertise, numerous small, medium, and micro-sized enterprises (SMMEs) do not adhere to proper information security governance principles. This problem has a huge impact on SMMEs, as it occurs worldwide.

The management of information security risks of ICT projects remains a problem for organisations, whether the ICT project is outsourced or not (Liu & Wang, 2014). Von Solms, Thomson and Maninjwa (2011) recommend that business protects their systems at different access levels, namely logical access to the systems, and computer network access to ensure that networks are reliable and not vulnerable. Von Solms, Thomson and Maninjwa (2011) further suggest that information security should be properly implemented from the highest to lowest levels, since information is seen as one of the most important assets of business.

The problem with the recommendations is that a number of organisations have limited knowledge of information security and risks that should be considered when outsourcing ICT functions (Hamlen & Thuraisingham, 2013; Urbach & Würz, 2012). What makes the problem worse is that budgets for ICT departments are limited and

ICT departments do not always have the funds to invest in ICT security processes and systems (Marabelli et al., 2013).

Another contributor to ICT security risks is ICT service providers finding it challenging to provide compliance and assurance against security breaches (Bahl & Wali, 2013). Bachlechner et al. (2014) explain the importance of ICT vendors to provide proof that they adhere to security requirements, as this fulfilment is the main reason why organisations stay away from complex ICT outsourcing arrangements. Bahl and Wali (2013) elaborate on the security requirements issue and ask the following question—ICT outsourcers may have all the latest technology and processes for security, but do they adhere to the security services required of them?

Several methods have been developed to reduce the information security risks associated with ICT outsourcing and adhere to security requirements, for example, Cheng (2012) suggests that employees having access to confidential information must go through security authentication and sign that they agree to the security and confidentiality measures put in place by business. This is needed because information security threats to resources can arise from inside and outside the organisation (Sommetstad et al., 2014). Cheng (2012) further proposes that internal networks should be isolated from public networks to reduce ICT security risks.

From a business perspective, Blazent (2010) recommends that SLAs between business and ICT vendors include security and vulnerability issues. Khidzir et al. (2013a) support this suggestion and state that when outsourcing ICT projects, business should ensure that they have an appropriate plan in place to minimise the risks associated with the project. In terms of ICT service providers, Herath and Kishore (2009) explain that ICT suppliers are not always 100% sure of the technical requirements when they bid, as incomplete information is sometimes provided by business. Khidzir et al. (2013a) suggest that when ICT projects are outsourced, ICT security experts should pay more attention to information security and technical requirements. Another challenge highlighted throughout this paper is the lack of awareness of ICT security. Bachlechner et al. (2014) explain that one of the major role players in ICT outsourcing is people. ICT service providers need to ensure that their employees know the importance of security and compliance by making use of proper ICT governance.

Humphreys (2008:250-252) suggests the following processes/methods to manage information security and determine the effectiveness of information security management within the organisation:

- i) Recording of system and network service usage by employees
- ii) How procedures are used and followed by employees
- iii) Auditing of servers
- iv) Auditing of internal activities
- v) Monitoring and reviewing of firewalls and intrusion detection systems
- vi) Feedback and suggestion to improve security weaknesses from customers, vendors, and employees
- vii) Access should be given to individuals based on the responsibilities and duties they have on a daily basis. Access requests should be formally documented and approved by an authorised person. If employees are moved to a new position, their access needs to be reviewed and amended accordingly
- viii) Business needs to have a measurement process in place to measure the effectiveness of controls such as the testing of segregation duties that are implemented, access control effectiveness, user awareness, and the monitoring of system resources

Moreira et al. (2008) report that although there are several tools on the market to assist administrators in determining vulnerabilities in their system, the problem is that these tools are designed to detect specific attacks and do not cover all security needs; for example, a network scanner will only scan for vulnerabilities on the network. Rastogi and von Solms (2012) argue that technology tools can be used to control and monitor end-user behavior, as technology is regarded as more reliable than end-users.

Everett (2011) states that when conducting an audit, it is not necessary for business to follow controls that are implemented as long as business has well documented reasons for deviating from the controls or making certain decisions. According to Karyda et al. (2006), business should align ICT security strategies with business objectives. For organisations to manage security, they need a framework that enables business to think about information security on various levels, not only on a technical level (Moreira et al., 2008), but if business does not understand and manage risks, it could lead to financial losses and failure of projects (Abdullah & Verner, 2012).

2.6 ICT outsourcing frameworks

According to Gulla and Gupta (2012:30), frameworks can be defined as “conceptual structures used to solve or address complex issues”. These frameworks assist

managers in understanding what to do, when to do, and how to do things when carrying out ICT outsourcing processes. A number of documents related to ICT governance have been produced by national and international organisations for using ICT effectively and efficiently (Bin-abbas & Haj, 2014).

Abu-Musa (2010) references a number of frameworks that organisations can implement to ensure best practice. Some of the frameworks include Control Objective for Information related Technology (COBIT), International Standardisation Organisation (ISO) 17799, and FIPS Production Publication 200. Bin-abbas and Haj (2014) also mention ISO 38500, the Massachusetts Institute of Technology (MIT) IT governance method and the ISO 2000 as frameworks that can be used. Other frameworks and methods developed in recent years include “the conceptual framework of IT outsourcing” with the main focus on concentrating on the core functions of business and outsourcing less critical functions, which include the following:

- ICT (Lee et al., 2013)
- The Fountains Framework, focusing on factors that influence the design, development, implementation, and use of technology by business (Duhamel et al., 2014)
- ISO 27005, recommending ICT security risk management methods (Wahlgren, Bencherifa & Kowalski, 2013)
- Information Systems (IS) Framework, assisting managers in deciding the appropriate IS outsourcing level for their business

These frameworks and methods can help organisations to measure information security performances, assess security risks, and develop security controls appropriate for the risks identified in the outsourcing process (Bin-abbas & Haj, 2014).

A number of frameworks associated with outsourcing or ICT outsourcing can be found in literature (Kutsikos & Sakas, 2014; Pratap, 2014; Shamala, Ahmad & Yusoff, 2013; Lee et al., 2012; Abdullah & Verner, 2012; Nassimbeni et al., 2012; Karyda et al., 2006). The author will discuss some of these frameworks and shortcomings or gaps that can be found, starting with COBIT and ISO 38500.

According to Bin-abbas and Haj (2014:262), COBIT can be described as a framework that provides “support to the business requirements of the organisations concerned”. Alramahi, Barakat and Haddad (2014:194) provide a more in depth description of COBIT and state that the aim of COBIT is “to research, develop,

publish, and promote an authoritative, up to date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals, and assured professionals”.

COBIT can be broken down into *plan*, *do*, *check*, and *act* to provide a governance direction. The framework considers the available ICT resources and the performance criteria required for those resources. If the resource is data, business needs to plan and organise the data and ensure that the quality of the data is on standard, based on the criteria used. Another example can be the acquiring and implementation of application systems; if business implements application systems (resource), they must ensure that the application can be trusted and contains the security requirements (Bin-abbas & Haj, 2014).

COBIT is seen as the most complete IT governance framework, but due to the lack of academic studies or case studies on this governance framework, the effectiveness and actual use of COBIT is not clear (Mangalaraj, Singh & Taneja, 2014; Zhang & Fever, 2013). As previously mentioned, to use COBIT as an ICT governance support tool, business must have a great deal of knowledge of the framework (Simonsson, Johnson & Wijkström, 2007). Zhang and Fever (2013) as well as Mangalaraj et al. (2014) support this statement and identify a lack of guidance to implement COBIT as an ICT governance framework in an established ICT environment and complex structures as some of the weaknesses of COBIT.

COBIT consists of 34 ICT processes, 222 control objectives, and more than 300 key performance indicators (KPIs). These ICT processes are divided into four domains, known as *plan and organise*, *acquire and implement automated solutions*, *deliver*, and *support* (Khther & Othman, 2013). Zhang and Fever (2013) argue that COBIT consists of too many goals and metrics; for example, how is it possible that management can review more than 300 KPIs on a daily basis to ensure that ICT performances are on track? According to Mataracioglu and Ozkan (2011), COBIT does not always give details on “how” to perform certain things when implementing the ICT framework, but focuses mostly on “what” must be done. This may be the reason why the study conducted in 2008 and 2010 found that the usage of COBIT as an ICT governance framework has reduced from 12% to 10% (Zhang & Fever, 2013). Another study performed on 1,562 random companies found that only 30% of the companies know of COBIT, while only 6% of the 1,562 companies use the ICT governance framework to some extent (Mangalaraj et al., 2014).

Bin-abbas and Haj (2014:262) explain that: “ISO 38500 provide[s] guiding principles on effective, efficient, and acceptable use of IT”. Six basic issues or principles and a development process are associated with these principles. The basic issues consist of *responsibility, strategy, acquisitions, performance, conformance, and human behavior*. The development process comprises three phases known as *evaluate, direct, and monitor*. One example that can be used is the evaluation of ICT support and ICT strategies. Business needs to evaluate ICT support based on the requirements of business and direct ICT strategies in such a way that it satisfies the overall business strategies.

According to Sylvester (2011), ISO 38500’s main objective is to provide directors with a structure of principles in order to evaluate, direct, and monitor usage of ICT within the organisation. In the previous paragraph, the researcher mentioned that ISO 38500 consists of six principles or basic issues. Just as with COBIT, the principles refer to “what” must be done, but do not explain “how” or “when” to implement these principles (Badenhorst, 2009). Another weakness of ISO 38500 is that the framework takes a holistic view of the ICT organisation and does not focus on outsourcing specifically (Badenhorst, 2009). Nassimbeni et al. (2012) propose the First Assessment Framework Analysis (FMEA) to manage security risks when outsourcing ICT (Figure 2.2).

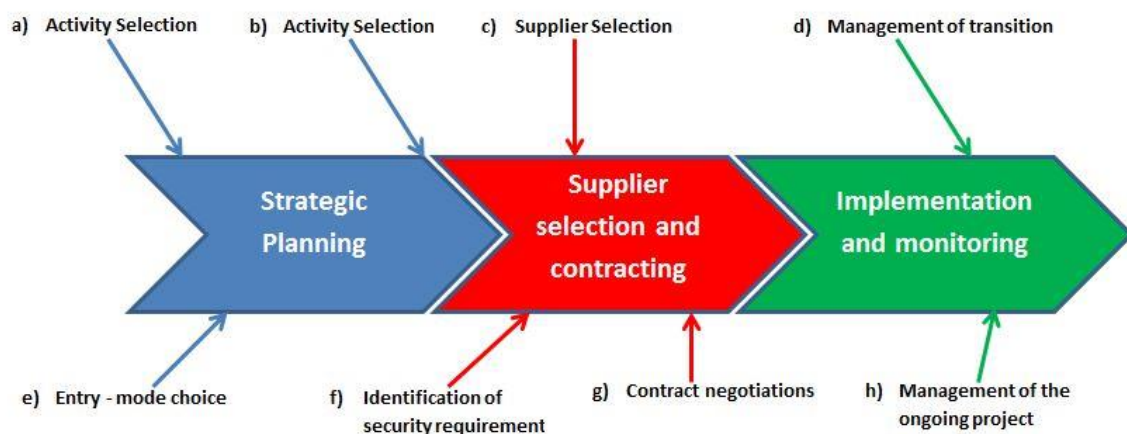


Figure 2.2: First Assessment Framework Analysis (FMEA)
(Nassimbeni et al., 2012:410)

The FMEA is a methodology that can be used to analyse potential failures that can arise, the root cause of the failure, the impact of the failure, and the corrective actions that can be taken. The FMEA assessment framework consists of three phases, namely *strategic planning, supplier selection and contracting, and implementation and monitoring* when outsourcing. Each phase is subdivided into

sub-phases. Nassimbeni et al. (2012) identify several failures or gaps that can be found in the FMEA phases when outsourcing ICT, as indicated in table 2.1 below.

Table 2.1: Failures/gaps within FMEA phases

Phases	Failures/ Gaps in FMEA phase
Strategic planning	<ul style="list-style-type: none"> • Inaccurate preventative analysis, which refers to outsourcing activities that are unsuitable • Inadequate breakdown and assignment of outsourcing activities • Inaccurate selection and management intermediaries • Underestimation of the country's security risks and use of inadequate protection tools that will not work in the foreign country when outsourcing ICT activities • A lack of awareness of the destination and original legal environment
Supplier selection	<ul style="list-style-type: none"> • A lack of/inadequate security requirements when creating the supplier selection criteria • No guarantee that the supplier will adhere to the established security requirements • Organisations failing to check if the suppliers really comply with the security requirements as stipulated by business
Contracting	<ul style="list-style-type: none"> • Security clauses that are not defined properly • A lack of/inadequate security metrics definitions in contracts • Contracts that are not reviewed over time or the inability to make changes as a result of inflexibility • Penalties that are not effective • No exit strategy in place if any violations or problems occur
Implementation and monitoring	<ul style="list-style-type: none"> • Incorrect planning of resources/information such as software, hardware, information, and data • Unawareness of the confidentiality of data and procedures that are in place to protect that data • Incorrect outcomes when transferring activities to the vendor, which can result in to extra costs • A lack of/ inadequate training of security issues • Both parties (outsourcing business and ICT vendor) fail to implement adequate technical protection tools • Monitoring methods that are inadequate

Kutsikos and Sakas (2014) recommend a Service Configuration Decisions Framework when outsourcing. The description of each quadrant and its factors are beyond the study; the author will therefore only provide a brief description of the framework and its components. The framework consist of two capabilities, namely *commodity capabilities* referring to capabilities that are required for day-to-day activities, and *dynamic capabilities* for developing competitive advantages for the outsourcing organisation. Two resource categories can also be identified, known as dependent, which means the resources depend on each other to function, and *combined* referring to resources that re not functioning independently from each other. In addition to the resource categories, the outsourcing business must also consider the various service provider approaches as indicated in figure 2.4.



Figure 2.3: Framework for service configurations decisions
(Kutsikos & Sakas, 2014:607)

Lee et al. (2012) propose a Risk Measurement Outsourcing Framework consisting of two parts (Figure 2.3):

- Qualitative risk assessment in which FMEA is used to develop a risk map, allowing business to score and prioritise each risk that can be associated with outsourcing
- Quantitative risk assessment based on the Monte Carlo simulation (MCS) to determine the cost and time impact through the use of scenarios before and after outsourcing agreements

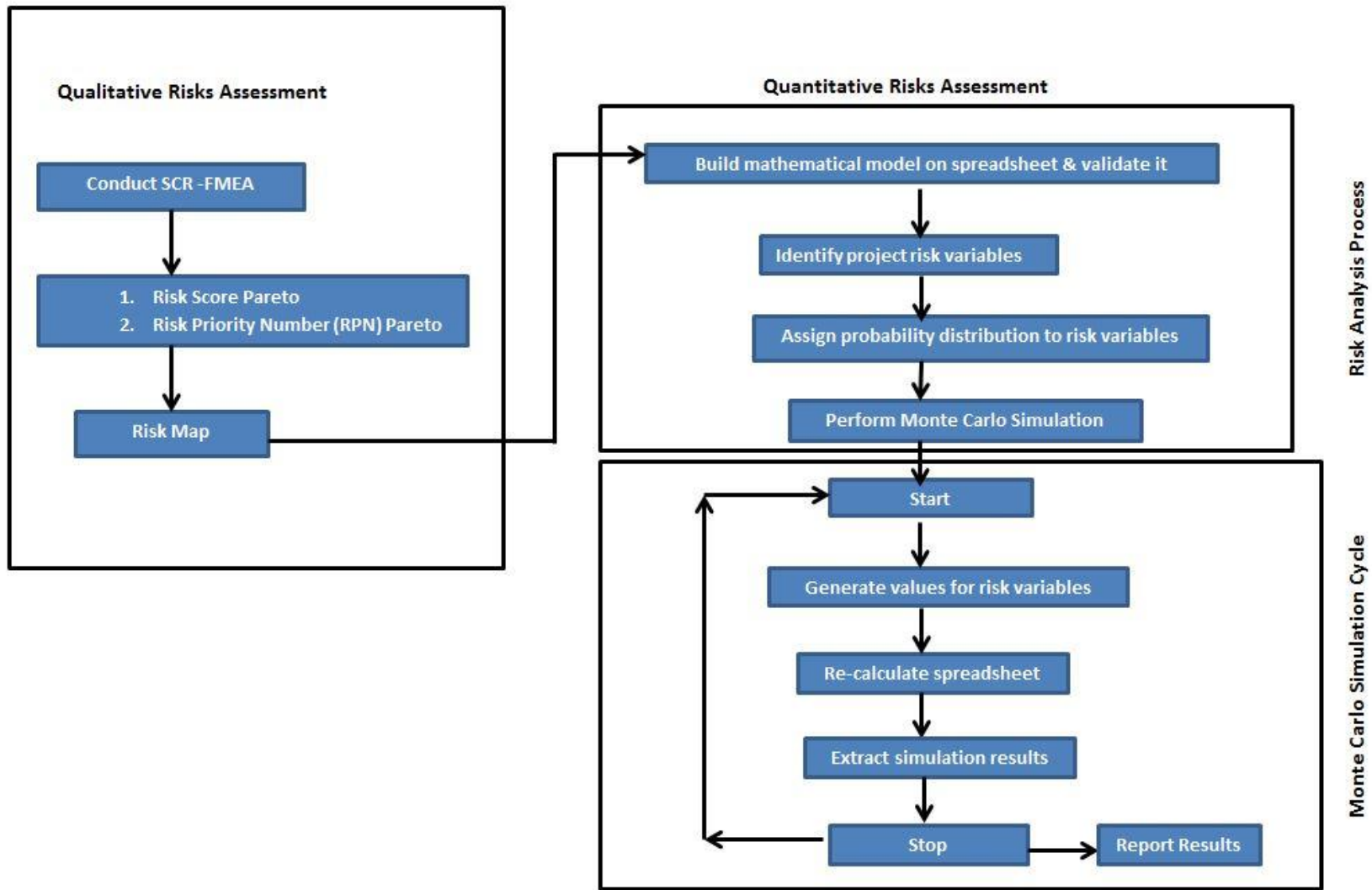


Figure 2.4: Risk Measurement Outsourcing Framework
(Lee et al., 2012:544)

Lastly, Pratap (2014) developed an outsourcing capability framework known as FARM (Flexibility, Absorptive Capacity, Relationships and Monitoring), based on a farmland where farmers have to deal with different conditions applying the various skills and techniques that are available to ensure an output. Similar to the farmland, the outsourcing business also needs to use varied strategies for outsourcing processes. The framework matrix makes use of Indian weather patterns for illustration purposes in figure 2.5.

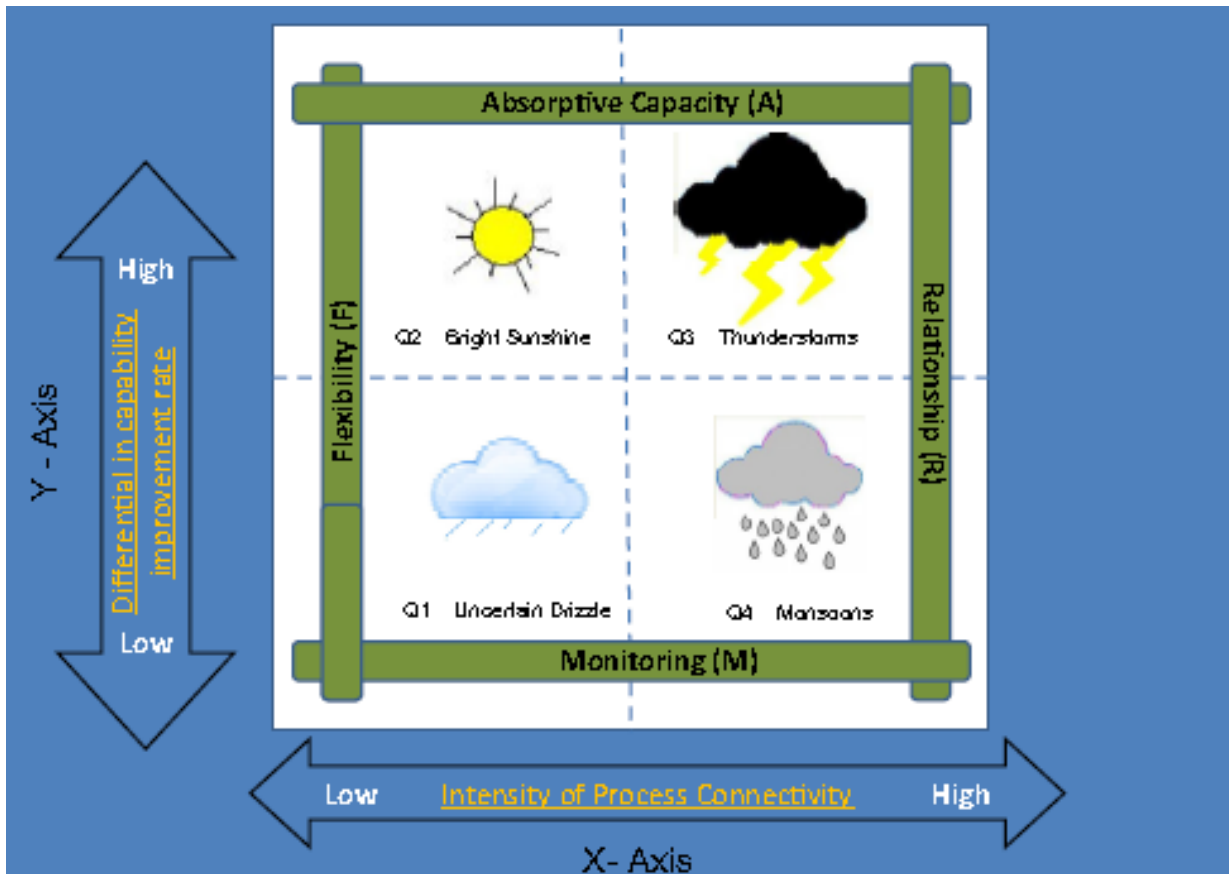


Figure 2.5: FARM outsourcing matrix
(Pratap, 2014:237)

2.7 User awareness

As there is an increase in ICT systems and networks around the world, there is also an increase in software services requests, which leads to growth in the ICT outsourcing business; therefore, as a result of the increase and growth, business and users are facing various information security challenges that go hand-in-hand with ICT outsourcing (Bahl & Wali, 2014).

It is important that organisations change their information security strategies accordingly to adapt to the new information risks and threats that may arise due to

the growth of new technologies (AlHogail, 2015). Information security training is seen as one of the most effective ways for business to protect their information resources, then again, it is also true that several organisations do not have information security awareness programmes in place (Veiga & Martins, 2015). It has been found that cyber criminals often target countries with high crime rates, as there are many people that have limited access to education systems and education on cyber security (Venter, 2014). To change the users' behavior towards ICT security, business needs to understand how users see risks and how they make decisions regarding security (Tsohou et al., 2015). Tsohou et al. (2015) agree with Rastogi and von Solms (2012) and state that compliance to information security policies and controls are determined by how the information security culture is passed or perceived in the organisation.

Venter (2014) points to a lack of proper information security awareness training in business. With proper training, users would easily be able to identify cyber or security issues. Implementing an information security awareness culture within the organisation can reduce risks, especially information security risks to information resources (AlHogail, 2015). Tsohou et al. (2015) agree with AlHogail (2015) and explain that users do not always adhere or comply with ICT security policies that are put in place and suggest that security awareness programmes be put in place to make them aware of the importance of ICT security and the management thereof. Veiga and Martins (2015) suggest that business should attempt to improve the information security culture in such a way that employees comply with information security policies and processes that are put in place. Da Veiga and Eloff (2010) indicate that the success of information security approaches is dependent on the employees' behavior towards various approaches that are put in place by business. Then again, Górnjak-Kocikowska (2008) argues that if people are unhappy with the new technology the resistance may grow, causing the technology to fail. Da Veiga and Eloff (2010) are in agreements with Górnjak-Kocikowska (2008).

2.8 Conclusion

Organisations consider the adoption and usage of ICT as an important factor, as ICT can be found everywhere. The outsourcing strategy is used in several industries, from manufacturing to ICT services. ICT as a tool is integrated into procedures and products within organisations, government, and communities. Organisations are using ICT to make informed decisions and develop competitive advantages to stay ahead in the market.

Information products and services are the responsibility of the internal ICT department, but this is changing as ICT outsourcing becomes an alternative. Outsourcing of ICT has become a strategy widely accepted; it continues to grow, as it has the ability to satisfy the needs of vendors and clients by creating a business model that is attractive for both parties in the universal business playground. It is suggested that the outsourcing of functions should be part of business's long-term strategy and not simply a short-term benefit. Although outsourcing is beneficial to business, it can also be associated with hidden costs or higher costs; a lack of ICT control over vendors; poor service delivery; opportunistic vendor behaviors; dependency on vendors; vendors making changes to the system without the acknowledgement of the outsourcing business; and a lack of vendor capability to provide the service.

Before business decides on the ICT services to be outsourced, they need to define their core and non-core functions that support their business processes. Once this is done, they can start with the vendor selection and contract process. When it comes to outsourcing, the contract is one of the most important components as it includes financial and legal issues as well as the service level agreement. The contract can be seen as the relationship agreement between the vendor and business. Although it is suggested that business has a single vendor, it is also found that having only one vendor opens the gate to several risks such as alignment issues, which include vendor commitments and effectiveness, slow implementation, and the ability to understand information needs. The problem is that there are still managers not having the necessary knowledge to put controls in place that will deal with ICT security abuse. Not having the necessary knowledge can be seen as a risk since ICT managers and information security personnel must be able to identify and understand ICT related issues in order to address the source(s) of the threat properly.

Lastly, data and information being sent are collected, processed, and stored in ICT systems. This makes information a valuable and critical asset to the organisation for survival; information must therefore be kept safe and protected at all times. Several methods exist that can be used to protect information and systems, such as risk management (governance) that includes information security management methods. Some of these methods are auditing, access management, security feedback from stakeholders, and monitoring of intrusion systems. The success of information security is not always solely dependent on technical aspects that are put in place, but also on user behaviour, while using ICT systems as employees are still seen as

the largest contributors. Information security must be viewed by business as a technological as well as human issue. Although business may have all these methods and processes in place, they still need to make users aware of the various information and security risks.

The next chapter (3) will discuss the research methodology used in this research, which includes the research philosophy, research approach, research strategy, data collection techniques, and how the data were analysed.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

To understand how the research is done, the author explains the terms associated with research methodology. These terms include research, methods, and methodology. According to Dellis, Skolarikos and Papatsoris (2014), research can be defined as the process of searching for scientific knowledge and advancing knowledge by following a systematic or scientific approach. A number of research types can be found in literature, namely population-based research, laboratory research and translational research. Wilson (2013) provides a more holistic definition of research by stating that research is the process of investigating a set of research questions, with the aim of answering the questions through collecting, analysing, and interpreting the data, while (Myers, 2013:06) describes research as “an original investigation undertaken in order to contribute to knowledge and understanding a particular field”. Research usually starts with an idea originating from an observation or theories (MacDermid, 2015), as indicated in figure 3.1.

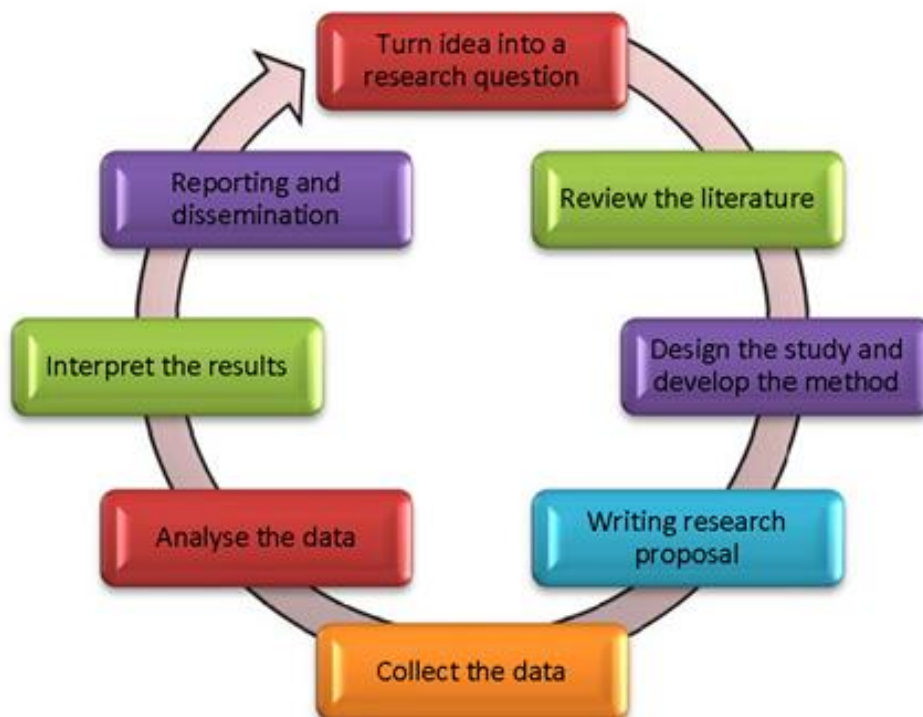


Figure 3.1: The research process
(Majid, Ahmad, Din, Rambely, Suradi & Shahabudin, 2012:395)

The second term that can be found in research methodology is method/s. Methods refer to the what is used (tools and approaches) by the researcher to conduct the

research (Smyth & Morris, 2007). Hyland (2016) describes methods as the different ways of collecting data and states that there is more than one method or formula for doing research. These methods are discussed at later stage in Chapter 3. Lastly, methodology can be defined as systems used to do something or the process to perform an activity, herein referred to as the research processes (Smyth & Morris, 2007). Hyland (2016:117) explains that methodology has to do with “how research is done, how we found out about things and how knowledge is gained”.

Research design is the blueprint or action plan for the research process from the start to the end (Yin, 2006). According to Hyland (2016), any research design can be used to answer any research question. In this study, the research questions are:

RQ 1: What information risks does the ICT department manage when outsourcing ICT projects?

RQ 2: How can the ICT department protect their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT?

The aim of the study is exploring how the transport organisation can manage information risks through the usage of infrastructure risk management when outsourcing ICT projects. Mkansi and Acheampong (2012) explain that confusion with conducting research arises when classifying research philosophies such as epistemologies and ontologies.

The following is discussed below: i) the research philosophy; ii) research approach; iii) research strategy; iv) data collection techniques; and v) how the data were analysed. The chapter ends with the ethics considered throughout the research process.

3.2 Research philosophy

Research philosophy can be linked to how knowledge is viewed, meaning the way knowledge is viewed determines how authors will conduct or approach their research (Wilson, 2013). When conducting social research, ontology and epistemology are seen as two of the main philosophies that must be considered (Zou, Sunindijo & Dainty, 2014). Figure 3.2 provides a graphical presentation of how ontologies, epistemologies, methodologies, methods, and data sources fit into each other.

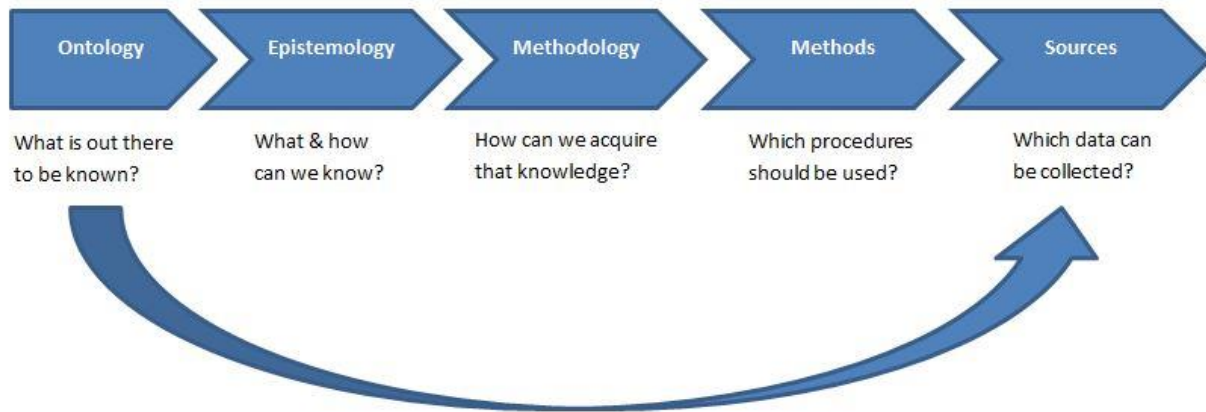


Figure 3.2: Graphical presentation of how ontologies, epistemologies, methodologies, methods, and data sources fit together
(Zou et al., 2014:318)

3.2.1 Ontology

Compton (2013:428) defines ontology as “an area of philosophy that to some extent, depending on the orientation of the philosopher, questions and/or provides an outline for being, entities, and reality in general and relationships within and between the three”. Ontologies can be used for the development of various things such as information systems, integration of applications, and e-commerce products structuring (Saito, Umemoto & Ikeda, 2007). Wilson (2013) as well as Zhu, Kong, Hong, Li and He (2015) explain that ontology has to do with the nature of reality and how the world is seen by humans. Zou et al. (2014) identify two perspectives in which the world can be seen—objectivism and subjectivism. Objectivism can be defined as an “ontological position that implies that social phenomena confront us as external beyond our reach and influences” (Bryman & Bell, 2015:32). The author used an organisation as a tangible object to explain objectivity. An organisation consist of rules, people in various departments, policies and procedures, mission statements, and many other regulations. These features are not the same for all organisations and exist independently from individuals who must adhere to them.

Researchers adopt a subjective view when they see the world as independent from social actors (Wilson, 2013). Zou et al. (2014:318) explain that: “...social phenomena are produced through social interactions and they are in a constant state of revision”. Abdel-Fattah (2015:311) provides a more detailed description by explaining that subjectivists see reality as a “subjective or a social construction”, meaning that reality is a product or exists in the mind of the individual. Objectivism is seen as important in positivist research (Luft & Shields, 2014), while subjectivism is usually linked to interpretivism (Wilson, 2013) as indicated in figure 3.3.

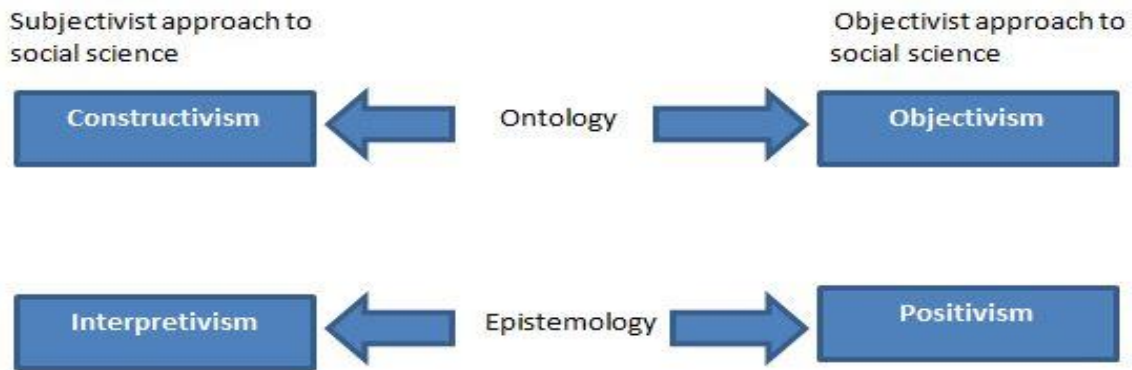


Figure 3.3: Nature of social sciences
(Zou et al., 2014:318)

For this study, a subjective ontological stance was followed, as all participants had their own view of the phenomenon that was investigated.

3.2.2 Epistemology

Morgan (2014:405) refers to epistemology as the studying of knowledge, the acquiring of knowledge, as well as how knowledge is socially structured, while Wheeler and Zagzebski (2008:1) define epistemology as the “philosophy study of knowing and other desirable ways of believing and attempting to find the truth”. Myers (2013:36) provides a shorter description of epistemology and explains that epistemology is all about “...how knowledge is obtained and the assumption of it”. If the author takes all three definitions into consideration, it can be said that epistemology is concerned with what is acceptable knowledge (Bryman & Bell, 2015; Zou et al., 2014). Mkansi and Acheampong (2012) identify positivism and interpretivism as epistemology perspectives that can be adopted in research, while Myers (2013) and Zou et al. (2014) identify three research philosophies or methodologies that can be categorised—positivism, interpretivism and critical theory.

Organ and Stapleton (2013:118) explain that interpretivism “is concerned with the study of people’s environment based on their own perspective, beliefs, and feelings”. Interpretivists believe that equation methods and formulas cannot be used to study people. Wilson (2013) agrees with Organ and Stapleton (2013) and states that interpretivism is the epistemology that takes on a subjective approach and indicates that researchers interact with the social world in order to examine the phenomenon. More than one research method can be applied to interpretivist

research. These methods include case studies, action research, and grounded theories (Abdel-Fattah, 2015). For the purpose of this research, a case study was used as research strategy.

Positivists adopt an objective view and are not dependent on the phenomena being studied, meaning that there is minimal interaction with participants and the research is objective, since the researcher is not dependent on the research (Wilson, 2013). Myers (2013) explains that a positivist research stance assumes the reality is independent from the researcher and his/her tools used. The paradigm is all about testing theories in order to understand a phenomenon. Positivism is usually associated with quantitative theory testing research (Luft & Shields, 2014; Saunders & Bezzina, 2015). Lastly, critical research can be seen as a combination of qualitative and quantitative research (Myers, 2013). This combination is done to gain knowledge that is more scientific (Song, 2016). To conduct this study and answer the research questions, an interpretivist epistemology was adopted, as there are multiple ways of looking at the phenomena (things in reality).

3.3 Research approach

When conducting research, there are several approaches or methods that can be followed including mixed methods, a qualitative approach, and a quantitative approach (Mkansi & Acheampong, 2012). For the purpose of the study, the researcher will only provide a broad overview of qualitative and quantitative approaches. Quantitative research is also known as deductive, explanatory and exploratory research, while qualitative research is a synonym to inductive as well as exploratory research (Mkansi & Acheampong, 2012). Khaikleng, Wongwanich and Sujiva (2014:1390) describe an inductive approach as a method that “involves theory development using information collected from [the] stakeholder and the observations of actual conditions”, while a deductive approach can be described as the “reconstruction of theory that already exists to create a new one”. Wilson (2013) and Sik (2015) elaborate on the two research approaches and explain that by following an inductive approach, the researcher performs an observation of the phenomena under investigation to formulate a new theory, while with a deductive approach, the researcher applies the current theory to solve a phenomenon being investigated.

Inductive studies are associated with interpretivism (Ali & Birley, 1999) and deductive studies with positivism (Wilson, 2013). In order to decide which methodology (quantitative or qualitative) to be used, the researcher needs to

determine the information needed to answer the phenomena and what the results of the findings will be used for (Harness, 2009). The researcher adopted an inductive approach as an investigation was conducted where data were collected from 17 participants to formulate a theory on how the transport organisation could manage information risks through the usage of infrastructure risk management in outsourced ICT projects.

3.4 Research strategy

Two main research strategies can be identified—qualitative and quantitative (Dellis et al., 2014; Wilson, 2013). Qualitative research includes action research, case study research, grounded theory, ethnography, and semiotics, which can be seen as text based, while quantitative research includes surveys, simulations, laboratory experiments, and mathematical modeling that are more numerically based (Myers, 2013). To elaborate, qualitative studies focus more on the experience of humans and theoretical information, while quantitative studies focus on information in the form of numerical values for analysis or statistical purposes (Dellis et al., 2014; Wilson, 2013; Van Griensven, Moore & Hall, 2014). Qualitative strategies can be linked to inductive studies, while quantitative strategies are associated with deductive studies (Wilson, 2013; Van Griensven et al., 2014). As this is a qualitative study, attention was given to qualitative approaches.

With qualitative studies, there is more than one way or several possibilities to understand or explain a phenomenon or the truth (Fletcher, Massis & Nordqvist, 2016) as qualitative research approaches give the researcher a better understanding of the things that people say and do (Myers, 2013). With qualitative research, it is actually impossible to understand why a specific event occurred or why someone did something without talking to this person about it. One of main reasons why researchers choose qualitative over quantitative research, is that researchers can communicate with the participants or humans to understand the natural world; for example, researchers can asks questions or read what was written to understand why something happened or to explain certain actions (Myers, 2013).

Qualitative studies are usually associated with case studies as it has the ability to answer “how and “why” questions of a phenomena (Mkansi & Acheampong, 2012; Harness, 2009), hence the reason why the author conducted a case study on the transport organisation.

3.4.1 Case study

Case studies can be seen as one of many ways of conducting research (Yin, 2006) and is used to answer “why” and “how” research questions (Phelan, 2011). According to Hyland (2016), case studies are used to achieve a better understanding of a person, process, events, or even a group. Yin (2006) explains that case studies should be used when researchers want to cover contextual conditions of a phenomenon that is being studied. Baxter and Jack (2008) and (Yin, 2014) recommend that a case study be used when the researcher conducts research to answer “how” and “why” questions and the researcher has no influence on the answers or behavior of the participants. Several types of case studies can be identified in literature such as explanatory, exploratory, descriptive, multiple-case, intrinsic, instrumental, and collective studies (Baxter & Jack, 2008; Phelan, 2011). Case studies can also be used for qualitative and quantitative studies or both (Phelan, 2011; Gerring, 2007; Yin, 2014). Lee and Lo (2013) state that case studies can be inductive or deductive depending on how it is used by the researcher. Phelan (2011) identifies six sources of data or information when conducting case studies. These sources include company documents such as letters and reports, interviews, direct observations of participants/units, participant observations for example being part of the process, physical artefacts, and revisiting of archived records. One disadvantage that can be related to case studies is that it usually takes time and the researcher can end up with many documents.

The author performed an exploratory case study at a transport organisation as the problem is not clearly defined or no previous studies were done on the phenomena under investigation (Majid et al., 2012), and the research questions are “how” and “why” questions.

3.4.2 Sampling

Daniel (2011:6) describes sampling “as the selection of a subset of a population for the inclusion in a study”, while a sample can be defined as “a small set of cases a researcher selects from a pool and generalises to the population” (Neuman, 2010:240).

According to Zou et al. (2014:318), data can be collected by means of structured interviews, questionnaires, and observations in order “to generalise from a sample of a population”. For this study, a non-random, purposive selected sample was used. The samples for the research were ICT professionals working in the outsourcing company. The sample size was based on the availability of ICT

professionals and the willingness to participate. The sample size for the study was 17 ICT professionals working in the outsourcing company.

3.4.3 Unit of analysis

Phelan (2011) defines the unit of analysis as the source from where the researcher obtains the required information to answer the research questions, while Bengtsson (2016) describes the sample that is used to conduct the research as the unit of analysis. Baxter and Jack (2008) state that identifying the unit of analysis (case) in case studies are not an easy process and could become a challenge. To make the identification process easier, it is suggested that the researcher asks him/herself, "What do I want to analyse?" The case can be an individual, an event, programme, process implementation, or any entity (Yin, 2006). For this study, the unit of analysis is the outsourcing business and the unit of observation is the ICT professionals.

3.5 Data collection

Data collection is seen as an important part of any research project (Bryman & Bell, 2015). Knipe and Bottrell (2015) and Khaikleng et al. (2014) name various data collection methods that can be used in the research process, namely surveys, interviews, observations, documents, and data mining, while Bryman and Bell (2015) also identify interviews (including semi-structured interviews) and participant research as research methods than can be used for data collection. Data collected during interviews are often captured via video or audio and then transcribed, which is an interpretive process.

To perform the investigation and answer the research questions, interviews using semi-structured questionnaires were conducted to collect data from 17 participants. The participants included ICT managers, executive managers, security consultants, and analysts in the ICT field. Even though top management approved the interview process or the collection of data, a few of the participants refused to answer some of the research questions as they viewed it as sensitive information. All participants were made aware of the ethics adhered to during and after the data collection process (see section 3.7).

The data collection process was executed as follows: Permission was obtained from top management of Transnet to conduct research at the organisation. Once approval was received from top management, participants were contacted through the usage of email to inform them of the research and requested if they would be willing to take part in the research. Several declined for personal reasons, while 17

accepted. All participants were made aware of the ethics as indicated on an individual consent form that needed to be signed by each participant.

As already mentioned, interviews were conducted using semi-structured questionnaires. Participants were asked if they are comfortable with being recorded during the interview (data collection) process; all 17 participants agreed. Once the data collection process was completed, the researcher started the data analysing process. The process of data collection and data analysis is time consuming (Bengtsson, 2016).

3.6 Data analysis

Data analysis is all about breaking the data down into smaller pieces to make more sense to the researcher. Methods that can be used for the analysis include the transcribing of recordings and thematic analysis to make data more understandable (Myers, 2013). Bengtsson (2016:09) defines the analysis of data as “a research technique for the objective, systematic and quantitative description of the manifest content of communication”. According to Phelan (2011), the analysis of data is seen as the most difficult activity when it comes to case studies.

Other analysis methods mentioned in literature include statistical analysis, verbal analysis, documents analysis (Knipe & Bottrell, 2015), content analysis (Bengtsson, 2016), and thematic analysis (Bryman & Bell, 2015). Bengtsson (2016) identifies two types of content analysis—qualitative content analysis in which data are in the form of words or even themes that can be interpreted to gain a better understanding of the data, and quantitative content analysis where facts are generated from text in the form of numbers or percentages. Qualitative content analysis can be used for analysing data collected during interviews (Laudel & Glaser, 2014); this data can be transcribed into text format, keeping it in its raw format to make it easier for analysis (Obalola & Adelopo, 2012). The type of analysis will be determined by the type of case study selected (Baxter & Jack, 2008). Bengtsson (2016) explains that it does not really matter which method is used for the analysis process, as all the analysis processes are either reducing the amount of data collected, categorising the data, or gaining a better understanding of the data.

The researcher made use of qualitative content analysis as the data were collected in the form of words. Data collected during the interview process were transcribed into text format and kept in its raw format. All data collected were then summarised, organised, and categorised to provide the researcher with a better understanding of the data and the development of themes.

3.7 Ethics

Resnik (2015:1) defines ethics as the “norms of conduct that distinguish between acceptable and unacceptable behavior”. Ethical norms can be learned or adopted at home, school, church, or any social environment during childhood and as people mature. Ethical principles include honesty, plagiarism, informed consent, and permission to publish (Myers, 2013). According to Resnik (2015), when people think about ethics, they immediately think about what is right or wrong. Bengtsson (2016) states that before, during, and after the research process, ethics must always be taken into consideration. It is suggested that all participants involved in the study should be informed of what the study is about and must be ensured that all information collected during the interview processes will be seen as confidential. The participants must also know their right to withdraw their data at any time. Many attempts have been made to determine the effectiveness of ethics (Obalola & Adelopo, 2012) as ethical norms ensure accountability to the public (Resnik, 2015).

Resnik (2015:2) identifies the following ethical principles:

- a) **Honesty:** The researchers must report all their findings honestly and not falsify or fabricate data
- b) **Integrity:** Adhere to all promises and agreements made, also to interviewees or participants
- c) **Openness:** The researchers should be open to any criticism or ideas that may arise
- d) **Confidentiality:** The researchers should protect confidential data at all times
- e) **Animal care:** If animals are used in the research, they must be protected and cared for

For this study, various ethical principles were considered. Consent was obtained from top management (Appendix C) as well as from each participant for data collection purposes. Although the researcher received consent from Transnet and participants, no data will be published without the organisation’s permission.

Before the interview, the participants were made aware that they do not have to answer any question if they are uncomfortable and can withdraw their answers at any time. Participants were also ensured that all data collected from them would not be discussed with other colleagues and stored electronically in password-protected files.

Data collected during the literature review as well as the data collection process will not be falsified or fabricated, and all contributors will be recognised. Data collected will be kept for any enquiries that may arise in the future and the researcher will ensure that all the results/findings based on the data collected, are honest.

3.8 Summary

Methodology focuses on how research is conducted, how to find out about things/phenomena, and how knowledge is gained or the different ways of collecting data. In Chapter 3, the author discussed the research methodology followed throughout the research process, which included the research philosophy, research approach, research strategy, data collection techniques, and how the data were analysed.

The chapter started with explaining research philosophy, followed by ontology and epistemology. Research philosophy can be linked to how knowledge is viewed, meaning the way knowledge is seen will determine how authors conduct or approach their research. For this study, a subjective ontological stance was followed, as all participants of the research had their own view of the phenomenon that was investigated, while an interpretivist epistemology was adopted, as there are multiple ways of looking at the phenomena under investigation.

When conducting research or investigating a phenomena there are several approaches or methods that can be followed, including a mixed methods, qualitative, or quantitative approach. Qualitative research is a synonym for inductive and exploratory research. For this study, an inductive approach was followed as the researcher observed the phenomena under investigation to formulate a new theory. With qualitative research, there is more than one way of understanding or explaining a phenomena or the truth. Qualitative research can include action research, case study research, grounded theory, and semiotics, which can be seen as text based. For this research, an exploratory case study was adopted as it can be used to answer “how” and “why” research questions.

For the case study, a non-random, purposive sample was used. The sample consisted of 17 ICT professionals working in the outsourcing company, and the selection of the sample was based on the availability of participants as well as their willingness to participate. The unit of analysis was identified as the outsourcing company and the unit of observation as the ICT professionals.

In order to collect data from the 17 participants, permission was first obtained from top management of Transnet, which allowed the research to be conducted at the organisation. Data were collected by means of interviews that were conducted using of semi-structured questionnaires. Once all data were collected from the 17 participants, it was analysed. The researcher made use of qualitative content analysis as data were in the form of words. All data collected were summarised, organised, and categorised to provide the researcher with a better understanding of the data and the development of themes.

The chapter ended with a discussion on ethics, being considered from the beginning to the end of the research process. When people think of ethics, they immediately think about what is right or wrong. For this study, various ethical principals were considered; firstly, consent was obtained from top management as well as from each participant individually for data collection purposes. Secondly, each participant was made aware of their rights not to answer any question if they feel uncomfortable, and that they are allowed to withdraw their answer/s at any time. The author/researcher also ensured participants that the data collected will not be discussed with colleagues, and that all data will be saved in a password-protected folder. Lastly, no data will be falsified. All data collected in the literature review as well as interviews will be kept for any queries that may arise in future.

In the next chapter (4), information of the case used for the research will be discussed. The chapter will also analyse the interviews conducted during the research processes and formulate findings based on the analysis of the interview answers of the 17 participants.

CHAPTER 4: ANALYSIS AND FINDINGS

4.1 Introduction

In this chapter, information of the case used in the research is discussed. The chapter analyses the interviews conducted during the research process and findings formulated based on the analysis of the 17 participants' answers. For the convenience of the reader the problem statement, key research questions, and aim of the study are stated below.

Problem statement: It is unclear how to manage information risks through the usage of ICT infrastructure risk management when outsourcing ICT projects, and this exposes organisations to ICT security risks.

RQ 1: What information risks does the ICT department manage when outsourcing ICT projects?

RQ 2: How can the ICT department protect their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT?

Aim of the study: To explore how the organisation can manage information risks through the usage of infrastructure risk management when outsourcing ICT projects.

In the next sections, the case as well as the findings of the research is discussed. The chapter ends with a summary of the findings and the themes developed from the findings.

4.2 The case

Transnet SOC Ltd was established on 1 April 1990; it is the largest and most important transport and logistics supply chain ensuring that goods are delivered to South Africans on a daily basis. Transnet SOC Ltd can be tracked back to the late 1850's when the proposal was made for railway transport between the Cape and KwaZulu-Natal harbours. Transnet SOC Ltd plays a vital role, not only in the life of ordinary South Africans, but also in the nation's economy and other African countries making use of Transnet SOC Ltd harbours and networks for importing and exporting goods.

Transnet SOC Ltd consists of five operation divisions, fully owned by the government of South Africa although it is operated as a corporate entity. The operating divisions are as follow:

- Transnet Freight Rail (TFR)
- Transnet Rail Engineering (TRE)
- Transnet National Ports Authority (TNPA)
- Transnet Port Terminals (TPT)
- Transnet Pipelines (TP)

TFR is the largest division of Transnet and employs almost 25,000 employees. The division is responsible for the transportation of freight such as fuel, containers, iron ore, grain, and granite. Another large division of Transnet is TRE, seen as the backbone of the railway industry, and employing more than 15,000 employees. The division is responsible for maintenance, repairs, upgrading, and building of freight wagons and suburban coaches.

The TNPA division performs the 'landlord' function as it provides the port infrastructure and marine services. The division also ensures that the national port system is safe, effective, and efficient. Without TNPA, Transnet Port Terminals will not be able to function. TPT is responsible for handling (importing and exporting) containers, bulk, break-bulk, and automotives through TNPA's port infrastructures. TPT operates in seven terminals around South Africa.

TP is the last division of Transnet, owning South Africa's strategic pipeline assets and responsible for transporting gas and petroleum. The division handles over 16 billion litres of petrol and more than 450 million cubic metres of gas annually.

Each division consists of different departments such as Human Resources, Operations, Marketing, and ICT. For the purpose of this research, the focus is on the ICT departments of the various operating divisions. Based on these operating divisions and their requirements, ICT services can be outsourced or kept in-house. Transnet SOC Ltd outsources various ICT functions, including networks, Active Directory, perimeter defense, CCTV support, application development, email, and helpdesk support at certain divisions.

4.3 The participants

To be able to answer the research questions, 17 participants have been interviewed (Table 4.1).

Table 4.1: Job title, years of experience, and work specification of participants

Job title	Years of experience	Work specifications
EIMS governance risk and compliance consultant	10 years	Responsible for leading and directing the development and maintenance of IT risks, IT governance, information security, and compliance management strategies Collaborating with group compliance, internal auditors, group risk management and various teams in the design and approval of audits, risk assessment, and regulatory compliance frameworks for Transnet ICT
Executive manager, service delivery	5 years	Head of ICT service delivery Responsible for operational systems, infrastructure, and end-user support for Transnet Port Terminals
Field support specialist	20 years	Software and hardware support Virtual server management and maintenance of domain controllers, Active Directory services, and exchange
ICT manager	7 years	Responsible for various ICT projects, including CCTV implementation and improvement of management systems Ensuring that ICT performs their daily tasks to achieve business objectives and service clients
ICT manager	8 years	Responsible for the ICT functions in the Cape Town Terminals, which include all ICT Systems, voice, telephony, and wired/wireless networks
ICT manager	16 years	Responsible for maintaining information technology strategies by managing staff, researching and implementing best solutions within budget and on time
Information security analyst	1 year and 8 months	Responsible for developing/reviewing information security standards, procedures, awareness programmes, and advice on projects to ensure IT security is sufficiently taken into account.
Information security officer	9 years and 11 months	Responsible for information security standards, strategies, and policy development Information security design and implementation of controls based on risk assessments Information security awareness training and risk management
National systems manager	19 years	ICT service delivery Managing of development teams Managing of outsourced systems Responsible for ICT requirements for the bulk, break-bulk, and automotive sector

Job title	Years of experience	Work specifications
Operating division security liaison	2 years	<p>Managing the relationship and serving as a point of contact between the operating divisions and information security management team for all matters relating to information security</p> <p>Responsible for ensuring that cost-effective and compliant security is considered and embedded in all implemented technology</p> <p>Responsible for implementation of the information security policies, procedures, and awareness efforts</p>
Principle specialist: governance, risk and compliance	3 years and 6 months	<p>Developing and reviewing new and existing ICT policy and procedure documentation in line with the organisation's ICT governance framework, methodologies, and standards</p> <p>Implementing policies, procedures, standards, and guidelines in line with TPT ICT security strategy</p> <p>Monitoring compliance of ICT systems and functions in relation to the ICT control checklist, policies, procedures, and standards</p> <p>Assisting in creating and managing ICT information security and risk management awareness programmes</p>
Security analyst	9 years	<p>Information systems auditing and advisory services</p> <p>Responsible for governance, risk and compliance, and information security at Transnet Port Terminals</p> <p>Project management, risk assessments, and the development of security awareness campaigns in the organisation</p>
Senior information security analyst	15 years	<p>Development of information security standards, strategies, policies</p> <p>Responsible for ensuring that information security related tasks or projects are completed as per contractual agreements</p>
Senior key account manager	26 years	<p>Ensuring that a close relationship is built with an understanding of the client's business environment achieved via existing experience, industry exposure, and research</p> <p>Engaging in a consultative selling and business solution crafting approach</p> <p>Effectively solve problems and manage risks to ensure achievement of targets</p>
Service delivery manager	10 years	<p>Project management and technology problem solving</p> <p>Quality assurance and measuring of ICT results</p> <p>Optimising solutions for ICT equipment within the available budget</p>

Job title	Years of experience	Work specifications
Service manager	6 years	Dealing with escalations from clients and assuring they receive good services Reporting on fault resolutions and outages to determine where services can be optimised Assisting clients with new requirements
Technical support analyst	4 years	National server administrator of 200 Windows servers Second line support for desktop personal, servicing 4,500 users nationally Infrastructure coordinator for Group IT projects Applying TPT security compliance and governance as well as testing security policies and settings

The participants have years of experience in ICT and ICT outsourcing. The participants included managers and executive managers as well as consultants, analysts, and specialists in the ICT field. Although consent was obtained from top management to conduct interviews with the participants, some declined answering certain questions for personal reasons or because they deemed the information to be sensitive.

4.4 Findings

In the following section, the interview responses collected during the research process are discussed. Based on the answers of the 17 participants, findings were drawn for each interview question. As stated in Chapter 3, interviews have been transcribed, coded (keywords and key phrases), and summarised; categories were developed (Appendices D and E) and findings were drawn. From the findings, themes for discussion were identified. This section is presented in such a way that the research questions, research sub-questions, and interview questions are linked. After each interview question, the findings are presented.

4.4.1 Interviews

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

Interview Question 1.1.1: What does the term 'information risks' mean to you?

There is no specific definition in the company for information risks. The majority (7) of participants (P) referred to information risks as inappropriate or unwanted access of data, while others mentioned that information risks can be used to exploit the

vulnerability of IT assets and harm the systems. P6 stated that the term ‘information risks’ “refers to the threat of information (electronic or printed) being impacted any one way or the other by a threat factor due to a weakness in the controls that are meant to protect such information. The possible impacts are loss of integrity (including reliability), confidentiality, and availability” (Appendix B6, IQ 1). P1 supported P6 with the following shorter description: “Information risks are any risk that can be used to exploit a vulnerability of IT assets and systems to cause harm to organisations, by either crippling systems or stealing information” (Appendix B1, IQ 1).

Finding 1: There is no specific definition for information risks within the organisation

Interview Question 1.1.2: *How important is information risk management to the business?*

Of the 17 participants interviewed, 16 participants agreed that information risk management is important. However, P6 disagreed with the other participants, indicating that information risk management is not as important to the business since business focuses more on information risk management processes than managing information risks itself. P9 stated that “Information risks management is of [the] utmost importance. Information in its simplest form can pose risks in many ways that could have implications ranging from legal and financial to goodwill defamation” (Appendix B9, IQ 2). P13 elaborated on the issue and explained that the importance of information risk management “depends on the amount and type of information and the reliance the business has on it. For a large corporation like us, information risk management will be extremely important” (Appendix B13, IQ 2). Although the majority (13) of participants agreed that information risk management is important, P1 said that, “currently the business shows more importance in identifying risks to the business, but the importance of resolving the risks and issues is of a less importance to the business” (Appendix B1, IQ 2).

Finding 2: Information risk management is seen as important to the business

Interview Question 1.1.3: *Are there process/es in place for ICT vendors to gain access to Transnet’s information and systems?*

The majority (14) of participants have knowledge of access management processes, but most of the processes mentioned are different, such as user access

management processes that allow the user to connect directly to the corporate network or via remote tools such as Citrix and VPN. P1 said:

“Currently vendors that provide us with services have ability to gain access to our systems by completing a user access request form which gives them access to the corporate domain as a contractor, from there these users can then request access to the required systems that they need access to. This access is either gained via signing directly onto the domain on the corporate network, gaining access remotely via secure Citrix servers or VPN onto the corporate domain” (Appendix B1, IQ 3).

P10 supported P1 and explained that access to the systems for vendors is requested via the normal user account management process. The user account management process consists of completing an access request form that is sent to a line manager who will either approve or reject the request. If the request is approved, it will only be valid for a limited period.

P15 elaborated on the vendor access processes: “The main thing around it is that there are now external parties that are onsite and they [are] coming into the business” (Appendix B15, IQ 3). To address the issue of vendors being onsite, P15 indicated that external parties or vendors need to sign an access register and must be accompanied by ICT personnel at all times. Then again, P15 also pointed out that there are also vendors who have remote access to the system from outside the organisation, for example Neotel, owning the network switches and being one of the primary ICT vendors. By having remote access, the business will not always be able to track the vendor’s activities and that is seen as a big risk.

In addition to what P15 explained, P6 highlighted that, “due to the large landscape of systems at Transnet, these processes are not always enforced consistently” (Appendix B6, IQ 3). P9 supported P6, stating the following: “The processes are covered by agreements or policies and are not enforced or reviewed with the strictest nature” (Appendix B9, IQ 3).

Finding 3: There are different ICT vendor access processes

Finding 4: ICT vendor access management processes are not enforced or reviewed frequently

Interview Question 1.1.4: *Do the process/es include the type of access for ICT vendors?*

Access to ICT vendors range from read and write to full access. P7 stated that access is “dependent on their role in the company and the position they have; some of the vendors do have read and write, however, they do follow an approval process for the access granted to them as well as changes (write) is done in line with the appropriate business decisions” (Appendix B7, IQ 4). According to P2, “the access is on a need-to-know basis; least privilege is enforced with regard to the access to information available to the vendor” (Appendix B2, IQ 4). P5 explained that “T-systems have access to areas where they influence and manage - nothing more. Anything outside that, we will ask questions. For example, a company is looking after server x and wants information about server y. We [are] not going to give the information to them” (Appendix B5, IQ 4).

Contrary to P2, P5, and P7, P15 stated the following: “Key suppliers have full access because they are managing our AD domains, our DCs, our domain controllers against AD rights, and they are managing our exchange servers. Between those two key suppliers, you basically have access to everything” (Appendix B15, IQ 4). P11 supported P7, stating that “vendors have different access, such as read and write, but one can never cover or close all the gaps that go with it; for example, Neotel, our network infrastructure provider, has full access to our entire network” (Appendix B11, IQ 4).

According to P9, restrictions are not always specific and more access is given than needed to perform duties, for example, vendors have access to Active Directory, which means they have access to the email address lists. Another issue highlighted by P9 is the fact that vendors have access to several resources when onsite, which makes it easy for them to access information. This information can be in electronic format or paper trail documents that are just “lying around” in the office. Drawing from the answers of P9, P11, and P7 it can be concluded that most of the key ICT vendors have full access since as they own the systems and network infrastructure.

Finding 5: Access restriction is not always specific

Finding 6: Key suppliers have full access to the systems and network infrastructure

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

Interview Question 1.1.5: *In your opinion, what is the highest information risk when outsourcing?*

All participants are aware of some kind of risk when outsourcing ICT. P3, P6, P7, P11, P12, and P14 mentioned the disclosure or exploitation of confidential information to third parties as the highest information risk when outsourcing, whereas P1, P2, and P9 indicated ownership or intellectual property as the biggest risk. Based on personal experience, P1 stated:

“Ownership or intellectual property is the biggest risk currently that are seen when outsourcing projects to companies for ICT functionality or new projects that we undertake; once these projects are under way or completed the organisation do not [sic] have ownership of the intellectual data or back-end designs of these systems that are managed or built” (Appendix B1, IQ 5).

Other risks detected include hacking (unauthorised access), vendors not complying with information security requirement, and gaining intimate knowledge of the business. According to P15, “the highest risk probably is putting in controls”. (Appendix B15, IQ 5). Business can have several controls in place to monitor vendors, including access control, audit logs, and behavior scanners, but the human factor remains a big problem when implementing controls. For example, business will have individuals of third party organisations who know the username and administrator passwords for specific systems and bypass all the controls that were implemented. P15 identified people as the weakest link when implementing controls.

Finding 7: Exploiting or disclosure of confidential information to third parties is seen as a risk

Interview Question 1.1.6: *Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?*

According to the majority of participants (11), the ICT department has methods in place to determine the impact of information risks when outsourcing ICT projects. However, six participants, including ICT managers and the national systems manager, were unaware of any methods/did not know. One of the methods mentioned many times is risk meetings and assessments to determine the risks as well as the impact of a risk on a project. According to P7, “risk management is in place for all projects; should information risks be a concern, the risk will be captured

and managed accordingly. Further to this, vendors and contractors do sign confidentiality agreements as part of their contracts to ensure the information of Transnet cannot be exploited, exposed, or sold/shared” (Appendix B7, IQ 6). P10 supported P7 by stating that, “as part of Transnet’s risk management process, a risk analysis is performed. All project risks, including outsourcing, are considered and documented” (Appendix B10, IQ 6). Contrary to what the majority said, P6 pointed out that they “are currently working on such mechanisms. Risks are managed through *ad-hoc* security assessments, but this is not the case for all outsourced environments” (Appendix B 6, IQ 6). According to P9, “it seems like ICT would accept the non-disclosure agreements, and trust with the vendors as acceptable” (Appendix B9, IQ 6).

Finding 8: Risk meetings and risk assessments are conducted per project

Finding 9: Risks are managed through *ad-hoc* security assessments, but this is not the case for all outsourced environments

Finding 10: Several participants are not aware of methods used to determine the impact of information risks when outsourcing ICT projects

SRQ 1.3: What strategies do the ICT department have in place to manage information risks associated with ICT outsourcing?

Interview Question 1.1.7: *Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

From the 17 participants interviewed, only P16 was not sure of information and ICT infrastructure security risks when outsourcing. However, P16 did not feel comfortable to provide any further details. It is clear that most of the participants are aware of the various risks. P1, P5, P9, P12, and P14 all said that some of their core systems are hosted by the ICT vendor. P1 explained:

“One of the major risks is with our network provider where we have identified that some core systems that support our system are also hosts to other companies at these break out points. This risk means that if another company is breached through a certain breakout by our provider, we could be in a position that we are breached as well” (Appendix B1, IQ 7).

P5 supported P1’s explanation, stating that, “There is always a risk because the minute you open yourself to [a] third party, there is also risk that they can be hacked indirectly into our systems” (Appendix B5, IQ 7). Other risks mentioned by P10, P13,

and P17 include vendor management and monitoring that are not adequate, illegal activities not reviewed or detected, and compliance not monitored. In addition to the ICT infrastructure security risks mentioned above, application dis-functionality, lack of escalation procedures for risks, and incompatibility of technology and processes were all mentioned as risks during the interviews.

Finding 11: The majority of participants are aware of information and ICT infrastructure security risks when outsourcing

Finding 12: Core systems are hosted by an ICT vendor

Finding 13: Illegal activities are not reviewed or picked up, and compliance is not monitored

Interview Question 1.1.8: *Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

The majority (15) of participants knew of methods that are in place to reduce and manage ICT infrastructure security risks identified in interview question 1.1.7. Only P12 and P14 indicated that they are not sure since they are not part of the discussions and assessment of ICT infrastructure security risks. These discussions usually take place at Group level. Some of the methods mentioned during the interviews include internal audits, data protection strategies, risk management processes with mitigation plans, penetration testing, and monthly vulnerability assessments. P10 indicated that:

“...Service level agreements and vendor management are in place. Also regular audits of vendors, e.g. audit of T-Systems and Neotel by Transnet Internal Audit (TIA) take place on an annual basis. There is an audit scope, which is normally based on the Transnet Minimum Control Framework (IT). The vendor processes, e.g. backup process; if they manage our backups, the vendor will be audited and reported on” (Appendix B10, IQ 8).

P6 also mentioned audits, but pointed out that, “although there are ‘right-to-audit’ clauses in outsourced contracts, assurance exercises take place on an ad-hoc basis. There are periodic risk assessments as well as auditing exercises; however, there are no direct mechanisms to deal with the risks of infrastructure outsourcing” (Appendix B6, IQ 8).

Finding 14: The majority participants are familiar with methods in place to reduce and manage information and ICT infrastructure security risks

Finding 15: Audits take place on a yearly or *ad-hoc* basis

Finding 16: There are no direct mechanisms to deal with the risks of infrastructure outsourcing

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

Interview Question 1.1.9: *Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

Of the 17 participants interviewed, four (4) participants said no, seven (7) participants said they are not sure, and six (6) participants said yes to interview question 1.1.9. All seven participants who indicated they are not sure, explained that measuring the ICT security rate of ICT vendors are usually done at group level, thus they are not involved in the process. Some of the criteria mentioned by the participants who said yes include service level agreements (SLA), audit reviews, and periodic reporting of vendors. P1 stated:

“When we use these vendors, we often sign SLA agreements with the vendors; in these agreements, we have matrixes and percentages that we can manage them. Two of the main criteria we have are system vulnerability percentage of less than 95 percent of the environment that needs to be secured and vulnerability free. The other is a ‘zero breaches’ in the year of organisation systems” (Appendix B1, IQ 9).

P2 said: “Service agreements are the vehicles used to monitor adherence of the vendor to the strategies” (Appendix B2, IQ 9), which supports participant 1’s answer.

Contrary to the answers of P1 and P2, P9 indicated:

“In the past, there have never been major issues with regard to security breaches until two years ago; hence, there was no real drive to put these measures in place. Of recent, there are procedures and protocols being drawn up for security; they are setting up architecture councils and security councils to address these, however, they are still in infancy stages hence the measurement tools and matrices are still to be implemented in my opinion” (Appendix B9, IQ 9).

P6 also differs from P1 and P2, pointing out that “the maturity of the security teams and its process is far off from being able to measure this [sic]” (Appendix B6, IQ 9).

Finding 17: The majority of participants are not aware of criteria used to measure the ICT security success rate of ICT vendors

Interview Question 1.1.10: *Does the ICT department spend money on ICT infrastructure security?*

Two (2) of the 17 participants indicated that the ICT department does not spend money on ICT infrastructure, while 15 participants answered yes. All 15 participants who said yes gave different rand values, and some did not know the average percentage spending on ICT infrastructure security as this function occurs at Group level. P1 said that, “currently the ICT department relies on Group initiatives to resolve infrastructure security” (Appendix P1, IQ 10). P4 supported P1, stating that, “security is a Group function not Operational division” (Appendix B4, IQ 10).

Finding 18: ICT infrastructure security budget is a Group function and not at operational level

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/threats from inside and outside Transnet?

Interview Question 1.1.11: *What ICT services does the ICT department outsource?*

All participants have knowledge of one or more ICT services that are outsourced.

P1, P2, P4, P5, P7, P9, P11, P13, and P14 mentioned Active Directory, network infrastructure, perimeter defence, email, and exchange as ICT services that they outsource. P2 stated that, “Security services are managed by external parties, for example, user administration (for user access, deletion, and modification). Internally, a dedicated team is overseeing the trends and act upon the resolution of breaches when identified” (Appendix B2, IQ 11). Other outsourced ICT services mentioned during the interviews include CCTV maintenance, network and server management, printer maintenance, management of IT systems and installation of fibre cables.

Finding 19: All participants know of ICT services that are outsourced

Finding 20: Several ICT services are outsourced depending on the Operating Division (OD), including Active Directory (AD); network infrastructure; CCTV maintenance; fibre cable installations; server management, compliance, and monitoring of ICT services; management of IT systems and workstations in some ODs; and emails and exchange

Finding 21: Security services are managed by external parties

Interview Question 1.1.12: *Why does the ICT department outsource these ICT services?*

The majority of interviewees mentioned cost savings, non-core functions, shortage of skills, and expertise as primary reasons for outsourcing ICT services, while P13 said he does not know why ICT services are being outsourced. P1 said that “our organisation used to own all these services in house; these departments were sold off to other companies and we went [on] a pay-per-service model, as it was cheaper to pay for the service than hosting it internally” (Appendix B1, IQ 12). P2 supported P1, stating that, “reasons could include that these are so specialised it would make more sense financially to have companies that are experts at this to do it and pay them” (Appendix B2, IQ 12).

P15 gave a broader reason for the cost factor:

“You outsource it generally because of the costs. If you had to insource that [the services], you would have to buy the hardware on which all those services/machines run; you would have maintenance done on that hardware. So you have that hardware, you [are] buying the hardware; so it is a capital outlay plus you got an operational apex cost to maintain that hardware and then probably the most important thing is your labour cost. So, I think the biggest reason for wanting to outsource is the fact that it is cost driven. There is a smaller element which then basically means that you can free up because, remember now, you got all that labour, hardware and stuff—you need to have all kinds of SOPs in place, how the equipment must be operated and all of that. You need SOPs. You need the government’s framework around it” (Appendix B15, IQ 12).

P4, P5, P9, P10, P11, P12, and P16 all identified shortage of skills and expertise as well as the non-core function factors as the main reasons for outsourcing ICT services.

P5 pointed out that,

“This is not our core business so we outsource it. T-systems specialise [in] it so they can provide resources. As IT, we need to stay ahead of technology so [that the] vendor stays ahead on behalf of clients. If you know you [are] going to use that service for 20 years, you should surely take a long-term position having that service inside the company and train people to have the capacity to do the job and grow the business. ICT is important to business so I believe we should have it in-house and make it core” (Appendix B5, IQ 12).

P4 supported P5 by stating: “Most ODs do not have the skills and it is seen as non-core to Transnet business” (Appendix B4, IQ 12).

Other reasons identified during the interviews are internal ICT services, for example, the network that is part of Transtel (previous network infrastructure administrators and managers) has been inherited, and ICT outsourcing that is part of the Transnet strategy in order to build in-house capacity.

Finding 22: Primary reasons for outsourcing ICT services are cost factors; shortage of skills and expertise; ICT is seen as a non-core function by the organisations; certain ICT functions are inherited; and ICT outsourcing is seen as the Transnet strategy to build capacity in-house

Interview Question 1.1.13: *Are criteria used to select suitable ICT vendors?*

The majority (16) of participants mentioned the procurement process in place to select a suitable ICT vendor as a criterion. Only P8 indicated that he does not know what the process is or entails. The procurement process consists of several criteria based on the requirements or business case of the project. P5 indicated that “It is a long procurement process. It includes pricing, ability to serve countrywide (capacity), track record of vendor, tax clearance certificate, technical ability to serve business function such as licenses and software to address business need” (Appendix B5, IQ 13). P12 supported P5, indicating that “This is done through a tender process that our procurement department handles. We provide them with specifications such as what services we needed, etc. They will then go out on tender for three quotes. Procurements will look at different factors such as cost, experiences, and reputations of ICT vendors” (Appendix B12, IQ 13).

P14, P16, and P17 also mentioned the reliability of the supplier, track records, business licensing, and Black Economic Empowerment (BEE) status as criteria that are included in the procurement process when selecting a suitable vendor.

Finding 23: Well-documented procurement processes are in place, which include criteria that must be fulfilled

Interview Question 1.1.14: *Does any of the ICT vendors have access to your systems or networks?*

Of the 17 participants, 14 indicated that ICT vendors do have access to the systems or network, while P2, P16, and P17 said no. P2 said that ICT vendors do not have access to the systems or networks, and “access is granted as an exception to maintain absolute control” (Appendix B2, IQ 14). Contrary to P2, P1 explained that, “as they own the network and services that they provide to us they are the custodians and have full access to our systems and networks; for them the ability to support the business and service they provide” (Appendix B1, IQ 14). P4 also pointed out that the ICT vendors are connected directly onto the network. P11 went a step further, explaining the direct access by stating that “some have direct access because of the nature of their services provided, such as network infrastructure and/or control of our Active Directory. Others need to follow software authentication through firewalls and other software such as Citrix” (Appendix B11, IQ 14).

P6, P9, P12, and P14 mentioned Virtual Private Networks (VPN), Access Point Name (APN), and Citrix as some of the remote tools used by vendors to access the systems and network from outside the organisation. Additionally to the remote tools. P7 said that vendors can also obtain a username and password (AD account) to access the systems by following the access management process.

Finding 24: Some ICT vendors have full access to the systems and networks

Interview Question 1.1.15: *Are there different levels of access to the systems and networks for ICT vendors?*

The majority (14) of participants indicated that access could range from read-only to full access based on the role of the vendor and their contract. P2 however disagreed with the majority of the participants, stating that, “a standard procedure is applicable to all vendors and access is granted on an exception basis” (Appendix B2, IQ 15). P6 disagreed with P2 by saying that “ICT Vendors have full access to most systems/services as a bulk of our environment is outsourced” (Appendix B6, IQ 15).

P1 agreed with P6, clarifying as follows:

“If we own the system and the vendors require access to assist us with say software that we have where we own the back-end, we give them read and write access to assist; in trouble shooting the system we retain full access. If it is a service that is provide to us like networks or exchange, the vendor retains the full access and we get the read and write access” (Appendix B1, IQ 15).

P15 supported what P6 said by stating that “there will be different levels of access depending on the level of outsourcing. If it is fully outsourced, they run it, so they will have admin rights. We as Transnet might not have the same access as them” (Appendix B15, IQ 15).

Finding 25: Levels of access range from read to full access depending on the role of ICT vendor

Finding 26: Participants disagree on how levels of access to systems and networks are granted to ICT vendors

Interview Question 1.1.16: *Is there any measures in place to deal with ICT security risks/ threats at the different levels?*

Thirteen (13) participants know the measures in place to deal with ICT security risks/threats at the different levels, while four (4) participants are unsure of what these measures are. P12 stated the following: “Yes, this is determined by the type of service they provide” (Appendix B12, IQ 16). P11 supported what P12 said: “This is controlled at Group level, and at local level, we do receive reports regarding ‘traffic’ through our firewalls giving us an insight of what may potentially be a threat, and how often the attempts are made” (Appendix B11, IQ 16). Contrary to what P12 and P11 said, P1 explained:

“If we own and manage the system we scan these often for security risks and vulnerabilities and fix them where required; these are done by using systems to scan all environments that we have for changes and implement accordingly to manage and monitor our risks and threats we have. Environments that are not owned by us, we rely on the service agreements and our Group security team to scan these systems and rectify these services outside of our control for security issues and vulnerabilities” (Appendix B1, IQ 16).

P4 stated that the organisation has a “Network and Security Operations Centre is in place that monitors the environment for vulnerabilities, breaches, etc. This is going to be further invested in with a new system that is being procured at a group level” (Appendix B4, IQ 16). Although the new systems are in the beginning stages, P6

said the ICT department has “vulnerability management, penetration testing, security assessments and audits” (Appendix B6, IQ 16) in place to deal with ICT security risks/threats at the different levels. Furthermore, P9 provided more detail by explaining that ICT security risks/threats are “escalated at Group level and then pushed down to the OD level for rectifying. A timeframe is given to fix the vulnerability depending on the seriousness of the risk. There is a ranking scale in terms of high, medium, and low” (Appendix B9, IQ 16). P10 agreed with what P9 said, stating that measures are,

“...as per incident response categories. Incidents (e.g. failed log in attempts—could be a possible hack/attack; virus activity, etc.) are logged on the T-systems help desk. Categories are based on business risk, for example, Level 1 priority incident (show stopper) needs to be resolved in a much shorter time frame (e.g. 2 hours) compared to a level 4 (no immediate impact on business) of 48 hours” (Appendix B10, IQ 16).

Other measures mentioned during the interviews include access management processes, virus protection software, networking monitoring tools, and policies that are in place. Drawing from what most of the participants answered, one can say that the organisation does have measures in place to deal with ICT security risks/ threats at the different levels.

Finding 27: The ICT department does have measures in place to deal with ICT security risks/threats at the different levels

Finding 28: Some participants still believe putting measures in place to deal with ICT security risks/threats at the different levels is a Group function/responsibility

Interview Question 1.1.17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

The majority (11) of the participants indicated that the ICT department does have information security awareness programmes in place, but outsourcing and vendor risks are not included. P11 said that, “we do have briefings every now and then but I think we do not do enough” (Appendix B11, IQ 17). P9 agreed with P11, pointing out that training is “to a minimal extent; travel as [part of] the company is on cost cutting strategies, and travel for such a nature is cut, and it is not effective holding such awareness campaigns over a video conference” (Appendix B9, IQ 17).

In terms of the cost factor and training programmes, P1 said that,

“...these programmes are needed and all security risks need training programmes in our organisation. It is seen as money spent and a cost, so it is often not done from budget point of view as seen as money wasted. The people controlling the budgets do not understand the impact of these risks as many have never experienced one first hand” (Appendix B1, IQ 17).

Finding 29: The ICT department does have ICT training programmes in place; however, it does not cover infrastructure security risks associated with ICT outsourcing

Finding 30: There is minimal awareness training on infrastructure security risks due to cost cuts

SRQ 2.2: How does the ICT department ensure that they do not become dependent on their ICT service providers?

Interview Question 1.1.18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

Based on the responds of the 17 participants during the interviews it can be concluded that the ICT department will not be able to operate without ICT service providers. The majority of the interviewees gave a scale value of eight (8), followed by ten (10) in response to IQ 1.1.18.

Finding 31: The ICT department is highly dependent on the ICT service provider

Interview Question 1.1.19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

The majority (9) of participants indicated that the ICT department does not have any plan to replace the ICT vendors immediately if something goes wrong, while five participants (P2, P10, P13, P15, P16) said yes and three participants (P3, P14, P17) indicated that they are unsure. P10, who said yes, explained that since December 2014 Transnet got a contract in place. Neotel manages the network and Transnet owns the infrastructure with critical spares, making Transnet less dependent. Should anything happen to vendors, such as buy out for some reason, new vendors can go onsite and manage the network based on a contract agreement.

P13, who also indicated yes, explained the following:

“...currently, if Neotel or T-Systems experience problems, we are affected. There are plans to change the structure of the networks, which will reduce reliance on the vendors. I am aware that if a specific datacentre goes down, we do lose access to some of the applications. I cannot speak to the specific plans if that happens; I have not seen anything regarding that” (Appendix B13, IQ 19).

P2 believed that “the current thinking is that absolute dependence on vendors should be minimised and internal resources be upskilled to counter the threat” (Appendix B2, IQ 19). Contrary to what the above participants said, P1 provided more details for why he said that the ICT department does not have any plans in place to replace the ICT vendors immediately if something goes wrong. P1 explained:

“We sign lengthy contracts with these service providers and often do not include exit and termination conditions in these contracts when signed; our ability to change providers rapidly is non-existent. Also, as our organisation has multiple ODs, certain ODs have built their dependencies on certain providers that also makes it impossible for us to ever leave our providers we have at current, let alone if something goes wrong. And as we have seen, two of our service providers are still the current service providers that we had when we were breached and compromised, yet our systems rely on them too much for us to get new providers in” (Appendix B1, IQ 19).

Even though P1 mentioned the breach, P4 indicated that:

“Contracts with key vendors have just been renewed or extended. At this stage, we do not have any alternative short term to replace the vendor; the vendor management from both a financial sustainability and performance point of view ensure that we do not put the business at risk of this occurring” (Appendix B4, IQ 19).

P9 is in agreement with P1 and P4, stating: “The current vendors are so entrenched into the organisation that breakaway is very costly and the handover/transition period is very long. The organisation has to plan a buy-back option of infrastructure before it can move to other service providers so as not to lose business productivity” (Appendix B9, IQ 19).

Finding 32: The ICT department does not have plans in place to replace ICT vendors immediately if something goes wrong

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet information against ICT infrastructure security threats when outsourcing ICT functions?

Interview Question 1.1.20: Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?

The majority (11) of participants do have knowledge of the ICT frameworks used to protect business against ICT infrastructure security threats when outsourcing ICT functions. P3 mentioned COBIT for IT risk and governance, ISO 27001 and ISO 27002 for information security, and ITIL for service delivery. P10 agreed with P3 by explaining:

“Transnet has adopted the ISO 27001 as the information security framework. However, there is also a governance framework (minimum control framework), based on COBIT and ITIL, that is in place and covers certain information security controls. Transnet also mapped the gaps not covered in the Minimum control framework to ISO27001” (Appendix B10, IQ 20).

According to P4, the transport organisation “Transnet has a customised internal control framework for EIMS/ICT” (Appendix B4, IQ 20) that is based on ITIL and COBIT.

Finding 33: The ICT department uses ITIL, ISO 27001/2, and COBIT as frameworks to protect business against ICT infrastructure security threats when outsourcing ICT functions

Interview Question 1.1.21: Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?

Most (11) of the participants are in agreement that the ICT frameworks mentioned in finding 33 can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions. ICT frameworks provide guidelines for best practice implementation, assist in identifying threats, help integrating previous learning and experiences, and provide a base to build on. P1 explained:

“The frameworks give us a base to build on and a guide of what is required and needed from using the frameworks. We often take these and use them to build our own internal frameworks based on these international standards to have a more robust and properly define framework catered for our individual systems, to better manage and get what is required from us to our vendor” (Appendix B1, IQ 21).

P5 offered a shorter reason: “Someone did the pre-thinking for us; all we need to do is follow the guidance and do not need to re-invent the wheel” (Appendix B5, IQ 21).

According to P4, frameworks ensure that appropriate governance and controls are in place in order to manage vendors and contracts accordingly. P10 supported P4 by stating that ICT frameworks can provide certain controls to ensure that the ICT department manages and monitors risks associated with vendors effectively. However, P10 also points out that “if the control is not enforced, it will not operate adequately” (Appendix B10, IQ 21).

Finding 34: The majority of participants are of the opinion that ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions

Finding 35: Controls in the ICT frameworks are not adequately enforced

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

Interview Question 1.1.22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

From the 17 participants interviewed, the majority (10) said that the ICT department does have systems in place to check if ICT vendors adhere to security and compliance requirements. P1, P2, P3, and P6 all mentioned internal audits as a method/system that is used to determine if vendors adhere to the security and compliance requirements. P2 stated that “adherence to policies and standard is checked and enforced by the security team or Internal Audit” (Appendix B2, IQ 22). To support P2, P3 said that “SLAs are defined and the vendors are measured against it. They are also audited to ensure that they comply with the policies and standards of our organisation” (Appendix B3, IQ 22). P10 also mentioned regular audits (annually) of high-risk ICT vendors (e.g. T-Systems/Neotel) as a method. According to P10, “service level agreements should also cover adherence to information security policies and procedures; not sure if this is in place for all vendors” (Appendix B10, IQ 22).

There were other methods/systems mentioned during the interviews, namely automated tools used for monitoring of vendors and the procurement processes that must be followed to ensure that vendors adhere to internal standards. However, two

participants (P11, P12) were unsure or had no knowledge of any systems in place to check if ICT vendors adhere to the security and compliance requirements. P12 indicated that this function resides at Group level, thus he was not sure. P11 said that “there are vendor management department/s but I have no knowledge on the how. Locally, we set and request the access levels to vendors we deal with directly” (Appendix B11, IQ 22). Contrary to what the majority said, P9 indicated that at present there are not any systems in place to check if ICT vendors adhere to security and compliance requirements. P9 suggested “a monitoring facility/SLA reporting on the vendor’s security policies, procedures, their audit reports, and access to any information regarding any vulnerability within the vendor’s organisation in terms of security” (Appendix B9, IQ 22). P4, who also answered no, indicated that audits are done on an exception basis. According to P10, issues detected by the Security Operations Centre and monitoring should be investigated immediately.

Finding 36: The ICT department does have systems in place to check if ICT vendors adhere to security and compliance requirements

Finding 37: Vendor security and compliance issues are not addressed immediately when detected

Interview Question 1.1.23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

P2, P3, P4, P5, P7, P8, P9, P15, and P16 pointed to a condition in the primary contracts stating that sub-contractors must adhere to the same rules as the primary ICT vendor. P4 explained that “all contract terms and all associated rules apply to sub-contractors (where this is allowed). We do not have other tools to do this” (Appendix P4, IQ 23). From the 17 participants interviewed, a few participants are unsure of processes/procedures in place to ensure that sub-contractors adhere to the same rules of primary vendors. P10 said that he is “not sure if these exist specifically for sub-contractors of primary vendors. However, this would fall under the same procedure/process as for primary vendors. The only difference is that sub-contractors should be the responsibility of the primary vendor and the primary vendor will be held accountable/liable for any misconduct” (Appendix B10, IQ 23).

P13 is in agreement with P10, stating that, “I am not aware of any specific processes/procedures for sub-contracting. The vendor is ultimately responsible and accountable for delivering according to requirements—they must take the risk of

sub-contracting. I suppose any restrictions will be included in the contract/SLA” (Appendix B13, IQ 23).

P1 and P6 disagree with the majority of participants. P1 argued that,

“...the contracts we have do not include the sub-contractors that do the work of the vendor. Those agreements are often between the vendor and his sub-contractor. If there are issues, we have to measure the vendor, which in some cases is not the person or company actually doing the work. Usually the issues that I have seen is due to the vendor not conveying the rules and requirements through to the sub-contractor, leaving the issue between the organisation and vendor to resolve and not the sub-contractor” (Appendix B1, IQ 23).

P6, who also answered no, indicated that “some ICT suppliers deal directly with end-users, bypassing security controls; no end-to-end visibility or enforcement” (Appendix B6, IQ 23).

Finding 38: Primary contracts stipulate that secondary vendors must adhere to the same rules of the primary vendor

Finding 39: Primary vendors do not convey rules to secondary vendors

Finding 40: End-users deal directly with ICT vendors, bypassing security controls

4.4.2 Summary of the findings

For the ease of reading, findings are listed per research question below. Based on the findings, the developed themes are indicated in sub-section 4.4.1.

RQ 1: What information risks does the ICT department manage when outsourcing ICT projects?

SRQ 1.1: What type of access do the ICT vendors have to Transnet’s information and systems?

For findings, see Table 4.2.

Table 4.2: Findings of SRQ 1.1

Finding 1	There is no specific definition for information risks within the organisation
Finding 2	Information risk management is seen as important to the business
Finding 3	There are different ICT vendor access processes
Finding 4	ICT vendor access management processes are not enforced or reviewed frequently
Finding 5	Access restriction is not always specific
Finding 6	Key suppliers have full access to the systems and network infrastructure

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

For findings, see Table 4.3.

Table 4.3: Findings of SRQ 1.2

Finding 7	Exploiting or disclosure of confidential information to third parties is seen as a risk
Finding 8	Risk meetings and risk assessments are conducted per project
Finding 9	Risks are managed through <i>ad-hoc</i> security assessments, but this is not the case for all outsourced environments
Finding 10	Several participants are not aware of methods used to determine the impact of information risks when outsourcing ICT projects

SRQ 1.3: What strategies do the ICT department have in place to manage information risks associated with ICT outsourcing?

For findings, see Table 4.4.

Table 4.4: Findings of SRQ 1.3

Finding 11	The majority of participants are aware of information and ICT infrastructure security risks when outsourcing
Finding 12	Core systems are hosted by an ICT vendor
Finding 13	Illegal activities are not reviewed or picked up, and compliance is not monitored
Finding 14	The majority participants are familiar with methods in place to reduce and manage information and ICT infrastructure security risks
Finding 15	Audits take place on a yearly or <i>ad-hoc</i> basis
Finding 16	There are no direct mechanisms to deal with the risks of infrastructure outsourcing

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

For findings, see Table 4.5.

Table 4.5: Findings of SRQ 1.4

Finding 17	The majority of participants are not aware of criteria used to measure the ICT security success rate of ICT vendors
Finding 18	ICT infrastructure security budget is a Group function and not at operational level

RQ 2: How can the ICT department protect their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside Transnet?

For findings, see Table 4.6.

Table 4.6: Findings of SRQ 2.1

Finding 19	All participants know of ICT services that are outsourced
Finding 20	Several ICT services are outsourced depending on the Operating Division (OD), including Active Directory (AD); network infrastructure; CCTV maintenance; fibre cable installations; server management, compliance, and monitoring of ICT services; management of IT systems and workstations in some ODs; and emails and exchange
Finding 21	Security services are managed by external parties
Finding 22	Primary reasons for outsourcing ICT services are cost factors; shortage of skills and expertise; ICT is seen as a non-core function by the organisations; certain ICT functions are inherited; and ICT outsourcing is seen as the Transnet strategy to build capacity in-house
Finding 23	Well-documented procurement processes are in place, which include criteria that must be fulfilled
Finding 24	Some ICT vendors have full access to the systems and networks
Finding 25	Levels of access range from read to full access depending on the role of ICT vendor
Finding 26	Participants disagree on how levels of access to systems and networks are granted to ICT vendors
Finding 27	The ICT department does have measures in place to deal with ICT security risks/threats at the different levels
Finding 28	Some participants still believe putting measures in place to deal with ICT security risks/threats at the different levels is a Group function/responsibility

Finding 29	The ICT department does have ICT training programmes in place; however, it does not cover infrastructure security risks associated with ICT outsourcing
Finding 30	There is minimal awareness training on infrastructure security risks due to cost cuts

SRQ 2.2: How does the ICT department ensure that they do not become dependent on their ICT service providers?

For findings, see Table 4.7.

Table 4.7: Findings of SRQ 2.2

Finding 31	The ICT department is highly dependent on the ICT service provider.
Finding 32	The ICT department does not have plans in place to replace ICT vendors immediately if something goes wrong

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet information against ICT infrastructure security threats when outsourcing ICT functions?

For findings, see Table 4.8.

Table 4.8: Findings of SRQ 2.3

Finding 33	The ICT department uses ITIL, ISO 27001/2, and COBIT as frameworks to protect business against ICT infrastructure security threats when outsourcing ICT functions
Finding 34	The majority of participants are of the opinion that ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions
Finding 35	Controls in the ICT frameworks are not adequately enforced

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

For findings, see Table 4.9.

Table 4.9: Findings of SRQ 2.4

Finding 36	The ICT department does have systems in place to check if ICT vendors adhere to security and compliance requirements
Finding 37	Vendor security and compliance issues are not addressed immediately when detected
Finding 38	Primary contracts stipulate that secondary vendors must adhere to the same rules of the primary vendor
Finding 39	Primary vendors do not convey rules to secondary vendors
Finding 40	End-users deal directly with ICT vendors, bypassing security controls

4.4.3 Summary of findings and theme development

Table 4.10 presents the findings and related themes linked to Research Question 1.

Table 4.10: Findings and related themes for RQ 1

Research Question 1	Sub-themes	Themes
Finding 1: There is no specific definition for information risks within the organisation	Information risk definitions	Information risks
Finding 2: Information risk management is seen as important to the business	Information risk management	Risk management
Finding 3: There are different ICT vendor access processes	ICT vendor access processes	Vendor access and management
Finding 4: ICT vendor access management processes are not enforced or reviewed frequently	ICT vendor access processes Enforcing of access processes	Vendor access and management
Finding 5: Access restriction is not always specific	Access management/ restriction	Vendor access and management
Finding 6: Key suppliers have full access to the systems and network infrastructure	Full access to systems and network infrastructure	Vendor access and management
Finding 7: Exploiting or disclosure of confidential information to third parties is seen as a risk	Confidential information disclosure or exploitation	Information risks
Finding 8: Risk meetings and risk assessments are conducted per project	Risk assessments	Risk management
Finding 9: Risks are managed through <i>ad-hoc</i> security assessments, but this is not the case for all outsourced environments	Risk Management Ad-hoc security assessments	Risk management
Finding 10: Several participants are not aware of methods used to determine the impact of information risks when outsourcing ICT projects	Unawareness of determining impacts of information risks when outsourcing	Information risks
Finding 11: The majority of participants are aware of information and ICT infrastructure security risks when outsourcing	Awareness of information and ICT infrastructure security risks	Information risks

Research Question 1	Sub-themes	Themes
Finding 12: Core systems are hosted by an ICT vendor	Hosting of core systems	Vendor access and management
Finding 13: Illegal activities are not reviewed or picked up, and compliance is not monitored	Illegal activities not reviewed	Vendor access and management
Finding 14: The majority participants are familiar with methods in place to reduce and manage information and ICT infrastructure security risks	Methods in place to reduce and manage information and ICT infrastructure security risks	Information risks
Finding 15: Audits take place on a yearly or <i>ad-hoc</i> basis	Ad-hoc audits	Risk management
Finding 16: There are no direct mechanisms to deal with the risks of infrastructure outsourcing	No mechanisms for dealing with infrastructure outsourcing risks	Risk management
Finding 17: The majority of participants are not aware of criteria used to measure the ICT security success rate of ICT vendors	Unawareness of criteria used to measure ICT security success rates of ICT vendors	Vendor access and management
Finding 18: ICT infrastructure security budget is a Group function and not at operational level	Accountability and responsibility of ICT infrastructure security	Costs

Table 4.11 presents the findings and related themes linked to Research Question 2.

Table 4.11: Findings and related themes for RQ 2

Research Question 2	Sub-themes	Themes
Finding 19: All participants know of ICT services that are outsourced	Knowledge on ICT services that are outsourced	ICT Outsourcing
Finding 20: Several ICT services are outsourced depending on the Operating Division (OD), including Active Directory (AD); network infrastructure; CCTV maintenance; fibre cable installations; server management, compliance, and monitoring of ICT services; management of IT systems and workstations in some ODs; and emails and exchange	Various services outsourced by ICT department	ICT Outsourcing
Finding 21: Security services are managed by external parties	Managing of security services	Vendor access and management
Finding 22: Primary reasons for outsourcing ICT services are cost factors; shortage of skills and expertise; ICT is seen as a non-core function by the organisations; certain ICT functions are inherited; and ICT outsourcing is seen as the Transnet strategy to build capacity in-house	Motives for outsourcings ICT services	ICT Outsourcing

Research Question 2	Sub-themes	Themes
Finding 23: Well-documented procurement processes are in place, which include criteria that must be fulfilled	Procurement processes and criteria	ICT Outsourcing
Finding 24: Some ICT vendors have full access to the systems and networks	Access management to systems and networks	Vendor access and management
Finding 25: Levels of access range from read to full access depending on the role of ICT vendor	Access management	Vendor access and management
Finding 26: Participants disagree on how levels of access to systems and networks are granted to ICT vendors	Disagreement amongst participants on access	Vendor access and management
Finding 27: The ICT department does have measures in place to deal with ICT security risks/threats at the different levels	Dealing with ICT risks or threats at different levels	Risk management
Finding 28: Some participants still believe putting measures in place to deal with ICT security risks/threats at the different levels is a Group function/responsibility	Accountability and responsibility of ICT security risks/threats	Risk management
Finding 29: The ICT department does have ICT training programmes in place; however, it does not cover infrastructure security risks associated with ICT outsourcing	ICT programmes / training / awareness	User awareness
Finding 30: There is minimal awareness training on infrastructure security risks due to cost cuts	Infrastructure security risks awareness programmes	User awareness
Finding 31: The ICT department is highly dependent on the ICT service provider	Dependability on ICT vendors	ICT vendor dependency
Finding 32: The ICT department does not have plans in place to replace ICT vendors immediately if something goes wrong	Dependability on ICT vendors	ICT vendor dependency
Finding 33: The ICT department uses ITIL, ISO 27001/2, and COBIT as frameworks to protect business against ICT infrastructure security threats when outsourcing ICT functions	ITIL, ISO 27001/2 and COBIT	Frameworks
Finding 34: The majority of participants are of the opinion that ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions	Importance of implementing frameworks to protect ICT department against information and infrastructure security threats when outsourcing ICT functions.	Frameworks
Finding 35: Controls in the ICT frameworks are not adequately enforced	Importance of implementing frameworks	Frameworks
Finding 36: The ICT department does have systems in place to check if ICT vendors adhere to security and compliance requirements	Adhering to security and compliance requirements	Vendor access and management

Research Question 2	Sub-themes	Themes
Finding 37: Vendor security and compliance issues are not addressed immediately when detected	Adhering to security and compliance requirements	Vendor access and management
Finding 38: Primary contracts stipulate that secondary vendors must adhere to the same rules of the primary vendor	Secondary vendor management	Vendor access and management
Finding 39: Primary vendors do not convey rules to secondary vendors	Secondary vendor management	Vendor access and management
Finding 40: End-users deal directly with ICT vendors, bypassing security controls	Dealing with ICT vendors	User awareness

4.5 Themes

In this chapter, information of the case used for the research is discussed. Data from the interviews (consisting of 23 interview questions and answered by 17 participants) conducted during the research process, is analysed. Forty (40) findings are identified based on the analysis of the data. Eight themes deemed important are identified from the 40 findings.

These eight themes are as follows:

- I. Information risks
- II. ICT Outsourcing
- III. Costs
- IV. Vendor access and management
- V. ICT vendor dependency
- VI. Risk Management
- VII. Frameworks
- VIII. User awareness

Tables 4.12 and 4.13 present the themes per research question.

Table 4.12: Themes developed based on RQ 1 and research sub-questions

Research Questions	Themes
RQ 1: What information risks does the ICT department manage when outsourcing ICT projects?	<ul style="list-style-type: none"> • Information risks • Risk management • Vendor access management • Costs
RQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?	<ul style="list-style-type: none"> • Information risks • Risk management • Vendor access management
RQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?	<ul style="list-style-type: none"> • Information risks • Risk management
RQ 1.3: What strategies do the ICT department have in place to manage information risks associated with ICT outsourcing?	<ul style="list-style-type: none"> • Information risks • Vendor access management • Risk management
RQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?	<ul style="list-style-type: none"> • Vendor risk management • Costs

Table 4.13: Themes developed based on RQ 2 and research sub-questions

Research Questions	Themes
RQ 2: How can the ICT department protect their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT?	<ul style="list-style-type: none"> • ICT outsourcing • Vendor access management • Risk management • User awareness • ICT vendor dependency • Frameworks • User awareness
RQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside the Transnet?	<ul style="list-style-type: none"> • ICT outsourcing • Vendor access management • Risk management • User awareness
RQ 2.2: How does the ICT department ensure that they do not become dependent on their ICT service providers?	<ul style="list-style-type: none"> • ICT vendor dependency
RQ 2.3: How can the implementation of an ICT framework/s protect Transnet information against ICT infrastructure security threats when outsourcing ICT functions?	<ul style="list-style-type: none"> • Frameworks
RQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?	<ul style="list-style-type: none"> • Vendor access management • User awareness

4.6 Summary

Chapter 5 provided the reader with a background of the case used for the research, herein referred to Transnet SOC Ltd. Transnet SOC Ltd is the largest and most important transport and logistics supply chain ensuring that goods are delivered to South Africans on a daily basis. The organisation consists of five (5) operating divisions, fully owned by the Government of South Africa although the company is operated as a corporate entity. Each division consists of various departments, e.g. Human Resources, Operations, Marketing, and ICT.

For the purpose of the research, 17 participants situated across the five operating divisions, were interviewed. The participants included managers and executive managers as well as consultants, analysts, and specialists in the ICT field. All of the participants have years of experience in ICT and ICT outsourcing.

Based on the responses and analysis of the answers, findings were developed for each interview question through transcribing, summarising, and categorising the data, as discussed in Chapter 3. From the 40 findings, 10 headline findings have been identified.

Headline finding 1: ICT vendor access management processes are not enforced or reviewed frequently as required

Headline finding 2: Access restriction is not always specific

Headline finding 3: Key suppliers have full access to the systems and network infrastructure

Headline finding 4: Core systems are hosted by an ICT vendor

Headline finding 5: There is no specific definition for information risks within the organisation

Headline finding 6: Several participants are not aware of methods used to determine the impact of information risks when outsourcing ICT projects

Headline finding 7: The exploitation or disclosure of confidential information to third parties are seen as the highest information risk when outsourcing ICT

Headline finding 8: Risks are managed through ad-hoc security assessments

Headline finding 9: The outsourcing business does not have any plans in place to replace ICT vendors immediately if anything goes wrong

Headline finding 10: Compliance issues are not addressed immediately when detected by the outsourcing business

From the 40 findings, eight themes were identified. These themes are: ICT outsourcing, information risks, costs, ICT vendor dependency; vendor access and management; risk management; user awareness; and frameworks. In Chapter 5, the themes are discussed and linked to the research questions and aim of the study.

CHAPTER 5: DISCUSSION

5.1 Introduction

With increasing costs and higher risks, organisations are facing more and bigger challenges in securing their ICT portfolio. In an endeavour to be more cost effective and efficient and to satisfy the organisation's needs, many organisations turn to the outsourcing of their ICT portfolio or at least some part of the portfolio. By doing so, the organisation is exposed to risks. From the findings as described in Chapter 4, eight themes have been identified. These themes are ICT outsourcing, information risks, costs, ICT vendor dependency, vendor access and management, risk management, user awareness, and frameworks.

In Chapter 5, the themes are discussed and linked to the research questions and aim of the study. At the end of the chapter, guidelines are proposed and conclusions given. Several risks/information risks are identified when outsourcing ICT. The information risks are related to vendor access management processes, information risk management processes, ICT infrastructure security processes, and at the end-user level. Table 4.2 to Table 4.10 in Chapter 4 provide details of each finding and themes developed based on the 40 findings.

For ease of reading, the problem statement, research questions, and aim of the study are listed below:

Problem Statement: It is unclear how to manage information risks through the usage of ICT infrastructure risk management when outsourcing ICT projects, and this exposes organisations to ICT security risks.

Research Question 1: What information risks does the ICT department manage when outsourcing ICT projects?

Research Question 2: How can the ICT department protect their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT?

Aim of the study: To explore how the organisation can manage information risks through the usage of infrastructure risk management when outsourcing ICT projects.

5.2 The themes

5.2.1 Theme 1: ICT outsourcing

ICT outsourcing is the handover or re-location of ICT activities or processes such as ICT projects, assets, hosting of websites, ICT infrastructures, training of staff, auditing of ICT security, and application development to a third party or company within the country or outside (Samantra et al., 2014; Sá-soares et al., 2014; Khidzir et al., 2013a; Urbach & Würz, 2012; Narasimhaiah & Chiravuri, 2011).

In the organisation where the study has been conducted, all of the participants are aware and know of the ICT services being outsourced (Table 4.10, Finding 19). Several ICT services are outsourced depending on the Operating Division (OD), including Active Directory (AD); network infrastructure; CCTV maintenance; fibre cable installations; server management, compliance, and monitoring of ICT services; management of IT systems and workstations in some ODs; and emails and exchange (Table 4.10, Finding 20).

Numerous reasons are mentioned in literature for the outsourcing of ICT, such as cost cuts, focusing on core functions, and improving efficiency (Murthy et al., 2015; Teo & Bhattacharjee, 2014; Yildiz & Demirel, 2014; Kang et al., 2014; Samantra et al., 2014). The findings show that the main reasons for outsourcing ICT services are the same as identified in literature; cost, shortage of skills and expertise, ICT considered as a non-core function, and certain inherited ICT functions are but some of the reasons. The outsourcing of ICT is also seen as a Transnet strategy to build in-house capacity (Table 4.10, Finding 22).

Lee et al. (2012) propose that the outsourcing of ICT functions is included as a business long-term strategy and not simply a short-term benefit. Business needs to have measures in place to ensure that outsourcing strategies are implemented effectively (Kang et al., 2014). It is also evident that selecting the wrong vendor could have negative consequences for outsourced ICT projects (Wattjatrakul, 2014). Business must therefore look at several factors such as security compliance, risk management, and financial matters before outsourcing (Bahl & Wali, 2013).

Mann et al. (2015) go a step further and explain that although the ICT outsourcing strategy may seem as an option for many organisations, the implementation can become complex since business has to find the vendors that suit their needs. To choose an appropriate vendor is a difficult and tedious process. There are many factors to consider before deciding which vendor to select. Fortunately, there are

well-documented procurement processes available that include criteria that must be fulfilled to become an ICT vendor (Table 4.10, Finding 23). P5 stated that the selection of an ICT vendor “is a long procurement process. It includes pricing, ability to serve countrywide (capacity), track record of vendor, tax clearance certificate, technical ability to serve business function such as licenses and software to address business needs” (Appendix B5, IQ 13). Participant 12 mentioned “cost, experiences and reputations of ICT vendors” as some of the factors to be considered by business for the procurement process. Participants 14, 16, and 17 identified other requirements such as the reliability of the supplier, business licensing, and Black Economic Empowerment (BEE) status as some of the factors to consider at before selecting a suitable supplier.

Although the outsourcing business may have a well-documented procurement process in place, a study done by Narasimhaiah and Somers (2014) indicates that the satisfaction level for ICT outsourcing is only 33%, while it is between 70-80% for non-ICT outsourced activities. As a result of the low satisfaction rate or rate of failure, it is important that business pays attention to factors that could have a negative or positive impact on outsourced ICT projects (Lee et al., 2013). According to Hamlen and Thuraingham (2013), many businesses believe that outsourcing is good for both parties involved in the outsourcing agreement, but they do not know of the security vulnerabilities that accompany ICT outsourcing.

5.2.2 Theme 2: Information risks

Information can be seen as the most important asset to the business and threatened by several risks (Silva et al., 2014). A risk can be described as any unexpected problem or threat that needs attention in order to prevent dissatisfaction of a project (Saetang & Haider, 2014). Risks can vary from project to project; for example, the risks associated with ICT infrastructure security projects are different from software development projects, therefore stakeholders needs to have a good understanding of the possible risks each ICT project may carry in order to minimise the impact of the risk and ensure that projects are implemented successfully (Talet et al., 2014:).

It is evident from the research that there is no specific definition for information risks within the organisation (Table 4.9, Finding 1). Participants have a different definition or understanding regarding information risks. P6 stated that the term ‘information risks’ “refers to the threat of information (electronic or printed) being impacted any one way or the other by a threat factor due to a weakness in the controls that are meant to protect such information. The possible impacts are the loss of integrity

(including reliability), confidentiality, and availability” (Appendix B6, IQ 1), while P15 said: “If you look at information as an asset and the fact that it has value, you can then apply all kinds of risks. The asset can be made unavailable or the asset can be stolen. Any of the risks that can have a negative effect on the information asset” (Appendix B15, IQ 1).

When outsourcing ICT services or systems to a third party there are various risks involved (Patil & Wongsurawat, 2015; Kumar et al., 2014). Talet et al. (2014) classify the top five ICT project risks as i) shortage of personnel, ii) unreasonable schedules and budgets, iii) requirements that are not complete, iv) expectations that are unrealistic, and v) software not delivered on time. From the research, it is found that although all participants are aware of some kind of risk when outsourcing ICT, several participants indicated that the exploitation or disclosure of confidential information to third parties is seen as the highest information risk when outsourcing ICT (Table 4.9, Finding 7). Khidzir et al. (2013a) describe information security risks as the theft of employee data and utilisation of intellectual property, while he points out that information security risks can be seen as one of the highest information risks when outsourcing ICT. P1 stated that:

“Ownership or intellectual property is the biggest risk currently that are seen when outsourcing projects to companies for ICT functionality or new projects that we undertake; once these projects are under way or completed the organisation do not [sic] have ownership of the intellectual data or back-end designs of these systems that are managed or built” (Appendix B1, IQ 5).

P9 explains that, “[it is] the loss of intellectual property and business process models that gives the company its competitive edge of doing business over its competitors” (Appendix P9, IQ 5).

Other information risks mentioned by participants include: i) unauthorised access and hacking (P4, P16), ii) vendors not complying with information security and requirements (P10, P13), and iii) the human factors itself (P14). Sá-soares et al. (2014) emphasise that ICT outsourcing risks must be seen as an important factor that needs to be considered when outsourcing ICT activities. Although the participants are aware of some of the information risks, several participants are not aware of methods used to determine the impact of information risks when outsourcing ICT projects (Table 4.9, Finding 10).

ICT projects are not risk free, and the risks encountered during implementation of ICT projects are not just due to financial factors. It is therefore the responsibility of

ICT project managers to take an overall view of the risks and not simply focus on financial risks (Talet et al., 2014). According to Khidzir et al. (2013a), information security risks is seen as one of the highest types of risk when outsourcing ICT projects. From the research conducted, it has been found that the majority of participants are aware of information and ICT infrastructure security risks when outsourcing (Table 4.9, Finding 11). P5 stated that “there is always a risk because the minute you open yourself to [a] third party, there is also risk that they can be hacked indirectly into our systems” (Appendix B5, IQ 7). P1 explained that:

“One of the major risks is with our network provider where we have identified that some core systems that support our system are also hosts to other companies at these break out points. This risk means that if another company is breached through a certain breakout by our provider, we could be in a position that we are breached as well” (Appendix B1, IQ 7).

P10, P13, and P17 mentioned that vendor management and monitoring are not adequate, illegal activities are not reviewed or detected, and compliance is not monitored, as information and ICT infrastructure security risks that can be associated with ICT outsourcing. Silva et al. (2014) point out that there are still managers who do not have the necessary knowledge to put controls in place to deal with ICT security abuse. This could be seen as a huge risk, since ICT managers and information security personnel must be able to identify and understand ICT related issues to be able to address the sources of the threat properly (Shropshire et al., 2015). In this study, it is found that the majority of participants are familiar with methods that are in place to reduce and manage information and ICT infrastructure security risks (Table 4.9, Finding 14). P6 mentioned audits as one of the methods to reduce and manage information and ICT infrastructure security risks, but pointed out that although there are “right-to-audit” clauses in outsourced contracts, assurance exercises take place on an *ad-hoc* basis, while P10 indicated that the outsourcing business do have service level agreements and vendor management processes in place. Petri et al. (2012) suggest that when business decides on a vendor, a SLA must be in place to be used for various reasons such as reward/penalty agreements and identifying the responsibilities of both parties. Rastogi and von Solms (2012) however, point out that information security is still viewed as a technical issue and therefore the responsibility of technical staff in most organisations.

5.2.3 Theme 3: Costs

Security risks can be caused by internal and external factors, and are sometimes seen as a challenging task due to complex environments (Feng et al., 2014). Bayrak (2013) highlights that at corporate level of the organisation, directors and investors

care more about how the applications can help increase revenue and decrease costs. Smaller amounts are invested into ICT security as they believe the risks of ICT security are not high (Silva et al., 2014). According Marabelli et al. (2013), there are only a few organisations that invest in their information or infrastructure security. Although there are many ways to protect information and prevent information security incidents, business cannot protect all their ICT systems as it is not always economically feasible (Nazareth & Choi, 2015). From the research, it was found that the outsourcing business does spend money on ICT infrastructure security, although none of the participants knew the exact amount. The majority indicated that the ICT infrastructure security budget and spending is a Group function, not an operational level function (Table 4.9, Finding 18). P1 said that, “currently the ICT department relies on Group initiatives to resolve infrastructure security” (Appendix P1, IQ 10), This is supported by P4, P5, and P14 who also indicated that the spending on ICT infrastructure security is a Group function.

5.2.4 Theme 4: ICT vendor dependency

According to Bahl and Wali (2014), businesses are critically dependent on the use of ICT. The dependency on ICT has grown (Tøndel et al., 2014) in such a way that when developing strategic ICT systems, many organisations depend on ICT vendor resources, capabilities, and processes (Abdullah & Verner, 2012). Bayrak (2013) agrees with Abdullah and Verner (2012) and states that a major disadvantage of outsourcing is that the business can become heavily depended on a vendor that delivers critical functions to the business and as a result, loses control over the processes. The relationship between the client and ICT service provider may have grown in such a way that the service provider ends up knowing the business processes and ICT services better than the client, ensuring a dependency on the ICT service provider (Aundhe & Mathew, 2009).

Coertze and von Solms (2013b) elaborate that the dependency on ICT by business has increased and ICT is present in almost every business process, which makes it a requirement for the business to operate effectively and efficiently. In the organisation where the study was conducted, the ICT department is highly dependent on the ICT service providers (Table 4.10, Finding 31) and does not have any plans in place to replace ICT vendors immediately if something goes wrong (Table 4.10, Finding 32).

Participant 13 stated that,

“...currently, if Neotel or T-Systems experience problems, we are affected. There are plans to change the structure of the networks, which will reduce reliance on the vendors. I am aware that if a specific datacentre goes down, we do lose access to some of the applications. I cannot speak to the specific plans if that happens; I have not seen anything regarding that” (Appendix B13, IQ 19).

Tafti (2005) suggests that outsourcing business includes a reversible clause in the contract that could provide them with the option of buying back essential services and equipment; for example, human reversibility may allow business to hire individuals that were employed by the ICT vendor to acquire their services and skills. P9 goes a step further by stating: “The current vendors are so entrenched into the organisation that breakaway is very costly and the handover/transition period is very long. The organisation has to plan a buy-back option of infrastructure before it can move to other service providers so as not to lose business productivity” (Appendix B9, IQ 19). Bahli and Rivard (2013) explain that the outsourcing businesses are locked in the ICT relationship in such a way that they cannot get out without incurring costs or losing assets. When participants were asked to indicate the dependency level of business on ICT vendors on a scale from 1 to 10, the overall average of dependency was 80%.

5.2.5 Theme 5: Vendor access and management

It is evident from the research that ‘key suppliers’ have full access to systems and network infrastructure within the case organisation (Table 4.9, Finding 6 & Table 4.10, Finding 24) and that the core systems are hosted by these key suppliers (Table 4.9, Finding 12). It can also be concluded that different access processes are in place for ICT vendors (Table 4.9, Finding 3), and that there is still disagreement among participants on how levels of access to systems and networks are granted to ICT vendors (Table 4.9, Finding 26). Levels of access can vary from read only to full access depending on the role of the ICT vendor (Table 4.10, Finding 25). P7 explained that access is “dependent on their role in the company and the position they have; some of the vendors do have read and write, however, they do follow an approval process for the access granted to them as well as changes (write) is done in line with the appropriate business decisions” (Appendix B7: IQ 4).

However, P15 stated that, “key suppliers have full access because they are managing our AD domains, our DCs, our domain controllers against AD rights, and they are managing our exchange servers. Between those two key suppliers, you

basically have access to everything” (Appendix B15, IQ 4). Humphreys (2008:250-252) suggests that access must be given to individuals based on their responsibilities and duties on a daily basis. Access requests should be formally documented and approved by an authorised person, and business must have measurement processes in place to ensure that access controls are effective. Kang et al. (2014) point out that risk in outsourcing agreements can arise due to a lack of control over ICT vendors. The research however confirms that access restriction is not always specific (Table 4.9, Finding 5), ICT vendor access management processes are not enforced or reviewed frequently (Table 4.9, Finding 4), and illegal activities are not reviewed or picked up and compliance is not monitored (Table 4.9, Finding 13).

It is furthermore found that security services are managed by external parties (Table 4.10, Finding 21) and the majority of participants are not aware of criteria used to measure the ICT security success rate of ICT vendors (Table 4.9, Finding 17). P6 pointed out that “the maturity of the security teams and its process is far off from being able to measure this [sic]” (Appendix B6, IQ 9), while P4 stated that “it is understood that security measurements are in place, but not sure” (Appendix B4, IQ 9). P5 indicated that it is an “interesting and good question; [but] I am not sure about this” (Appendix B5, IQ 9), referring to the question if the ICT department has criteria in place to measure the ICT security success rate of ICT vendors.

According Bahl and Wali (2013), a contributor to ICT security risks is ICT service providers that find it challenging to provide compliance and assurance against security breaches. Bachlechner et al. (2014) state the importance of ICT vendors providing proof that they adhere to security requirements. From the research It is proven that the ICT department does have systems in place to check if ICT vendors adhere to security and compliance requirements (Table 4.10, Finding 36), but vendor security and compliance issues are not addressed immediately when detected (Table 4.10, Finding 37). P1, P2, P3, and P6 all mentioned internal audits as a method/system used to determine if vendors adhere to the security and compliance requirements. P9 suggested “a monitoring facility/SLA reporting on the vendor’s security policies, procedures, their audit reports, and access to any information regarding any vulnerability within the vendor’s organisation in terms of security” (Appendix B9, IQ 22). Humphreys (2008:250-252) also suggests that business performs audits, monitors and reviews firewalls and intrusion detection systems, and obtains feedback and suggestions from customers, vendors, and

employees to improve security weaknesses and determine the effectiveness of information security management.

Another issue identified in the vendor access and management process is that primary vendors that do not convey rules to secondary vendors (Table 4.10, Finding 39). Participant 1 argued:

“The contracts we have do not include the sub-contractors that do the work of the vendor. Those agreements are often between the vendor and his sub-contractor. If there are issues, we have to measure the vendor, which in some cases is not the person or company actually doing the work. Usually the issues that I have seen is due to the vendor not conveying the rules and requirements through to the sub-contractor, leaving the issue between the organisation and vendor to resolve and not the sub-contractor” (Appendix B1, IQ 23).

Bachlechner et al. (2014) mention the fact that organisations that outsource their ICT functions to more than one vendor make it difficult to manage their ICT infrastructures. Karyda et al. (2006) point out that having a single vendor for the total outsourcing of ICT functions can also be seen as a high risk. It is therefore important that security issues of ICT outsourcing be examined and addressed by business and all the suppliers involved (Hamlen & Thuraisingham, 2013). From the research, it is found that primary contracts do indeed stipulate that secondary vendors must adhere to same rules of the primary vendor (Table 4.10, Finding 38). Cheng (2012) suggests that sub-contractors adhere to the same rules of the primary ICT vendor. Then again, ICT vendors could lie about their knowledge and capabilities just to get a contract (Bahli & Rivard, 2013) or employ employees who are not fully qualified as requested by the outsourcing business to perform certain activities (Kumar et al., 2014).

5.2.6 Theme 6: Risk management

According to O'Neill (2014), risk management focuses risk identification, determining the acceptable level of tolerance, formulating strategies for risk mitigation, and putting action plans in place should a predicted risk occur. The management of risk can be seen as one of the primary objectives of an organisation (Tate & Ellram, 2009). When it comes to ICT risk management, the main goal is to ensure that information systems are responsible for retrieving, processing, exporting, and storing the organisation's information in such a way that business can make informed management decisions that justify the investment into ICT expenditures (Talet et al., 2014). From the research, it is evident that information risk

management is important to the business (Table 4.9, Finding 2). P9 stated that “Information risks management is of [the] utmost importance. Information in its simplest form can pose risks in many ways that could have implications ranging from legal and financial to goodwill defamation” (Appendix B9, IQ 2), while P13 explained that the importance of information risk management “depends on the amount and type of information and the reliance the business has on it. For a large corporation like us, information risk management will be extremely important” (Appendix B13, IQ 2). P1 however disagreed with all 16 participants, pointing out that “currently the business shows more importance in identifying risks to the business, but the importance of resolving the risks and issues is of a less importance to the business” (Appendix B1, IQ 2). This could be seen as a huge risk, as Humphreys (2008) indicates that once a risk has been identified, its needs to be captured in a risk register. The risk register should include the severity, impact, and type of risk in order to develop a risk profile of the business; secondly, management needs to measure the cost vs benefit factor of having controls in place to mitigate identified risks against not having any controls in place. Once business decides which controls to put in place, they need to provide training to staff, showing employees how the controls work and allocating security-related responsibilities and roles to individuals.

Ghosh et al. (2011) suggest that in order to manage ICT projects effectively, business needs to adopt and implement the various risk management principles, tools, and techniques. It was however found that risks meetings and risk assessments are conducted per project (Table 4.9, Finding 8) and risks are managed through *ad-hoc* security assessments, but this is not the case for all outsourced environments (Table 4.9, Finding 9). Lee et al. (2012) point out that risk assessments cannot not be done in a single phase; it needs to be an iterative process when formulating a risk management plan.

According to Munteanu and Fotache (2015), when risk assessment is performed on information security, more attention is given to technical factors than social and cultural factors. It is however true that ICT security has become an important factor when managing risks (Feng et al., 2014). ICT security is on the top-10 list of concerns for businesses in 2013. It is therefore important that business identifies information security requirements to ensure that information assets of the organisation are secured when it comes to information security risks (Onyeji et al., 2014). At some stage, an organisation will face some kind of incident related to information security (Tøndel et al., 2014). Nazareth and Choi (2015) indicate that the

management of information security to protect assets is critical for business and is still seen as a challenging task as security incidents increase. From the research, it is found that the case organisation does have measures in place to deal with ICT security risks/threats at the different levels (Table 4.10, Finding 27), although some participants still believe putting measures in place to deal with ICT security risks/threats at the different levels is a Group function/responsibility (Table 4.10, Finding 28). Organisations see ICT risks and governance as an ICT problem, but it should be seen as a business governance matter (Everett, 2011). P4 said that the organisation does have “network and Security Operations Centre is in place that monitors the environment for vulnerabilities, breaches, etc. This is going to be further invested with a new system that is being procured at a group level” (Appendix B4, IQ 16), while P6 stated that the outsourcing business does have “vulnerability management, penetration testing, security assessments and audits” in place to deal with ICT security risks/threats at the different levels (Appendix B6, IQ 16). On the other hand, these audits only occur on an annual or *ad hoc* basis (Table 4.9, Finding 15). Barham (2014) suggests that business can use various tools such as firewalls, antivirus software, password protection mechanisms, and digital signatures to deal with ICT security risks/threats at the different levels. The problems with these tools is that they are designed to detect specific attacks and it does not cover all security needs; for example, network scanners will only scan for vulnerabilities on the network (Moreira et al., 2008).

Humphreys (2008) point out that to protect the organisation’s information assets, the implementation of risk management is the key to the successful protection of information. The only problem is that to date, there is no process allowing business to reduce the risk circumstances before it happens (Ghosh et al., 2011). The managing of information security risks of ICT projects remains a problem for organisations, whether the ICT project is outsourced or not (Liu & Wang, 2014). Adding to the information security risks, it is also evident that the outsourcing business does not have mechanisms in place to deal with risks associated with infrastructure outsourcing (Table 4.9, Finding 16). This is ironic since various sectors depend on information infrastructures to conduct their daily activities and achieve business goals (Chatzipoulidis, 2015). P6 pointed out that, “...although there are ‘right-to-audit’ clauses in outsourced contracts, assurance exercises take place on an ad-hoc basis. There are periodic risk assessments as well as auditing exercises; however, there are no direct mechanisms to deal with the risks of infrastructure outsourcing” (Appendix B6, IQ 8). The conclusion to be made is that organisations have limited knowledge of information security and risks that should be considered

when outsourcing ICT functions (Hamlen & Thuraisingham, 2013; Urbach & Würz, 2012). What makes the problem worse is that budgets for ICT departments are limited and ICT departments do not always have the funds to invest in ICT security processes and systems (Marabelli et al., 2013).

5.2.7 Theme 7: User awareness

Sterlicchi (1996) states that most security breaches or threats originate from inside the organisation. Security breaches are usually associated with failures due to technical issues, vulnerabilities in the systems that do not get addressed, behavior of humans towards security, and fraud by various stakeholders (Silva et al., 2014). Organisations suffer major losses and have to pay huge fines due to system breaches, attacks, and poor procedure and policy process controls (O'Neill, 2014). Veiga and Martins (2015) explain that information security training is seen as one of the most effective ways for business to protect their information resources; then again, it is also true that many organisations do not have information security awareness programmes in place. From the research, it is evident that there is minimal awareness training on infrastructure security risks due to cost cuts (Table: 4.10: Finding 30). P9 said that training is “to a minimal extent; travel as [part of] the company is on cost cutting strategies, and travel for such a nature is cut, and it is not effective holding such awareness campaigns over a video conference” (Appendix B9, IQ 17). P1 stated that ICT security awareness training “is seen as money spent and a cost, so it is often not done from budget point of view as seen as money wasted. The people controlling the budgets do not understand the impact of these risks as many have never experienced one first hand” (Appendix B1, IQ 17). This creates a gap in terms of information security, as employees are still viewed as the largest contributors of information security incidents occurring in the organisation (Veiga & Martins, 2015). Veiga and Martins (2015) and Rocha Flores et al. (2014) suggest that when business develops information security policies, procedures and awareness programmes, it is important for the outsourcing business and ICT vendor to focus not only on controls in terms of technology and processes, but also include human elements such as norms, beliefs and attitudes, since end-users sometimes deal directly with ICT vendors, bypassing security controls (Table 4.10, Finding 40).

Although the ICT department does have ICT training programmes in place, it does not cover infrastructure security risks associated with ICT outsourcing (Table: 4.10, Finding 29). Venter (2014) points out that there is a lack of proper information security awareness training in businesses. The findings here support Venter (2014) to the same effect. If there is proper training, users would easily be able to identify

cyber or security issues. By implementing an information security awareness culture within the organisation, the organisation can reduce risks, especially information security risks to information resources (AlHogail, 2015). Tsohou et al. (2015) explain that users do not always adhere or comply with ICT security policies put in place and suggest that security awareness programmes be put in place to make them aware of the importance of ICT security and the management thereof.

5.2.8 Theme 8: Frameworks

According to Gulla and Gupta (2012:30), frameworks are “conceptual structures used to solve or address complex issues”. Frameworks can assist managers in understanding what to do, when to do, and how to do things when carrying out ICT outsourcing processes. Abu-Musa (2010) identifies a number of frameworks that organisations can implement to ensure best practice. Some of the frameworks include Control Objective for Information related Technology (COBIT), International Standardisation Organisation (ISO) 17799, and FIPS Production Publication 200. Bin-abbas and Haj (2014) also mention ISO 38500, the Massachusetts Institute of Technology (MIT) IT governance method and the ISO 2000 as frameworks that can be used. Other frameworks identified in literature are First Assessment Framework Analysis (FMEA) (Nassimbeni et al., 2012), a risk measurement outsourcing framework (Lee et al., 2012), FARM framework (Flexibility, Absorptive Capacity, Relationships and Monitoring) (Pratap, 2014), the conceptual framework of IT outsourcing (Lee et al., 2013), and ISO27005 (Wahlgren et al., 2013). The research of this study shows that the ICT the department uses ITIL, ISO 27001/2, and COBIT as frameworks to protect business against ICT infrastructure security threats when outsourcing ICT functions (Table 4.10, Finding 33). P10 stated that:

“Transnet has adopted the ISO 27001 as the information security framework. However, there is also a governance framework (minimum control framework), based on COBIT and ITIL, that is in place and covers certain information security controls. Transnet also mapped the gaps not covered in the Minimum control framework to ISO27001” (Appendix B10, IQ 20).

According to P4, the transport organisation “Transnet has a customised internal control framework for EIMS/ICT” (Appendix B4, IQ 20), based on ITIL and COBIT. The problem with these frameworks or documents are that it sometimes consist of complicated methods (Bin-abbas & Haj, 2014), for example, COBIT consists of 34 ICT processes, 222 control objectives, and more than 300 key performance indicators (KPI’s) (Khther & Othman, 2013). In order to use COBIT as an ICT governance support tool, business needs a great deal of knowledge of the

framework, meaning that the framework is not easy to understand and use (Zhang & Fever, 2013; Simonsson et al., 2007).

Even though the majority of participants are of the opinion that ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions (Table 4.10, Finding 34), it is found that controls in the ICT frameworks are not adequately enforced (Table 4.10, Finding 35). Everett (2011) states that IT can vary from months to years for an organisation to become fully compliant to a framework, and policies, procedures and controls need to be implemented and enforced throughout the organisation in order to be audited. P10 explained that ICT frameworks can provide certain controls to ensure that the ICT department manages and monitor risks associated with vendors effectively, however “if the control is not enforced, it will not operate adequately” (Appendix B10, IQ 21).. According to Bin-abbas and Haj (2014), frameworks and methods can help organisations to measure information security performances, assess security risks, and develop security controls that are appropriate for risks detected in the outsourcing process. For organisations to manage security they need a framework that enables business to think about information security at various levels and not only at a technical level (Moreira et al., 2008). It is important for businesses to realise that information security controls have an impact on how employees view information, systems, and processes (Veiga & Martins, 2015).

Samantra et al. (2014) state that limited attempts have been made to create an approach for assessing, managing, and analysing risks for best practice when outsourcing ICT. The author therefore, proposes guidelines based on COBIT, ISO 27001, ITIL, the FMEA, and the risk measurement outsourcing framework. From the three frameworks (COBIT, ISO 27001, ITIL) used by the case organisation, a number of shortcomings have been identified to solve the phenomena, including lack of adequate enforcement, effectiveness of frameworks, lack of implementation, complications of frameworks and gaps identified in Chapter 2 (Table 2.1).

5.3 The proposed guidelines

The guidelines consist of components that could assist the outsourcing business (section 2.1.1) to solve the phenomena under investigation. The components of the guidelines are i) systems and network, ii) access, iii) users, iv) training, v) control and vi) reporting. These components are discussed below.

i) Systems and network components

- All systems and network changes must be approved by the outsourcing business and must include at least one person of the outsourcing business who reports back to Group or the Operating division at the beginning, during, and after any change
- In order to minimise information risks, risk assessments must be done on a daily basis on the network and systems; not on an *ad hoc* basis or per project
- The outsourcing business in conjunction with the ICT vendor must develop procedures to deal with infrastructure risks that could occur during and after the outsourcing agreements
- The outsourcing business needs to have a proper plan that indicates the cost and benefits of implementing risk management for systems and networks as well as the impact of information risks on the operating divisions when outsourcing ICT
- A procedure for risk management enforcement needs to be implemented by all stakeholders

ii) Access components

- Access restriction must be specific at all times
- The outsourcing business must implement formal procedures on how access levels for systems and networks need be granted
- All access requests must be approved by the Operating division, an ICT representative, and the ICT vendor
- Key suppliers should be audited without prior notice to ensure that they adhere to the security requirements as set out in the SLAs

iii) User components

- All administrator user requests must be approved or signed off by the ICT manager and the operating division ICT headquarters representative
- ICT vendor user accounts must be monitored (check when they log onto systems or network)
- ICT related request must go through the ICT departments and not directly to ICT vendors
- Inform users of various ICT risks, especially information security and infrastructure security risks

iv) Training components

- Implement methods and train employees to determine the impact of information risks when outsourcing ICT functions
- Provide training on what ICT functions are outsourced and why it is outsourced, focusing on ICT departments
- Train users on various ICT frameworks used in organisations (COBIT, ISO) and the importance thereof

v) Control components

- All ICT environments must have structured risk assessments that should be on going and not terminate when a project is completed
- All illegal activities or compliance issues must be addressed immediately if picked up
- Implement methods or procedures to measure security success rates of ICT vendors
- Security services managed by external parties must be audited by external auditors as well as the outsourcing business ICT security team
- Sub-contractors that need access to the systems or business must work through the primary vendor and not directly with clients
- All sub-contractors must adhere to the same rules set out in SLAs for primary contractors
- Primary ICT vendors are responsible for enforcing sub-contractors to adhere to ICT security requirements
- Appoint risk management officers on division level for implementation of ICT frameworks (COBIT, ISO, SLA) and ensure that it is enforced
- All ICT operating divisions including ICT personnel and ICT managers must be responsible for ICT security, and not the Group function
- Although key suppliers have full access to the system and host the core systems, the outsourcing business must have contingency procedures in place if anything goes wrong; this however needs further research
- if ICT vendors do not adhere to SLAs, Implement penalties that are affective
- Develop a proper exit strategy if problems occur

vi) Reporting components

- Reports on illegal activities on a daily, weekly, and monthly basis
- Reports on user creation on a daily basis
- Reports on change management before and after completion

- Reports on competent ICT security users
- Reports on risk assessments performed

By adopting and enforcing the guidelines mentioned above, the outsourcing business will be able to manage and solve the phenomena under investigation.

5.4 Answering the research questions

Research Question 1: What information risks does the ICT department manage when outsourcing ICT projects?

Information risk management is seen as extremely important by all participants. From the research, several information risks were identified that the ICT department must manage when outsourcing ICT projects. Identified risks include unauthorised access and hacking, preventing the disclosure of confidential information to third parties, and ICT vendors that are not complying with information security and requirements. These information risks are related to the vendor access management processes, information risk management processes, ICT infrastructure security processes, and at the end-user level of the organisation. Results of the research shows that exploiting or disclosure of confidential information to third parties is seen the highest information risk when outsourcing ICT.

The information risks mentioned above are managed through audits, *ad hoc* security assessments, SLAs, access controls, firewalls, installation of anti-viruses, and as user awareness campaigns. Even though the majority participants are familiar with methods in place to reduce and manage information and ICT infrastructure security risks, the research proves that the outsourcing business does not have mechanisms in place to deal with the risks of infrastructure outsourcing. Furthermore, several participants are not aware of methods used to determine the impact of information risks when outsourcing ICT projects. This could be attributed to core systems of the outsourcing business being hosted by ICT vendors.

Research Question 2: How can the ICT department protect their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT?

From the research it is evident that the majority of participants are of the opinion that ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions; however, it is also found that controls in the ICT frameworks are not always adequately enforced.

Adding to this shortcoming are effectiveness of controls and lack of implementation due to complicated frameworks (Chapter 2).

Three frameworks (COBIT, ISO 27001, ITIL) are currently used by the outsourcing businesses. Based on the three frameworks as well as the FMEA and the Risk Measurement Outsourcing Framework, the author proposes guidelines consisting of various components that could assist the outsourcing business in protecting their information through infrastructure risk management against ICT security threats when outsourcing ICT. The components of the guidelines are composed of i) systems and network, ii) access, iii) users, iv) training, v) control, and vi) reporting as described above.

5.5 The aim

The aim of this study is to explore how the organisation can manage information risks through the usage of infrastructure risk management when outsourcing ICT projects.

Information risks or gaps that need to be addressed when outsourcing ICT projects have been identified. From the research conducted, guidelines consisting of components are proposed to assist the outsourcing business in the management of information risks through the usage of infrastructure risk management when outsourcing ICT projects.

However, various areas in the ICT outsourcing process still exist that need further research to ensure that business properly manage information risks through the usage of infrastructure risk management when outsourcing ICT projects. These areas include human behavior towards ICT security as well as proper methods to enforce the proposed guidelines.

5.6 Conclusion

Chapter 5 discussed the themes identified in Chapter 4 and elaborated on how each theme is linked to the research questions and aim of the study. The author proposed guidelines to assist business with the phenomena under investigation. The proposed guidelines are based on the three frameworks used by the outsourcing business (COBIT, ISO 27001, ITIL) as well as the FMEA and Risk Measurement Outsourcing Framework. The guidelines are sub-divided into six primary components identified as systems and network, access, users, training, control, and reporting.

In Chapter 5, the author focused on each component individually to provide a broader overview of what the outsourcing business should consider to ensure that information risks are managed through infrastructure risk management when outsourcing ICT projects.

In order to address the research problem, two main research questions were developed: Firstly, what information risks does the ICT department manage when outsourcing ICT projects, and secondly, how can the ICT department protect their information through the usage of infrastructure risk management against ICT security threats when outsourcing ICT?

At the end of the chapter, both research questions are answered and the aim of the research is addressed. The proposed guidelines can assist business in addressing the phenomena under investigation by adopting and enforcing the guidelines properly.

The following chapter (6) discusses the recommendations, reflections, and contributions of the research.

CHAPTER 6: RECOMMENDATIONS, REFLECTION AND CONTRIBUTIONS

In Chapter 6, recommendations are proposed, followed by a reflection on the research conducted. The chapter discusses the contributions towards i) research, ii) Information Technology, and iii) law and compliance. The chapter ends with research limitations experienced during the research and a conclusion.

6.1 Recommendations

The results of the research point to various gaps to be addressed in the outsourcing business to ensure that information is protected when outsourcing ICT projects. In order to resolve these gaps/breaches, it is recommended that measures are put in place and communication is improved among operating divisions.

Firstly, key ICT vendors/suppliers as well as any other ICT vendor need to be monitored constantly to ensure their adherence or compliance with ICT security as stipulated by the outsourcing business. By doing this, the outsourcing business will be able to review illegal activities immediately as it occurs, act on it, and be able to measure the security success rate of ICT vendors.

Secondly, business needs to conduct risk assessment regularly, not on an *ad hoc* basis. For example, risks associated with vendor access management processes need to be looked at in more detail, and the outsourcing business must constantly try to find ways to improve the access management process. These improvement processes should not only be applicable to primary vendors but also to sub-contractors who have to adhere to the same rules as the primary vendors.

In literature, it is found that most security threats originate from within the organisation, and from the findings it is clear that end-users dealing directly with ICT vendors create threats by bypassing security controls. Therefore, it is recommended that users be made aware of ICT security risks, especially with outsourcing projects and the implications it could have on them and the organisation. This could be done in the form of user awareness programmes or ICT security games that could ensure that all employees participate. It is also important that a culture is created by business in which employees understand that ICT security is not only the responsibility of ICT professionals, it starts with them as users. The author recommends that further research be conducted on the behavior of employees in terms of ICT security.

Lastly, it is recommended that measures are put in place to improve communication among operating divisions and the Group function, especially in terms of making divisions aware of various ICT security risks, how it should be handled, and budgets allocated to ICT security. By doing this, operating divisions will be able to address various ICT security risks appropriately and have knowledge on which steps to follow should any information security risk arise.

6.2 Reflection

The research followed a case study approach, limited to a specific transport organisation in South Africa. The research results are as accurate as possible and based on the interview answers from the 17 participants. It must be emphasised that the results cannot be generalised, as it is unique to the organisation.

Before and during the interviews various challenges were experienced, for example, interviewees were situated at ports across South Africa, and there were not sufficient time and funds to travel to all provinces. Secondly, interviewees were not always available for interviews; other arrangements such as after-hours Skype sessions had to be conducted. Although employees answered to the best of their knowledge, some of the interviewees declined answering certain questions, as they believed that confidential or sensitive information should be kept within the organisation despite the fact that the CEO granted permission for employees to answer.

The findings of the research open the doors to more questions that need to be answered, such as “how does business create an ICT security culture to ensure that information is protected at all times”, and “does vendor access management really get the necessary attention it requires?” Further study on human behaviour towards ICT security is needed to ensure that organisations are protected.

6.3 Contribution to research

Although there are several frameworks such as COBIT, ISO, and ITIL in literature (Chapter 2) that can be associated with ICT, none of these frameworks includes or references the managing of information risks through the usage of infrastructure risk management when outsourcing ICT projects. Therefore, the study introduced guidelines that could contribute to the management of information risks through the usage of infrastructure risk management when outsourcing ICT projects. By properly enforcing the guidelines, business might be in a better position to manage and reduce information risks when outsourcing ICT.

6.4 Contribution to Information Technology

Information is seen as one of the most important assets of the organisation, and therefore business needs to protect it at all cost. The research provides guidelines on how business can manage information risks through the usage of infrastructure risk management, especially focusing on vendor access management when outsourcing ICT projects.

The research identifies the importance of managing information security to ensure secured information. Employees are viewed as the major contributor of information security threats; it is therefore suggested that the human factor related to information security requires further research.

6.5 Contribution to law and compliance

It is evident that business does not always consider the importance of implementing methods to measure the ICT security success rate of ICT and putting controls in place. By implementing the proposed guidelines, business may be able to identify information risks to the system and at the same time ensure that vendors comply with the information security requirements of the outsourcing business. Further studies can assist the organisation to determine the importance and effect of information security compliance on the organisation.

By law, organisations are responsible for protecting their data; this includes customer data. The proposed guidelines could assist business in finding loopholes that have to be addressed so that the business can adhere to the specified laws. For example, proper vendor access management processes can ensure that business knows which data are accessible by third parties.

6.6 Limitations of research

A number of research limitations have been identified. The research findings are based on a specific transport company in South Africa, therefore the findings cannot be generalised to all transport organisations. Although the findings were obtained from the one organisation, the topic under investigation can be explored in other organisations to further knowledge.

Interviews were conducted with 17 participants, ranging from executives to ICT security professionals. All of the participants answered the questions to the best of their knowledge although the outcome could have differed if a different unit of analysis approach was applied.

Lastly, some questions were not properly answered by interviewees due to the sensitivity of the questions or participants who did not want to provide the answers, as they believed the information should be kept in-house.

The research identified a number of shortcomings in terms of outsourcing ICT functions, one of which is the human factor that can be regarded as a major contributor to information security risks. Although further studies on human behaviour towards ICT security is needed to ensure that organisations are protected, the proposed guidelines could assist with most of the findings identified in the research.

REFERENCES

- Abdel-Fattah, M.A. 2015. Grounded theory and action research as pillars for interpretive information systems research: a comparative study. *Egyptian Informatics Journal*, 16(3):309-327. <http://dx.doi.org/10.1016/j.eij.2015.07.002>.
- Abdullah, L.M. & Verner, J.M. 2012. Analysis and application of an outsourcing risk framework. *Journal of Systems and Software*, 85(8):1930-1952. <http://linkinghub.elsevier.com/retrieve/pii/S0164121212000647>. [Accessed: 20 March 2014].
- Abu-Musa, A. 2010. Information security governance in Saudi organisations: an empirical study. *Information Management & Computer Security*, 18(4):226-276. <http://www.emeraldinsight.com/10.1108/09685221011079180>. [Accessed: 17 March 2014].
- Albrechtsen, E. 2015. Major accident prevention and management of information systems security in technology-based work processes. *Journal of Loss Prevention in the Process Industries*, 36:84-91. <http://linkinghub.elsevier.com/retrieve/pii/S0950423015001254>. [Accessed: 23 July 2015].
- AlHogail, A. 2015. Design and validation of information security culture framework. *Computers in Human Behavior*, 49:567-575. <http://linkinghub.elsevier.com/retrieve/pii/S0747563215002447>. [Accessed: 23 July 2015].
- Ali, H. & Birley, S. 1999. Integrating deductive and inductive approaches in a study of new ventures and customer perceived risk. *Qualitative Market Research: An International Journal*, 2(2):103-110. <http://www.emeraldinsight.com/doi/abs/10.1108/13522759910270016>. [Accessed: 02 June 2016].
- Alramahi, N.M., Barakat, A.I. & Haddad, H. 2014. Information technology governance control level in Jordanian banks using: Control Objectives for Information and Related Technology (COBIT 5). *European Journal of Business and Management*, 6(5):194-206.
- Altinkemer, K., Chaturvedi, A. & Gulati, R. 1994. Information systems outsourcing: issues and evidence. *International Journal of Information Management*, 14(4):252-268.
- Aundhe, M.D. & Mathew, S.K. 2009. Risks in offshore IT outsourcing: a service provider perspective. *European Management Journal*, 27(6):418-428. <http://linkinghub.elsevier.com/retrieve/pii/S026323730900005X>. [Accessed: 2 March 2014].
- Ayogu, M.D. & Bayat, F. 2010. ICT governance: South Africa. *Telecommunications Policy*, 34(4):244-247. <http://dx.doi.org/10.1016/j.telpol.2008.12.009>.

- Bachlechner, D., Thalmann, S. & Maier, R. 2014. Security and compliance challenges in complex IT outsourcing arrangements: a multi-stakeholder perspective. *Computers & Security*, 40:38-59. <http://linkinghub.elsevier.com/retrieve/pii/S0167404813001533>. [Accessed: 14 March 2014].
- Badenhorst, M. 2009. *Governance as a quality paradigm*. Master's Dissertation. Cape Peninsula University of Technology.
- Bahl, S. & Wali, O.P. 2013. An empirical analysis of perceived significance of information security service quality to predict the organisational performance in software service industry. *CSI Transactions on ICT*, 1(3):221-230. [Http://link.springer.com/10.1007/s40012-013-0020-6](http://link.springer.com/10.1007/s40012-013-0020-6). [Accessed: 11 March 2014].
- Bahl, S. & Wali, O.P. 2014. Perceived significance of information security governance to predict the information security service quality in software service industry: an empirical analysis. *Information Management & Computer Security*, 22(1):2-23. <http://www.emeraldinsight.com/10.1108/IMCS-01-2013-0002>. [Accessed: 14 March 2014].
- Bahli, B. & Rivard, S. 2013. Cost escalation in information technology outsourcing: a moderated mediation study. *Decision Support Systems*, 56(1):37-47. <http://dx.doi.org/10.1016/j.dss.2013.04.007>.
- Barham, C. 2014. Confidentiality and security of information. *Anaesthesia and Intensive Care Medicine*, 15(1):46-48. <http://dx.doi.org/10.1016/j.mpaic.2013.11.001>.
- Baxter, P. & Jack, S. 2008. Qualitative case study methodology: study design and implementation for novice researchers. *The Qualitative Report*, 13(4):544-559. December.
- Bayrak, T. 2013. A decision framework for SME Information Technology (IT) managers: factors for evaluating whether to outsource internal applications to application service providers. *Technology in Society*, 35(1):14-21. <http://dx.doi.org/10.1016/j.techsoc.2012.11.001>.
- Bengtsson, M. 2016. How to plan and perform a qualitative study using content analysis. *Nursing Plus Open*, 2:8-14. <http://dx.doi.org/10.1016/j.npls.2016.01.001>.
- Bin-abbas, H. & Haj, S. 2014. Assessment of IT governance in organisations: a simple integrated approach. *Computers in Human Behavior*, 32:261-267. <http://dx.doi.org/10.1016/j.chb.2013.12.019>.
- Blazent. 2010. *IT outsourcing's 15% problem: the need for outsourcing governance*. San Mateo, CA. <http://itonews.eu/files/f1289402535.pdf>. [Accessed: 11 March 2014].
- Borghoff, T. 2014. International Supply Chain Management (ISCM): an emergent perspective on internationalisation driven by Information and Communications Technology (ICT). *Journal of Modern Accounting and Auditing*, 10(1):116-124.
- Bryman, A. & Bell, E. 2015. *Business research methods*. 4th ed. Oxford University Press.

- Ceazer, A., Cavusogly, H. & Srinivasan, R. 2010. Outsourcing information security: contracting issues and security implications. *In Workshop on the Economics of Information Security (WEIS)*, Harvard University, Cambridge, MA: 1-52. May.
- Chakravarty, A., Grewal, R., Sarker, S. & Sambamurthy, V. 2014. Choice of geographical location as governance strategy in outsourcing contracts: localized outsourcing, global outsourcing, and onshore outsourcing. *Customer Needs and Solutions*, 1(1):11-22. <http://link.springer.com/10.1007/s40547-013-0004-6>. [Accessed: 11 March 2014].
- Chandrasekaran, B., Josephson, J.R. & Benjamins, V.R. 1999. What are ontologies, and why do we need them? *IEEE Intelligent Systems*, 14(1):20-26. <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=747902>. [Accessed: 02 June 2014].
- Chatzipoulidis. 2015. Information infrastructure risk prediction through platform vulnerability analysis. *The Journal of Systems & Software*, 106:28-41. <http://dx.doi.org/10.1016/j.jss.2015.04.062>.
- Cheng, Y. 2012. Information security risk assessment model of it outsourcing managed service. *In 12th International Conference on Management of e-Commerce and e-Government Information*. Beijing, China: 116-121.
- Chou, D.C. & Chou, A.Y. 2009. Information systems outsourcing life cycle and risks analysis. *Computer Standards and Interfaces*, 31(5):1036-1043. <http://dx.doi.org/10.1016/j.csi.2008.09.032>.
- Coertze, J. & Von Solms, R. 2013a. A software gateway to affordable and effective information security governance in SMMEs. Port Elizabeth, South Africa: IEEE.
- Coertze, J. & Von Solms, R. 2013b. The Board and IT governance: a replicative study. *African Journal of Business Management*, 7(35):3358-3373.
- Compton, B.W. 2013. Ontology in information studies: without, within, and withal knowledge management. *Journal of Documentation*, 70(3):6. <http://www.emeraldinsight.com/journals.htm?issn=0022-0418&volume=70&issue=3&articleid=17101493&show=html>. [Accessed: 2 June 2016].
- Crow, G. & Muthuswamy, B. 2003. International outsourcing in the information technology industry: trends and implications. *Communications of the IIMA*, 3(1):25-34.
- Daniel, J. 2011. *Sampling essentials - practical guidelines for making sampling choices* (Paperback). United States: Sage.
- Da Veiga, A. & Eloff, J.H.P. 2010. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196-207. <http://dx.doi.org/10.1016/j.cose.2009.09.002>.
- Dellis, A., Skolarikos, A. & Papatsoris, A.G. 2014. Why should i do research? Is it a waste of time? *Arab Journal of Urology*, 12(1):68-70. <http://dx.doi.org/10.1016/j.aju.2013.08.007>.

- Deng, C.P., Mao, J.Y. & Wang, G.S. 2013. An empirical study on the source of vendors' relational performance in offshore information systems outsourcing. *International Journal of Information Management*, 33(1):10-9. <http://dx.doi.org/10.1016/j.ijinfomgt.2012.04.004>.
- Duhamel, F., Gutierrez-Martinez, I., Picazo-Vela, S. & Luna-Reyes, L.F. 2014. IT outsourcing in the public sector: a conceptual model. *Transforming Government: People, Process and Policy*, 8(1):8-27. <http://www.emeraldinsight.com/10.1108/TG-05-2013-0012>. [Accessed: 21 July 2015].
- Elitzur, R., Gavious, A. & Wensley, A.K.P. 2012. Information systems outsourcing projects as a double moral hazard problem. *Omega*, 40(3):379-389. <http://linkinghub.elsevier.com/retrieve/pii/S0305048311001009>. [Accessed: 20 March 2014].
- Everett, C. 2011. Is ISO 27001 worth it? *Computer Fraud and Security*, (1):5-7.
- Feng, N., Wang, H.J. & Li, M. 2014. A security risk analysis model for information systems: causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences*, 256:57-73. <http://dx.doi.org/10.1016/j.ins.2013.02.036>.
- Fink, D. 1994. A security framework for information systems outsourcing. *Information Management & Computer Security*, 2(4):3-8.
- Fink, L. 2010. Information technology outsourcing through a configurational lens. *Journal of Strategic Information Systems*, 19(2):124-141. <http://dx.doi.org/10.1016/j.jsis.2010.05.004>.
- Fletcher, D., Massis, A. De & Nordqvist, M. 2016. Qualitative research practices and family business scholarship: a review and future research agenda. *Journal of Family Business Strategy*, 7(1):8-25. <http://dx.doi.org/10.1016/j.jfbs.2015.08.001>.
- George, B., Hirschheim, R. & Von Stetten, A. 2014. Through the lens of social capital: a research agenda for studying IT outsourcing. *Strategic Outsourcing: An International Journal*, 7(2):107-134. <http://www.emeraldinsight.com/doi/full/10.1108/SO-12-2013-0025>. [Accessed: 23 July 2015].
- Gerring, J. 2007. *Case study research: principles and practices*. Cambridge University Press.
- Ghosh, S., Boswell, J.W., Kwak, Y.H. & Skibniewski, M.J. 2011. Risk governance framework for enterprise-wide application implementations. *In Technology Management Conference (ITMC), IEEE International*: 932-938.
- Gonzalez, R., Gasco, J.L. & Llopis, J. 2013. Information systems offshore outsourcing: managerial conclusions from academic research. *International Entrepreneurship and Management Journal*, 9(2):229-259.
- Gonzalez, R., Gasco, J.L. & Llopis, J. 2015. Information systems outsourcing satisfaction: some explanatory factors. *Industrial Management & Data Systems*, 115(6):1067-1085.

- Górniak-Kocikowska, K. 2008. ICT and the tension between old and new: the human factor. *Journal of Information, Communication and Ethics in Society*, 6(1):4-27.
- Gulla, U. & Gupta, M.P. 2012. Deciding the level of information systems outsourcing: proposing a framework and validation with three Indian banks. *Journal of Enterprise Information Management*, 25(1):28-59. <http://www.emeraldinsight.com/10.1108/17410391211192152>. [Accessed: 13 March 2014].
- Hamlen, K.W. & Thuraisingham, B. 2013. Data security services, solutions and standards for outsourcing. *Computer Standards & Interfaces*, 35(1):1-5. <http://linkinghub.elsevier.com/retrieve/pii/S0920548912000414>. [Accessed: 21 February 2014].
- Harness, T. 2009. Research methods for the empirical study of strategic human resource management. *Qualitative Market Research: An International Journal*, 12(3):321-336.
- Herath, T. & Kishore, R. 2009. Offshore outsourcing: risks, challenges, and potential solutions. *Information Systems Management*, 26(4):312-326. <http://www.tandfonline.com/doi/abs/10.1080/10580530903245549>. [Accessed: 3 March 2014].
- Humphreys, E. 2008. Information security management standards: compliance, governance and risk management. *Information Security Technical Report*, 13(4):247-255. <http://dx.doi.org/10.1016/j.istr.2008.10.010>.
- Hyland, K. 2016. Methods and methodologies in second language writing research. *System*, 59:116-125. <http://linkinghub.elsevier.com/retrieve/pii/S0346251X16300252>. [Accessed: 02 June 2016].
- Juiz, C., Guerrero, C. & Lera, I. 2014. Implementing good governance principles for the public sector in information technology governance frameworks. *Open Journal of Accounting*, 3(January):9-27. <http://dx.doi.org/10.4236/ojacct.2014.31003>.
- Kang, M., Wu, X., Hong, P., Park, K. & Park, Y. 2014. The role of organisational control in outsourcing practices: an empirical study. *Journal of Purchasing and Supply Management*, 20(3):177-185. <http://dx.doi.org/10.1016/j.pursup.2014.02.002>.
- Karlsson, F., Kolkowska, E. & Prenkert, F. 2016. Inter-organisational information security: a systematic literature review. *Information & Computer Security*, 24(5):418-451.
- Karyda, M., Mitrou, E. & Quirchmayr, G. 2006. A framework for outsourcing IS/IT security services. *Information Management & Computer Security*, 14(5):402-415.
- Khaikleng, P., Wongwanich, S. & Sujiva, S. 2014. Development of a program theory for evaluating the success of education reform policy implementation in schools by using inductive and deductive approaches. *Procedia - Social and Behavioral Sciences*, 116:1389-1393. <http://www.sciencedirect.com/science/article/pii/S1877042814004200>. [Accessed: 2 June 2016].

- Khidzir, N.Z., Mohamed, A. & Arshad, N.H. 2013a. ICT outsourcing information security risk factors: an exploratory analysis of threat risks factor for critical project characteristics. *Journal of Industrial and Intelligent Information*, 1(4):218-222. <http://www.jiii.org/index.php?m=content&c=index&a=show&catid=36&id=65>. [Accessed: 3 March 2014].
- Khidzir, N.Z., Mohamed, A. & Arshad, N.H. 2013b. Information security requirement: the relationship between information asset integrity and availability for ICT outsourcing. *Lecture Notes on Information Theory*, 1(3):118-123. <http://www.lnit.org/index.php?m=content&c=index&a=show&catid=32&id=41>. [Accessed: 3 March 2014].
- Khther, R.A. & Othman, M. 2013. COBIT Framework as a guideline of effective IT governance in higher education: a review. *International Journal of Information Technology Convergence and Services*, 3(1):21-29. <http://www.airccse.org/journal/ijitcs/papers/3113ijitcs02.pdf>. [Accessed: 30 July 2014].
- Kilubi, I. 2015. Strategic technology partnering: a framework extension. *The Journal of High Technology Management Research*, 26(1):27-37. <http://linkinghub.elsevier.com/retrieve/pii/S1047831015000048>. [Accessed: 23 July 2015].
- Kite, G. 2012. The impact of information technology outsourcing on productivity and output: new evidence from India. *Procedia Economics and Finance*, 1(12):239-248. [http://dx.doi.org/10.1016/S2212-5671\(12\)00028-7](http://dx.doi.org/10.1016/S2212-5671(12)00028-7).
- Knipe, S. & Bottrell, C. 2015. JARA Schedule: a tool for understanding research methodology. *Journal of Multidisciplinary Research*, 7(2):17-30.
- Kumar, S., Sharma, R.K. & Chauhan, P. 2014. ISM approach to model offshore outsourcing risks. *International Journal of Production Management and Engineering*, 2(2012):101-111.
- Kutsikos, K. & Sakas, D. 2014. A framework for enabling service configuration decisions: the case of it outsourcing providers. *Procedia - Social and Behavioral Sciences*, 148:604-610. <http://linkinghub.elsevier.com/retrieve/pii/S1877042814039901>. [Accessed: 23 July 2015].
- Lacity, M.C., Willcocks, L.P. & Khan, S. 2011. Beyond transaction cost economics: towards an endogenous theory of information technology outsourcing. *Journal of Strategic Information Systems*, 20(2):139-157. <http://dx.doi.org/10.1016/j.jsis.2011.04.002>.
- Laudel, G. & Glaser, J. 2014. Beyond breakthrough research: epistemic properties of research and their consequences for research funding. *Research Policy*, 43(7):1204-1216. <http://dx.doi.org/10.1016/j.respol.2014.02.006>.
- Lee, C.K.M., Yeung, Y.C. & Hong, Z. 2012. An integrated framework for outsourcing risk management. *Industrial Management & Data Systems*, 112(4):541-558.

- Lee, T., Lim, Y. & Yap, C. 2013. Explaining IT outsourcing satisfaction using Domberger's Theory. *Gadjah Mada International Journal of Business*, 15(1):45-60.
- Lee, V. & Lo, A. 2013. From theory to practice: teaching management using films through deductive and inductive processes. *International Journal of Management Education*, 12(1):44-54. <http://dx.doi.org/10.1016/j.ijme.2013.05.001>.
- Leszczyna, R. 2013. Cost assessment of computer security activities. *Computer Fraud and Security*, 2013(7):11-16. [http://dx.doi.org/10.1016/S1361-3723\(13\)70063-0](http://dx.doi.org/10.1016/S1361-3723(13)70063-0).
- Li, D. & Wan, S. 2014. Knowledge-Based Systems: a fuzzy inhomogeneous multi-attribute group decision making approach to solve outsourcing provider selection problems. *Knowledge-Based Systems*, 67:71-89. <http://dx.doi.org/10.1016/j.knosys.2014.06.006>.
- Liu, S. & Wang, L. 2014. Understanding the impact of risks on performance in internal and outsourced information technology projects: the role of strategic importance. *International Journal of Project Management*, 32(8):1494-1510. <http://linkinghub.elsevier.com/retrieve/pii/S0263786314000131>. [Accessed: 28 February 2014].
- Luft, J. & Shields, M.D. 2014. Subjectivity in developing and validating causal explanations in positivist accounting research. *Accounting, Organisations and Society*, 39(7):550-558. <http://dx.doi.org/10.1016/j.aos.2013.09.001>.
- MacDermid, J.C. 2015. The research process from ideas to implementation. *Journal of Hand Therapy*, 28(4):339-340. <http://linkinghub.elsevier.com/retrieve/pii/S0894113015001398>. [Accessed: 2 June 2016].
- Majid, N., Ahmad, R.R., Din, U.K.S., Rambely, A.S., Suradi, N.R.M. & Shahabudin, F.A.A. 2012. Academic research process: a review on current practices in School of Mathematical Sciences. *Procedia - Social and Behavioral Sciences*, 59(0):394-398. <http://www.sciencedirect.com/science/article/pii/S1877042812037408>. [Accessed: 2 June 2016].
- Mangalaraj, G., Singh, A. & Taneja, A. 2014. IT governance frameworks and COBIT - a literature review. *In Twentieth Americas Conference on Information Systems*, Savannah, Georgia: 1-10.
- Mann, A., Folch, D.C., Kauffman, R.J. & Anselin, L. 2015. Spatial and temporal trends in information technology outsourcing. *Applied Geography*, 63:192-203. <http://linkinghub.elsevier.com/retrieve/pii/S0143622815001629>. [Accessed: 21 July 2015].
- Marabelli, M., Newell, S. & Zang, Y. 2013. Managing the outsourcing of information security processes: the 'Cloud' solution. *Parallel & Cloud Computing*, 2(1):24-31.
- Martinsons, M. 1993. Outsourcing information systems: a strategic partnership with risks. *Long Range Planning*, 26(3):18-25. <http://linkinghub.elsevier.com/retrieve/pii/002463019390003X>. [Accessed: 21 July 2015].

- Mataracioglu, T. & Ozkan, S. 2011. Governing information security in conjunction with COBIT and ISO 27001. *International Journal of Information Technology and Computer Science*, 3(3):1-5.
- Mazza, T., Azzali, S. & Fornaciari, L. 2014. Audit quality of outsourced information technology controls. *Managerial Auditing Journal*, 29(9):837-862.
- Mclvor, R. 2000. A practical framework for understanding the outsourcing process. *Supply Chain Management: An International Journal*, 5(1):22-36.
- Mesquida, A.L. & Mas, A. 2014. Integrating IT service management requirements into the organisational management system. *Computer Standards and Interfaces*, 37:80-91. <http://dx.doi.org/10.1016/j.csi.2014.06.005>.
- Misuraca, G., Broster, D. & Centeno, C. 2012. Digital Europe 2030: designing scenarios for ICT in future governance and policy making. *Government Information Quarterly*, 29:S121–S131. <http://dx.doi.org/10.1016/j.giq.2011.08.006>.
- Mkansi, M. & Acheampong, E.A. 2012. Research philosophy debates and classifications: students' dilemma. *Electronic Journal of Business Research Methods*, 10(2):132-140.
- Mohammad, S. & Jafari, E. 2014. Strategic cost-cutting in information technology : toward a framework for enhancing the business value of IT. *Iranian Journal of Management Studies (IJMS)*, 7(1):21-39.
- Montesdioca, G.P.Z. & Maçada, A.C.G. 2015. Measuring user satisfaction with information security practices. *Computers & Security*, 48:267-280. <http://linkinghub.elsevier.com/retrieve/pii/S0167404814001618>. [Accessed: 23 July 2015].
- Moreira, E.D.S., Martimiano, L.A.F., Brandão, A.J.D.S. & Bernardes, M.C. 2008. Ontologies for information security management and governance. *Information Management & Computer Security*, 16(2):150-165.
- Morgan, P.K. 2014. Information literacy learning as epistemological process. *Reference Services Review*, 42(3):403.
- Mubarak, S. 2016. Developing a theory-based information security management framework for human service organisations. *Journal of Information, Communication and Ethics in Society*, 14(3):254-271.
- Munteanu, A.-B. & Fotache, D. 2015. Enablers of information security culture. *Procedia Economics and Finance*, 20(15):414-422. <http://linkinghub.elsevier.com/retrieve/pii/S221256711500091X>. [Accessed: 23 July 2015].
- Murthy, D.N.P., Karim, M.R. & Ahmadi, A. 2015. Data management in maintenance outsourcing. *Reliability Engineering & System Safety*, 142:100-110. <http://linkinghub.elsevier.com/retrieve/pii/S095183201500143X>. [Accessed: 23 July 2015].

- Myers, M.D. 2013. *Qualitative research in business and management*. Sage.
- Narasimhaiah, A. & Somers, T.M. 2014. Impact of IT outsourcing on information systems success. *Information & Management*, 1-50.
<http://linkinghub.elsevier.com/retrieve/pii/S0378720614000020>. [Accessed: 13 February 2014].
- Narasimhaiah, G. & Chiravuri, A. 2011. Information systems outsourcing success: a review. *2010 International Conference on E-business, Management and Economics (IPEDR)*, 3(2011):170-174 Hong Kong: IACSIT Press.
- Nassimbeni, G., Sartor, M. & Dus, D. 2012. Security risks in service offshoring and outsourcing. *Industrial Management & Data Systems*, 112(3):405-440.
<http://www.emeraldinsight.com/10.1108/02635571211210059>. [Accessed: 24 February 2014].
- Nazareth, D.L. & Choi, J. 2015. A system dynamics model for information security management. *Information & Management*, 52(1):123-134.
<http://linkinghub.elsevier.com/retrieve/pii/S0378720614001335>. [Accessed: 23 July 2015].
- Neuman, L.W. 2010. *Social research methods: qualitative and quantitative approaches*. 7th ed. USA: Pearson.
- Nunes-Vaz, R. & Lord, S. 2013. Designing physical security for complex infrastructures. *International Journal of Critical Infrastructure Protection*, 7(3):178-192.
<http://dx.doi.org/10.1016/j.ijcip.2014.06.003>.
- O'Neill, A. 2014. An action framework for compliance and governance. *Clinical Governance: An International Journal*, 19(4):342-359.
<http://www.emeraldinsight.com/doi/abs/10.1108/CGIJ-07-2014-0022>. [Accessed: 23 July 2015].
- Obalola, M. & Adelopo, I. 2012. Measuring the perceived importance of ethics and social responsibility in financial services: a narrative-inductive approach. *Social Responsibility Journal*, 8(3):418-432. <http://www.emeraldinsight.com/10.1108/17471111211247992>. [Accessed: 02 June 2016].
- Onyeji, I., Bazilian, M. & Bronk, C. 2014. Cyber security and critical energy infrastructure. *Electricity Journal*, 27(2):52-60. <http://dx.doi.org/10.1016/j.tej.2014.01.011>.
- Organ, J. & Stapleton, L. 2013. *Information systems risk paradigms: towards a new theory on systems risk*. IFAC. <http://linkinghub.elsevier.com/retrieve/pii/S1474667016342240>. [Accessed: 02 June 2016].
- Patil, S. & Wongsurawat, W. 2015. Information technology (IT) outsourcing by business process outsourcing/information technology enabled services (BPO/ITES) firms in India: a strategic gamble. *Journal of Enterprise Information Management*, 28(1):60-76.

- Pawlak, J., Polak, J.W. & Sivakumar, A. 2014. Towards a microeconomic framework for modelling the joint choice of activity-travel behaviour and ICT use. *Transportation Research Part A: Policy and Practice*, 76:92-112. <http://linkinghub.elsevier.com/retrieve/pii/S096585641400247X>. [Accessed: 23 July 2015].
- Petri, I., Rana, O.F., Regzui, Y. & Silaghi, G.C. 2012. Risk assessment in service provider communities. *Future Generation Computer Systems*, 41:32-43. http://dx.doi.org/10.1007/978-3-642-28675-9_10.
- Phelan, S. 2011. Case study research: design and methods. *Evaluation & Research in Education*, 24(3):221-222. https://books.google.co.za/books?hl=en&lr=&id=OgyqBAAQBAJ&oi=fnd&pg=PT243&dq=types+of+research+design&ots=FaJ6maj82l&sig=laNhsmxAq2x0AGx7msDTdcbhT_0\http://www.tandfonline.com/doi/abs/10.1080/09500790.2011.582317. [Accessed: 25 May 2016].
- Pratap, S. 2014. Towards a framework for performing outsourcing capability. *Strategic Outsourcing: An International Journal*, 7(3):226-252. <http://www.emeraldinsight.com/doi/abs/10.1108/SO-04-2014-0004>. [Accessed: 21 July 2015].
- Qi, L., Qingling, D., Wei, S. & Zhu, J. 2012. Modeling of risk treatment measurement model under four clusters standards (ISO 9001, 14001, 27001, OHSAS 18001). *Procedia Engineering*, 37:354-358. <http://dx.doi.org/10.1016/j.proeng.2012.04.252>.
- Rastogi, R. & Von Solms, R. 2012. Information security service culture – information security for end-users. *Journal of Universal Computer Science*, 18(12):1628-1642.
- Resnik, D.B. 2011. What is ethics in research & why is it important? *National Institute of Environmental Health Sciences*, 1-10. <http://www.niehs.nih.gov/research/resources/bioethics/whatis/>. [Accessed: 9 May 2014].
- Resnik, D.B. 2015. What is ethics in research & why is it important? *National Institute of Environmental Health Sciences*, 1-10. <http://www.niehs.nih.gov/research/resources/bioethics/whatis/>. [Accessed: 2 June 2016].
- Rocha Flores, W., Antonsen, E. & Ekstedt, M. 2014. Information security knowledge sharing in organisations: investigating the effect of behavioral information security governance and national culture. *Computers and Security*, 43:90-110. <http://dx.doi.org/10.1016/j.cose.2014.03.004>.
- Saetang, S. & Haider, A. 2014. IT governance, risk management and value delivery in construction organisations: literature review analysis. *Proceedings. The 17th International Symposium on Advancement of Construction Management and Real Estate*, Berlin Heidelberg. Springer: 935-942. <http://link.springer.com/10.1007/978-3-642-35548-6>. [Accessed: 20 March 2014].

- Safari, M.R. & Yu, L.Z. 2014. Impact of information and communication technology (ICT) on efficiency: evidence from the Iranian banking industry. *World Applied Sciences Journal*, 29(2):208-218.
- Saito, A., Umemoto, K. & Ikeda, M. 2007. A strategy-based ontology of knowledge management technologies. *Journal of Knowledge Management*, 11(1):97-114. <http://www.emeraldinsight.com/doi/abs/10.1108/13673270710728268>. [Accessed: 2 June 2016].
- Samantra, C., Datta, S. & Mahapatra, S.S. 2014. Risk assessment in IT outsourcing using fuzzy decision-making approach: an Indian perspective. *Expert Systems with Applications*, 41(8):4010-4022. <http://linkinghub.elsevier.com/retrieve/pii/S0957417413009998>. [Accessed: 28 February 2014].
- Sá-soares, F. De, Soares, D. & Arnaud, J. 2014. Towards a theory of information systems outsourcing risk. *Procedia Technology*, 16:623-637. <http://dx.doi.org/10.1016/j.protcy.2014.10.011>.
- Saunders, M.N.K. & Bezzina, F. 2015. Reflections on conceptions of research methodology among management academics. *European Management Journal*, 33(5):297-304. <http://dx.doi.org/10.1016/j.emj.2015.06.002>.
- Schenkl, S.A., Sauer, R.M. & Mörtl, M. 2014. A technology-centered framework for product-service systems. *Procedia CIRP*, 16:295-300. <http://dx.doi.org/10.1016/j.procir.2014.01.029>.
- Schmidt, N., Müller, M. & Rosenkranz, C. 2015. Identifying the giants: a social network analysis of the literature on information technology outsourcing relationships. In *Twenty-Third European Conference on Information Systems (ECIS)*, Germany: 0-17.
- Schware, R. 2013. Information and communications technology (ICT) agencies: functions, structures, and best operational practices. *Info*, 5(3):3-7.
- Schwarz, C. 2014. Toward an understanding of the nature and conceptualisation of outsourcing success. *Information and Management*, 51(1):152-164. <http://dx.doi.org/10.1016/j.im.2013.11.005>.
- Shaikh, A.A. & Karjaluoto, H. 2015. Making the most of information technology & systems usage: a literature review, framework and future research agenda. *Computers in Human Behavior*, 49:541-566. <http://linkinghub.elsevier.com/retrieve/pii/S0747563215002496>. [Accessed: 21 July 2015].
- Shamala, P., Ahmad, R. & Yusoff, M. 2013. A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, 18(1):45-52. <http://www.sciencedirect.com/science/article/pii/S221421261300029X>. [Accessed: 23 July 2015].

- Shropshire, J., Warkentin, M. & Sharma, S. 2015. Personality, attitudes, and intentions: predicting initial adoption of information security behavior. *Quaternary Geochronology*, 49:177-191. <http://dx.doi.org/10.1016/j.cose.2015.01.002>.
- Sik, K. 2015. Tradition or modernism in grammar teaching: deductive vs. inductive approaches. *Procedia - Social and Behavioral Sciences*, 197(February):2141-2144. <http://www.sciencedirect.com/science/article/pii/S1877042815043414>. [Accessed: 2 June 2016].
- Silva, M.M., De Gusmão, A.P.H., Poletto, T., Silva, L.C.E. & Costa, A.P.C.S. 2014. A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management*, 34(6):733-740. <http://linkinghub.elsevier.com/retrieve/pii/S0268401214000735>. [Accessed: 23 July 2015].
- Simonsson, M., Johnson, P. & Wijkström, H. 2007. Model-based IT governance maturity assessments with COBIT. *In European Conference on Information Systems*, St. Gallen, Switzerland: 1276-1287.
- Singh, S. & Karn, B. 2012. 'Right to Information Act' – a tool for good governance through ICT. *Journal of Information, Communication and Ethics in Society*, 10(4):273-287. <http://www.emeraldinsight.com/10.1108/14779961211285890>. [Accessed: 23 July 2015].
- Smyth, H.J. & Morris, P.W.G. 2007. An epistemological evaluation of research into projects and their management: methodological issues. *International Journal of Project Management*, 25(4):423-436.
- Sohail, M.S. 2011. Sustaining competitiveness through information technology outsourcing: evidence from an emerging nation. *Competitiveness Review: An International Business Journal incorporating Journal of Global Competitiveness*, 21(4):369-381. <http://www.emeraldinsight.com/10.1108/10595421111152165>. [Accessed: 24 February 2014].
- Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. 2014. Variables influencing information security policy compliance: a systematic review of quantitative studies. *Information Management & Computer Security*, 22(1):42-75. <http://www.emeraldinsight.com/10.1108/IMCS-08-2012-0045>. [Accessed: 20 February 2014].
- Song, Z. 2016. The debate between empirical and broader phenomenological approaches to research. *Tourism Management*, 1-5. <http://www.sciencedirect.com/science/article/pii/S0261517716000327>. [Accessed: 2 June 2016].
- Soni, G. & Kodali, R. 2013. *A critical review of supply chain management frameworks: proposed framework*. <http://www.emeraldinsight.com/10.1108/14635771311307713>. [Accessed: 23 July 2015].
- Sterlicchi, J. 1996. Big spending on security. *Computer Fraud & Security*, 1996 (8):2-20.

- Sylvester, D. 2011. ISO 38500 – Why another standard? *COBIT Focus*, 2(1):1-3.
- Tafti, M.H.A. 2005. Risks factors associated with offshore IT outsourcing. *Industrial Management & Data Systems*, 105(5):549-560.
- Takac, P.F. 1993. Outsourcing technology. *Management Decision*, 31(11):15-16.
- Talet, A.N., Mat-zin, R. & Houari, M. 2014. Risk management and information technology projects. *International Journal of Digital Information and Wireless Communications*, 4(1):1-9.
- Tate, W.L. & Ellram, L.M. 2009. Offshore outsourcing: a managerial framework. *Journal of Business & Industrial Marketing*, 24(3):25-268.
<http://www.scopus.com/inward/record.url?eid=2-s2.0-69449091690&partnerID=tZOtx3y1>. [Accessed: 23 July 2015].
- Teo, T.S.H. & Bhattacharjee, A. 2014. Knowledge transfer and utilisation in IT outsourcing partnerships: a preliminary model of antecedents and outcomes. *Information and Management*, 51(2):177-186. <http://dx.doi.org/10.1016/j.im.2013.12.001>.
- Tøndel, I.A., Line, M.B. & Jaatun, M.G. 2014. Information security incident management: current practice as reported in the literature. *Computers & Security*, 45:42-57.
<http://linkinghub.elsevier.com/retrieve/pii/S0167404814000819>. [Accessed: 23 July 2015].
- Tsohou, A., Karyda, M. & Kokolakis, S. 2015. Analysing the role of cognitive and cultural biases in the internalisation of information security policies: recommendations for information security awareness programs. *Computers & Security*, 52:128-141.
<http://linkinghub.elsevier.com/retrieve/pii/S0167404815000565>. [Accessed: 23 July 2015].
- Urbach, N. & Würz, T. 2012. How to steer the IT outsourcing provider. *Business & Information Systems Engineering*, 4(5):247-259.
<http://link.springer.com/10.1007/s12599-012-0231-7>. [Accessed: 11 March 2014].
- Van Griensven, H., Moore, A.P. & Hall, V. 2014. Mixed methods research – the best of both worlds? *Manual Therapy*, 19(5):367-371. <http://dx.doi.org/10.1016/j.math.2014.05.005>.
- Veiga, A. & Martins, N. 2015. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49:162-176.
- Venter, H.S. 2014. Security issues in the security cyber supply chain in South Africa. *Technovation*, 34(7):392–393. <http://dx.doi.org/10.1016/j.technovation.2014.02.005>.
- Von Solms, R. & Van Niekerk, J. 2013. From information security to cyber security. *Computers & Security*, 38:97-102.
<http://www.sciencedirect.com/science/article/pii/S0167404813000801>. [Accessed: 23 July 2015].

- Von Solms, R., Thomson, K. & Maninjwa, M. 2011. Information security governance control through comprehensive policy architectures. In *Information Security South Africa (ISSA)*. Johannesburg: ISSA: 1-6.
- Vorontsova, A. & Rusu, L. 2014. Determinants of IT outsourcing relationships: a recipient-provider perspective. *Procedia Technology*, 16:588-597.
<http://linkinghub.elsevier.com/retrieve/pii/S2212017314002345>. [Accessed: 21 July 2015].
- Wahlgren, G., Bencherifa, K. & Kowalski, S. 2013. A framework for selecting IT security risk management methods based on ISO27005. In 6th International Conference on Communications, Propagation and Electronics, Kenitra, Morocco. Academy Publisher.
- Watjatrakul, B. 2014. Vendor selection strategy for IT outsourcing: the weighted-criteria evaluation technique. *Journal of Enterprise Information Management*, 27(2):122-138.
<http://www.emeraldinsight.com/10.1108/JEIM-04-2012-0015>. [Accessed: 20 March 2014].
- Webb, J., Ahmad, A., Maynard, S.B. & Shanks, G. 2014. A situation awareness model for information security risk management. *Computers & Security*, 44:1-15.
<http://linkinghub.elsevier.com/retrieve/pii/S0167404814000571>. [Accessed: 23 July 2015].
- Wheeler, D. & Zagzebski, L.T. 2008. *On Epistemology*. Wadsworth.
- Wickramasinghe, V. 2015. Effects of human resource development practices on service quality of services offshore outsourcing firms. *International Journal of Quality & Reliability Management*, 32(7):703-717.
- Willcocks, L. & Choi, C.J. 1995. Co-operative partnership and 'total' IT outsourcing: from contractual obligation to strategic alliance? *European Management Journal*, 13(1):67-78.
- Willcocks, L., Fitzgerald, G. & Feeny, D. 1995. Outsourcing IT: the strategic implications. *Long Range Planning*, 28(5):59-70.
- Wilson, J. 2013. *Essential of Business Research: A guide to doing your research project*. 2nd ed. London, United Kingdom: Sage Publications.
- Yap, C.S., Lim, Y.M. & Jalaludin, F.W. 2016. Determinants of ICT outsourcing among the locally-owned manufacturers in Malaysia. *Strategic Outsourcing: An International Journal*, 9(3):324-342.
- Yildiz, S. & Demirel, Z.H. 2014. The benefits, risks and effects on performance of the outsourcing: a comparative study of seasonal and permanent hotels. *Procedia - Social and Behavioral Sciences*, 109:514-521.
<http://linkinghub.elsevier.com/retrieve/pii/S1877042813051318>. [Accessed: 21 July 2015].
- Yin, R.K. 2006. Case study research – design and methods. *Clinical Research*, 2:8-13.

- Yin, R.K. 2009. *Case study research. Design and methods*. 4th ed. Thousand Oaks, California: Sage.
- Yin, R.K. 2014. *Case study research: Design and methods*. 5th ed. Sage.
- Zhang, M. 2015. Capacitated lot-sizing problem with outsourcing. *Operations Research Letters*, 43(5):479-483. <http://dx.doi.org/10.1016/j.orl.2015.06.007>
- Zhang, S. & Fever, H. Le. 2013. An examination of the practicability of COBIT framework and the proposal of a COBIT-BSC Model. *Journal of Economics, Business and Management*, 1(4):391-395.
<http://www.joebm.com/index.php?m=content&c=index&a=show&catid=33&id=353>.
[Accessed: 30 July 2014].
- Zhu, Q., Kong, X., Hong, S., Li, J. & He, Z. 2015. Global ontology research progress: a bibliometric analysis. *Aslib Journal of Information Management*, 67(1):27-54.
<http://www.emeraldinsight.com/doi/abs/10.1108/AJIM-05-2014-0061>. [Accessed: 02 June 2016].
- Zhu, X. 2015. Management the risks of outsourcing: time, quality and correlated costs. *Transportation Research Part E: Logistics and Transportation Review*, 1-13.
<http://linkinghub.elsevier.com/retrieve/pii/S1366554515001271>. [Accessed: 21 July 2015].
- Zou, P.X.W., Sunindijo, R.Y. & Dainty, A.R.J. 2014. *A mixed methods research design for bridging the gap between research and practice in construction safety*. Elsevier.
<http://dx.doi.org/10.1016/j.ssci.2014.07.005>.

APPENDIX A: INTERVIEW GUIDE TEMPLATE

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

IQ 2: How important is information risk management to the business?

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

- **If yes**, what process/es are in place?
- **If no**, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

- **If yes**, what type of access do the process/es include for ICT vendors?
- **If no**, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

- **If yes**, how do the methods work?
- **If no**, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

IQ 7: Do you know of any information and ICT infrastructure security risks when outsourcing ICT?

- **If yes**, what information and ICT infrastructure security risks do you know of?
- **If no**, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

IQ 8: Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?

- **If yes**, what methods does the ICT department have in place to reduce and manage these ICT security risks?
- **If no**, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

IQ 9: Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?

- **If yes**, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?
- **If no**, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

IQ 10: Does the ICT department spend money on ICT infrastructure security?

- **If yes**, what is the average spending in terms of the percentage turnover?
- **If no**, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside Transnet?

IQ 11: What ICT services does the ICT department outsource?

IQ 12: Why does the ICT department outsource these ICT services?

IQ 13: Are criteria used to select suitable ICT vendors?

- **If yes**, what criteria are used?
- **If no**, why are there no criteria used?

IQ 14: Does any of the ICT vendors have access to your systems or networks?

- **If yes**, how do ICT vendors access the systems and networks?
- **If no**, how do ICT vendors support their services if they do not have access?

IQ 15: Are there different levels of access to the systems and networks for ICT vendors?

- **If yes**, on what criteria do you base the levels of access granted?
- **If no**, why do you not have different access levels to systems and networks?

IQ 16: Are there any measures in place to deal with ICT security risks/threats at the different levels?

- **If yes**, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

- **If no**, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

- **If yes**, what programmes do you have in place and how does it work?
- **If no**, why do you think the training programmes are not needed?

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

- **If yes**, what plans does the ICT department have in place?
- **If no**, why does the ICT department not have any plans in place?

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: *Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

- **If yes**, what ICT framework/s do you use and why do you use it?
- **If no**, why do you not use any ICT framework/s?

IQ 21: *Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

- **If yes**, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?
- **If no**, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

- **If yes**, how does the system work?
- **If no**, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

- **If yes,** what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?
- **If no,** why are there not processes/procedures in place?

APPENDIX B1: INTERVIEW ANSWERS OF PARTICIPANT 1

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

Information risks are any risk that can be used to exploit a vulnerability of IT assets and systems to cause harm to organisations, by either crippling systems or stealing information.

IQ 2: How important is information risk management to the business?

Currently the business shows more importance in identifying risks to the business, but the importance of resolving the risks and issues is of a less importance to the business.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Yes, currently vendors that provide us with services have [the] ability to gain access to our systems by completing a user access request form, which gives them access to the corporate domain as a contractor; from there these users can then request access to the required systems that they need access to.

This access is gained either via signing directly onto the domain on the corporate network, gaining access remotely via secure Citrix servers or VPN onto the corporate domain.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Yes, there are four types of main access that is given—full access to the systems, read access, write access, and read and write access to these systems. Each system defines these access types per user, as they require it. Domain access that is given is normal domain user access.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Ownership or intellectual property is the biggest risk currently that are seen when outsourcing projects to companies for ICT functionality or new projects that we undertake; once these projects are under way or completed the organisation do not [sic] have ownership of the intellectual data or back-end designs of these systems that are managed or built.

***IQ 6:** Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?*

If yes, how do the methods work?

Currently we have a governance and risk department that runs within our EIMS department that meets with Transnet Internal Alert (TIA) teams on all projects that run; these teams run all risks on projects and determine impact on all. Risks registers are then drafted and actioned to resolve as the projects go on.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

***IQ 7:** Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

Yes, one of the major risks is with our network provider where we have identified that some core systems that support our system are also hosts to other companies at these break out points. This risk means that if another company is breached through a certain breakout by our provider, we could be in a position that we are breached as well.

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

***IQ 8:** Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

Yes, currently we have internal audits that audit all our vendors for compliance and security issues as well as we internally scan all environments and manage them for changes and vulnerabilities every month. These are then actioned on a criticality basis and either resolved if can be, or risk mitigation is signed for them if we are unable to resolve these risks.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

***IQ 9:** Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

When we use these vendors, we often sign SLA agreements with the vendors; in these agreements, we have matrixes and percentages that we can manage them. Two of the main criteria we have are system vulnerability percentage of less than 95 percent of the environment that needs to be secured and vulnerability free. The other is a "zero breaches" in the year of organisation systems.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

IQ 10: Does the ICT department spend money on ICT infrastructure security?

If yes, what is the average spending in terms of the percentage turnover?

If no, why does the ICT department not spend any money on ICT infrastructure security?

No. currently the ICT department relies on Group initiatives to resolve infrastructure security.

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/threats from inside and outside Transnet?

IQ 11: What ICT services does the ICT department outsource?

Active Directory, networks, server environments, perimeter defence, email and exchange

IQ 12: Why does the ICT department outsource these ICT services?

Our organisation used to own all these services in house; these departments were sold off to other companies and we went [on] a pay-per-service model, as it was cheaper to pay for the service than hosting it internally.

IQ 13: Are criteria used to select suitable ICT vendors?

If yes, what criteria are used?

Each service is determined by a business requirements document that gets discussed and signed off by all ODs; this is then sent out to market as a tender for companies to bid on these services. Once all tenders are received, a tender committee is set up, and a scoring process takes place; these are scored on a number of things. At the end of the process the best candidate and tender is then awarded the service.

If no, why are there no criteria used?

IQ 14: Does any of the ICT vendors have access to your systems or networks?

If yes, how do ICT vendors access the systems and networks?

Yes, as they own the network and services that they provide to us they are the custodians and have full access to our systems and networks; for them the ability to support the business and service they provide.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: Are there different levels of access to the systems and networks for ICT vendors?

If yes, on what criteria do you base the levels of access granted?

If we own the system and the vendors require access to assist us with say software that we have where we own the back-end, we give them read and write access to assist; in trouble shooting the system we retain full access. If it is a service that is provide to us like networks or exchange, the vendor retains the full access and we get the read and write access.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

If we own and manage the system we scan these often for security risks and vulnerabilities and fix them where required; these are done by using systems to scan all environments that we have for changes and implement accordingly to manage and monitor our risks and threats we have.

Environments that are not owned by us, we rely on the service agreements and our Group security team to scan these systems and rectify these services outside of our control for security issues and vulnerabilities.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

If no, why do you think the training programmes are not needed?

No, these programmes are needed and all security risks need training programmes in our organisation. It is seen as money spent and a cost, so it is often not done from budget point of view as seen as money wasted.

The people controlling the budgets do not understand the impact of these risks as many have never experienced one first hand.

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

Our department is currently dependant on about 60 percent of service providers.

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

If no, why does the ICT department not have any plans in place?

No, we sign lengthy contracts with these service providers and often do not include exit and termination conditions in these contracts when signed; our ability to change providers rapidly is non-existent.

Also, as our organisation has multiple ODs, certain ODs have built there dependencies on certain providers that also makes it impossible for us to ever leave our providers we have at current, let alone if something goes wrong. And as we have seen, two of our service providers are still the current service providers that we had when we were breached and compromised, yet our systems rely on them too much for us to get new providers in.

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?

If yes, what ICT framework/s do you use and why do you use it?

We use ISO 27001. We use ISO 9000 for quality management on systems we provide to users.

If no, why do you not use any ICT framework/s?

IQ 21: Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

The frameworks give us a base to build on and a guide of what is required and needed from using the frameworks. We often take these and use them to build our own internal frameworks based on these international standards to have a more robust and properly defined framework, catered for our individual systems, to better manage and get what is required from us to our vendor.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?

If yes, how does the system work?

Currently we have internal audits of the compliance and security that we use to audit the vendors that provide us with services. We provide the auditors with our compliance requirements and security requirements as well as the contract signed; the auditors then issue an audit on behalf of us on those services provided to us and the results are then given through to us to discuss and action with the auditors as well as the vendor in question.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

If no, why are there not processes/procedures in place?

The contracts we have do not include the sub-contractors that do the work of the vendor. Those agreements are often between the vendor and his sub-contractor. If there are issues, we have to measure the vendor, which in some cases is not the person or company actually doing the work.

Usually the issues that I have seen is due to the vendor not conveying the rules and requirements through to the sub-contractor, leaving the issue between the organisation and vendor to resolve and not the sub-contractor.

APPENDIX B2: INTERVIEW ANSWERS OF PARTICIPANT 2

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

Possible threats to the organisational information and the systems that the information is resident on

IQ 2: How important is information risk management to the business?

Information risk is crucial to the management of business.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Yes, the process includes signing a non-disclosure agreement, and subscribing to the ICT policies to the letter.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

The access is on a need-to-know basis; least privilege is enforced with regard to the access to information available to the vendor.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Control of the information and the possible loss of intellectual property

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

Risk assessments are conducted prior to the outsourcing arrangements.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

***IQ 7:** Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

Data exfiltration that is the unauthorised copying, transfer, or retrieval of data from a computer or server and possible reputational/brand damage

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

***IQ 8:** Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

Data protection strategies are incorporated to lessen the impact of data breaches. This includes Hard Drive Encryption—to ensure data cannot be read without the encryption keys and password to access computers.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

***IQ 9:** Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

Yes, service agreements are the vehicles used to monitor adherence of the vendor to the strategies.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

***IQ 10:** Does the ICT department spend money on ICT infrastructure security?*

If yes, what is the average spending in terms of the percentage turnover?

Yes, the average spend is about 12% of percentage turnover and is increasing.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside Transnet?

IQ 11: *What ICT services does the ICT department outsource?*

Security services are managed by external parties, for example, user administration (for user access, deletion, and modification). Internally, a dedicated team is overseeing the trends and act upon the resolution of breaches when identified.

IQ 12: *Why does the ICT department outsource these ICT services?*

Reasons could include that these are so specialised it would make more sense financially to have companies that are experts at this to do it and pay them.

IQ 13: *Are criteria used to select suitable ICT vendors?*

If yes, what criteria are used?

Yes, this is all contained in the supply chain strategy.

If no, why are there no criteria used?

IQ 14: *Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

If no, how do ICT vendors support their services if they do not have access?

No, the access is granted as an exception to maintain absolute control.

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

If no, why do you not have different access levels to systems and networks?

No, a standard procedure is applicable to all vendors and access is granted on an exception basis.

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

Yes, constant monitoring of access is conducted by the incident management team.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

Yes, awareness programmes are conducted to educate the users of the risks.

If one wanted to create say a DVD for distribution to employees, one might outsource the acting to professionals instead of using the employees (an example of outsourcing).

If no, why do you think the training programmes are not needed?

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

IQ 18: On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?

10

IQ 19: Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)

If yes, what plans does the ICT department have in place?

Yes, the current thinking is that absolute dependence on vendors should be minimised and internal resources be upskilled to counter the threat.

If no, why does the ICT department not have any plans in place?

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?

If yes, what ICT framework/s do you use and why do you use it?

Yes, ISO 27001/2; COBIT—these are world-class standards.

If no, why do you not use any ICT framework/s?

IQ 21: Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Yes, consistency is derived from a common acceptance of criteria required to ascertain conformance.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?

If yes, how does the system work?

Yes, adherence to policies and standard is checked and enforced by the security team or Internal Audit.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

Yes, sub-contractors must also adhere to the policies regardless. Make it a condition in the contract that all their employees must attend a session where all policies relevant to them will be explained or where these can be found.

If no, why are there not processes/procedures in place?

APPENDIX B3: INTERVIEW ANSWERS OF PARTICIPANT 3

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

I would say it is the threats and vulnerabilities an organisation may be exposed to whilst relying on Information Technology (IT)

IQ 2: How important is information risk management to the business?

Extremely important as it assists in the identification, assessment, prioritisation, and mitigation strategies for IT risks.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Yes, we have an access request process with the signing of a non-disclosure agreement that all vendors must complete.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Yes, the type of access and reason for access must be specified on the request form.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

I would say the disclosure/theft of confidential and sensitive information.

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

Risks are evaluated as part of the project management methodology. Each project has a risk assessment that is attached to it.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

***IQ 7:** Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

- Unauthorised access
- Theft/disclosure/modification of information without permission
- Poor service delivery in terms of infrastructure security
- Lack of escalation procedures within the company

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

***IQ 8:** Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

The risk management process requires a mitigation plan for each identified risk, and controls need to be implemented in accordance with that plan.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

***IQ 9:** Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

The contracts with vendors outline the requirements of the service required. This include adherence to policies, standards, and measurement criteria.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

***IQ 10:** Does the ICT department spend money on ICT infrastructure security?*

If yes, what is the average spending in terms of the percentage turnover?

Yes but the actual total amount is unknown.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside Transnet?

IQ 11: *What ICT services does the ICT department outsource?*

- Compliance and monitoring of ICT services
- Antivirus and patch management
- Management of IT systems and workstations for certain divisions of the organisation

IQ 12: *Why does the ICT department outsource these ICT services?*

The cost vs benefit of having the infrastructure and skills in-house or outsourced are the main factors.

IQ 13: *Are criteria used to select suitable ICT vendors?*

If yes, what criteria are used?

The procurement processes of the organisation require that technical specifications are defined to evaluate vendors. This includes experience, cost, and reputation, etc.

If no, why are there no criteria used?

IQ 14: *Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

Access systems remotely via Citrix; access to the systems is always logged.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

Full control, read-only access; this is based on the role of the vendor within the organisation.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

These are logged in the risk register to determine the priority and mitigation plan for each risk.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

Information security awareness runs in the organisation; however, outsourcing risks have not been communicated.

If no, why do you think the training programmes are not needed?

SRQ 2.2: **How does the ICT department ensure they do not become dependent on their ICT service providers?**

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

8

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

I am really unsure about this, so I cannot give you an honest answer.

If no, why does the ICT department not have any plans in place?

SRQ 2.3: **How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?**

IQ 20: *Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

- COBIT – IT risk, governance
- ISO 27001 and ISO 27002, information security
- ITIL – service delivery

If no, why do you not use any ICT framework/s?

IQ 21: *Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

The frameworks that we adopt outline controls that can secure the IT environment.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: **How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?**

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

SLAs are defined and the vendors are measured against it. They are also audited to ensure that they comply with the policies and standards of our organisation.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

Yes, the access request covers sub-contractors in the contract of the primary vendor.

If no, why are there not processes/procedures in place?

APPENDIX B4: INTERVIEW ANSWERS OF PARTICIPANT 4

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

To me it refers to inappropriate access to data/information.

It can also be manipulation or corruption of data for [a] specific outcome.

IQ 2: How important is information risk management to the business?

Very important to the organisation

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

This is via an approval process and for limited access and time-periods.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Depending on the access required; in general only read access to production systems (for support purposes).

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Outsource vendors being given access to data that is not required.

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

If no, how does the ICT department determine the impact of information risk?

Overall risks (per project) are assessed; these may include information as well as other risks as appropriate.

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

***IQ 7:** Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

- Confidentiality of information (Information being leaked)
- Inappropriate access (excessive access)
- Viruses and other malware

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

***IQ 8:** Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

Yes, contractors and others need to have the Transnet image loaded on their machines; separate contractor Wi-Fi being commissioned. This will limit virus/malware risk.

Inappropriate access/confidentiality is managed through appropriate access management processes and procedures.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

***IQ 9:** Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

Critical outsource vendors are managed at a Group level, not at the divisional level. It is understood that security measurements are in place, but not sure.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

***IQ 10:** Does the ICT department spend money on ICT infrastructure security?*

If yes, what is the average spending in terms of the percentage turnover?

If no, why does the ICT department not spend any money on ICT infrastructure security?

Security is a Group function, not Operational division.

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside Transnet?

IQ 11: *What ICT services does the ICT department outsource?*

Active Directory and email

IQ 12: *Why does the ICT department outsource these ICT services?*

Most ODs do not have the skills and it is seen as non-core to Transnet business.

IQ 13: *Are criteria used to select suitable ICT vendors?*

If yes, what criteria are used?

Yes, each procurement process has a number of evaluation metrics, i.e. technical, financial, and BBEE.

If no, why are there no criteria used?

IQ 14: *Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

They are directly connected onto our network.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

Yes, this is done on a "per application" basis with supporting motivation.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

Network and Security Operations Centre is in place that monitors the environment for vulnerabilities, breaches, etc. This is going to be further invested in with a new system that is being procured at a group level.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

If no, why do you think the training programmes are not needed?

General information security awareness programmes are in place, but not specifically to ICT outsourcing as they are aimed mainly at the end-user.

SRQ 2.2: **How does the ICT department ensure they do not become dependent on their ICT service providers?**

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

8

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

If no, why does the ICT department not have any plans in place?

Contracts with key vendors have just been renewed or extended. At this stage, we do not have any alternative short term to replace the vendor; the vendor management from both a financial sustainability and performance point of view ensure that we do not put the business at risk of this occurring.

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: *Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

Based on ITIL and COBIT, Transnet has a customised internal control framework for EIMS/ICT.

If no, why do you not use any ICT framework/s?

IQ 21: *Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

The frameworks ensure appropriate governance and controls are in place to manage these vendors/contracts that we use.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

If no, how do you know that ICT vendors adhere to security and compliance requirements?

On an exception basis—issues are picked up via the Security Operations Centre and the monitoring that they do and investigated if needed.

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

All contract terms and all associated rules apply to sub-contractors (where this is allowed). We do not have other tools to do this.

If no, why are there not processes/procedures in place?

APPENDIX B5: INTERVIEW ANSWERS OF PARTICIPANT 5

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

I will say information risks involves information inside Transnet group is accessed or possibly accessed by persons that has no interest to that information. This can be operational, financial or customer based.

IQ 2: How important is information risk management to the business?

Very important to us, we have processes in places regarding this.

Information that exists and that we have is an economic risk to South Africa as the port is the gateway to cargo being in and out of South Africa. Imagine what will happen if the ports are stopped due to this.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

If any vendor outside Transnet needs access to information, they have to get it through an official process and senior IT manager. We would not just hand it over to vendors. For example, if they want to know what servers we have, we would not just give this information to them. We will ask why you want it, but it also depends on what information you want.

Vendors have access to our systems, but only limited to that. The senior ICT manager will give access or sign it off.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

T-systems have access to areas where they influence and manage - nothing more. Anything outside that, we will ask questions. For example, a company is looking after server x and wants information about server y. We [are] not going to give the information to them.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Difficult questions—Information that can bring business to standstill or discredit the company or discredit our customer base or influence our supplier base in a way that change our business model.

***IQ 6:** Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?*

If yes, how do the methods work?

If no, how does the ICT department determine the impact of information risk?

No, just use judgment on this. If you want to bring companies like T-system on board, we only deal with corporate; companies must have history of purity; looking at [a] company from a Procurement level will be part of the evaluation to make sure that we [are] dealing with a company that can support a company like our size or stature.

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

***IQ 7:** Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

There is always a risk because the minute you open yourself to [a] third party, there is also risk that they can be hacked indirectly into our systems.

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

***IQ 8:** Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

- We have firewalls and contracts in place regarding antivirus software which is 24/7
- Manage via SLA meeting and contracts
- Also log files, a lot can be determined from this

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

***IQ 9:** Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

Interesting and good question; I am not sure about this.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

IQ 10: Does the ICT department spend money on ICT infrastructure security?

If yes, what is the average spending in terms of the percentage turnover?

Yes, cannot give percentage because some are spend locally and some nationally; mostly nationally or at group level.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside Transnet?

IQ 11: What ICT services does the ICT department outsource?

- T-systems (Active Directory and email)
- Neotel (network)
- Cameras (security)

IQ 12: Why does the ICT department outsource these ICT services?

[The] first word that comes to mind [is] “human resources”.

This is not our core business so we outsource it. T-systems specialise [in] it so they can provide resources. As IT, we need to stay ahead of technology so [that the] vendor stays ahead on behalf of clients.

If you know you [are] going to use that service for 20 years, you should surely take a long-term position having that service inside the company and train people to have the capacity to do the job and grow the business.

ICT is important to business so I believe we should have it in-house and make it core.

IQ 13: Are criteria used to select suitable ICT vendors?

If yes, what criteria are used?

It is a long procurement process. It includes pricing, ability to serve countrywide (capacity), track record of vendor, tax clearance certificate, technical ability to serve business function such as licenses and software to address business need.

If no, why are there no criteria used?

IQ 14: Does any of the ICT vendors have access to your systems or networks?

If yes, how do ICT vendors access the systems and networks?

- Yes, most definitely
- They do it from their office (remote desktop).
- This is the scary part, the longer the value chain, the bigger the risk

If no, how do ICT vendors support their services if they do not have access?

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

That will depend on [the] nature of [the] contract and product they support.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

The answer is yes, but by telling you—that is a security risk. I see it as a need to know business. For example, who needs to know where servers are or the server room is. The less people know the safer and secure you are.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

Yes, we are busy with a workshop for all employees to coach them on desktop and internet security. There are people at Group that deals with security.

If no, why do you think the training programmes are not needed?

SRQ 2.2: **How does the ICT department ensure they do not become dependent on their ICT service providers?**

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

10

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

If no, why does the ICT department not have any plans in place?

I cannot really answer that question. No one is irreplaceable. This differs from system to system. We can find someone in a week or two but the risk is always the handover because any company that does that wants to do stock taking before they do.

SRQ 2.3: **How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?**

IQ 20: *Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

We use ITIL; ISO also followed, but not sure which ISO.

If no, why do you not use any ICT framework/s?

IQ 21: *Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

ITIL and ISO are the standards to follow. Someone did the pre-thinking for us; all we need to do is follow the guidance and do not need to re-invent the wheel.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

It goes back to [the] contract manager. He/she is responsible for that and it depends on what tool he uses to do it, for example, one vendor of us has [a] security system and one of the security requirements is that it has its own network that runs separately from [the] business network. Every now and then, we get a request to breach the two networks, but we just say no to it. All comes down to management.

Can have any systems in place, but do people comply with it?

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

The contracts that I have read clearly stipulate that if they use sub-contractors, they have the same rules and regulations of [the] primary contractor. They are jointly responsible.

If no, why are there not processes/procedures in place?

APPENDIX B6: INTERVIEW ANSWERS OF PARTICIPANT 6

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

This refers to the threat of information (electronic or printed) being impacted any one way or the other by a threat factor due to a weakness in the controls that are meant to protect such information. The possible impacts are loss of integrity (including reliability), confidentiality, and availability.

IQ 2: How important is information risk management to the business?

Many organisations depend on access to information for decision-making, sustainability, and day-to-day operations. Information has become intellectual property to organisations. Without information, many organisations would cease to exist. It is therefore crucial to ensure that there are adequate information risk management processes to address information-related risks.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

There are standard access-control and authorisation processes in place to ensure that only authorised ICT vendors have access to only the minimum information and systems required. Due to the large landscape of systems at Transnet, these processes are not always enforced consistently.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

- Yes, access ranges from remote access through Virtual Private Networks
- Remote read-only access
- Remote access through intermediate (virtualised systems such as Citrix)
- Once-only access for *ad-hoc* maintenance tasks

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Losing control over the flow of data that is processed and stored in outsourced systems as well as the secondary risk of other parties affiliated with the third party obtaining access to such information.

IQ 6: *Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?*

If yes, how do the methods work?

If no, how does the ICT department determine the impact of information risk?

We are currently working on such mechanisms. Risks are managed through *ad-hoc* security assessments, but this is not the case for all outsourced environments.

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

IQ 7: *Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

- Sabotage
- Espionage
- Data exfiltration/leakage through active sniffing
- Undetected unauthorised access to networks and systems

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

IQ 8: *Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

Although there are “right-to-audit” clauses in outsourced contracts, assurance exercises take place on an *ad-hoc* basis. There are periodic risk assessments as well as auditing exercises; however, there are no direct mechanisms to deal with the risks of infrastructure outsourcing.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

IQ 9: *Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

The maturity of the security teams and its process is far off from being able to measure this.

IQ 10: Does the ICT department spend money on ICT infrastructure security?

If yes, what is the average spending in terms of the percentage turnover?

If no, why does the ICT department not spend any money on ICT infrastructure security?

No, the current network management tender is worth around two billion rand but this includes non-security network infrastructure as well.

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/threats from inside and outside Transnet?

IQ 11: What ICT services does the ICT department outsource?

- Network management
- Server management
- End-user support
- Data centre hosting
- Patch management
- Licensing
- Asset management

IQ 12: Why does the ICT department outsource these ICT services?

This is Transnet's strategy while building capacity in-house.

IQ 13: Are criteria used to select suitable ICT vendors?

If yes, what criteria are used?

Yes, this is based on procurement processes, which are well defined and enforced.

If no, why are there no criteria used?

IQ 14: Does any of the ICT vendors have access to your systems or networks?

If yes, how do ICT vendors access the systems and networks?

Remote access through VPNs, APNs, Citrix, Local Network Access

If no, how do ICT vendors support their services if they do not have access?

IQ 15: Are there different levels of access to the systems and networks for ICT vendors?

If yes, on what criteria do you base the levels of access that are granted?

ICT Vendors have full access to most systems/services as a bulk of our environment is outsourced.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

Yes, although these are in the initial stages. These include vulnerability management, penetration testing, security assessments, and audits.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

If no, why do you think the training programmes are not needed?

No, there are no training/awareness programmes in place to directly address the outsourced environment. Current awareness programmes are aimed at end-users and IT teams.

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

9

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

If no, why does the ICT department not have any plans in place?

No, there is none. The environment is huge and the reliance on the service providers is huge; not enough resources internally.

Such frameworks will guide the decision-making, increase discipline as well as direct assurance efforts.

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: *Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

Yes, this will integrate previous learnings, experience, and best practices from other outsourced environments.

If no, why do you not use any ICT framework/s?

IQ 21: *Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Yes, this will integrate previous learnings, experience, and best practices from other outsourced environments.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

There are SLA steering committees as well as *ad-hoc* audits and assessments.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

If no, why are there not processes/procedures in place?

No, some ICT suppliers deal directly with end-users, bypassing security controls; no end-to-end visibility or enforcement.

APPENDIX B7: INTERVIEW ANSWERS OF PARTICIPANT 7

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

ICT Vendors have access to Transnet information, however their access is restricted by privileges they are given or not given due to their role within the company. Vendors do sign contracts that ensure the protection of Transnet intellectual property.

Information risk is the risk of Transnet information being exploited, exposed, and shared/sold to competitors. Further to this, the term also refers to the risk of intentional or unintentional attacks/errors on TPT data and systems.

IQ 2: How important is information risk management to the business?

Information Risk Management is very important to the organisation; there are a number of controls around information access management, monitoring, preventative and detective controls on the network and system to automatically prevent and detect attacks/errors on TPT data.

Risks around information are managed, tracked, and mitigated by risk champions within the company.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Yes, there are user access management processes in place to ensure that individuals are only provided with the limited access relevant to their role within the company.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Yes, this is dependent on their role in the company and the position they have; some of the vendors do have read and write, however, they do follow an approval process for the access granted to them as well as changes (write) is done in line with the appropriate business decisions.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Transnet information being exploited, exposed, and shared/sold to competitors; however, this is managed by the correct contracts and SLAs in place to protect the company's intellectual property.

IQ 6: *Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?*

If yes, how do the methods work?

Risk management is in place for all projects; should information risks be a concern, the risk will be captured and managed accordingly. Further to this, vendors and contractors do sign confidentiality agreements as part of their contracts to ensure the information of Transnet cannot be exploited, exposed, or sold/shared.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

IQ 7: *Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

Intentional or unintentional attacks/errors on TPT data and systems; however, there are a number of controls in place to manage the exposure of Transnet to these.

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

IQ 8: *Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

- Access management processes are in place to ensure access is appropriately assigned and restricted; segregation of duties processes for all critical applications; SAP GRC processes ensure segregation of duties; conflicts are flagged and addressed; backup procedures are implemented and embedded to ensure all systems can be reverted to a more stable state; internal monthly audits of access management
- Virus protection software has been implemented across all devices on the network. Virus protection software is updated periodically. Monitoring and reporting of these updates are performed on a monthly basis
- Offices are locked after hours, with physical security present
- All laptop users are provided with cable locks for their devices
- Monitoring tools are enabled on the network by the central information security team at Transnet Group. Numerous scanning tools are implemented to monitor and detect vulnerabilities in a timely manner
- User awareness campaign is performed periodically
- EIMS is involved in induction at TPT to make users aware of information security and Transnet policy
- All mobile devices that connect to the Transnet network are required to comply with the required Transnet platform standard; the device will have to accept the policies to encrypt and secure their device before it can connect to the Transnet network
- Monthly vulnerability assessments are performed by EIMS Group Information Security and distributed to operating divisions to address. The TPT EIMS team reviews and addresses the vulnerabilities and reports back on actions taken to remediate

- EIMS Group Information Security performs periodic penetration testing on critical applications and web services at TPT; the results are shared with the operating division and where areas of concern are flagged, the TPT EIMS team is required to address and report back on actions taken to remediate

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

IQ 9: Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

ICT Vendors are required to provide periodic reporting and feedback as well as periodic meetings.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

IQ 10: Does the ICT department spend money on ICT infrastructure security?

If yes, what is the average spending in terms of the percentage turnover?

Yes, the Transnet EIMS Information Security department ensures that all security tools are obtained. Unsure on the average spend.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/threats from inside and outside Transnet?

IQ 11: What ICT services does the ICT department outsource?

Network and management of Active Directory; management of the physical access to computer controls to computer rooms; and management of the protection systems in the computer rooms

IQ 12: Why does the ICT department outsource these ICT services?

This is a strategy within the company and in alignment with all departments.

IQ 13: Are criteria used to select suitable ICT vendors?

If yes, what criteria are used?

Yes, criteria are set per ICT vendor and procurement processes are complied with.

If no, why are there no criteria used?

IQ 14: *Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

Yes, via appropriate access management processes being followed and via a username and password, which must be changed on first log on.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

Yes, based on the required access an individual requires and approved by management. There are roles within systems that are assigned to individuals according to the approved access indicated by management.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

- Access management processes are in place to ensure access is appropriately assigned and restricted; segregation of duties processes for all critical applications; SAP GRC processes ensure segregation of duties conflicts are flagged and addressed; backup procedures are implemented and embedded to ensure all systems can be reverted to a more stable state; internal monthly audits of access management
- Virus protection software has been implemented across all devices on the network. Virus protection software is updated periodically. Monitoring and reporting of these updates are performed on a monthly basis
- Offices are locked after hours with physical security present
- All laptop users are provided with cable locks for their devices
- Monitoring tools are enabled on the network by the Central Information Security team at Transnet Group. Numerous scanning tools are implemented to monitor and detect vulnerabilities in a timeous manner
- User awareness campaign is performed periodically
- EIMS is involved in induction at TPT to make users aware of information security and Transnet policy
- All mobile devices that connect to the Transnet network are required to comply with the required Transnet platform standard; the device will have to accept the policies to encrypt and secure their device before it can connect to the Transnet network
- Monthly vulnerability assessments are performed by EIMS Group Information Security and distributed to operating divisions to address. The TPT EIMS team reviews and addresses the vulnerabilities and reports back on actions taken to remediate
- EIMS Group Information Security performs periodic penetration testing over critical applications and web services at TPT; the results are shared with the operating division and where areas of concern are flagged, the TPT EIMS team is required to address and report back on actions taken to remediate

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

***IQ 17:** Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

Yes, induction and yearly on-going EIMS Information Security awareness programmes

If no, why do you think the training programmes are not needed?

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

***IQ 18:** On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

8

***IQ 19:** Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

If no, why does the ICT department not have any plans in place?

No, but there are independent assurance processes in place.

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

***IQ 20:** Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

Yes, information security frameworks are required to be complied with. We are aligned to COBIT, ITIL, and ISO. We are also aligned to KING III.

If no, why do you not use any ICT framework/s?

***IQ 21:** Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Yes, frameworks provide control environment structures that must be complied with to manage the environments.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

***IQ 22:** Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

There is a procurement vendor management process, which must be followed to ensure that they are compliant to our internal standards.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

***IQ 23:** Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

Yes, via the contract signed by both the primary and secondary vendors.

If no, why are there not processes/procedures in place?

APPENDIX B8: INTERVIEW ANSWERS OF PARTICIPANT 8

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

The probability that the Information might be incorrect or misleading

IQ 2: How important is information risk management to the business?

Very important as all business decisions are based on the information available.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Yes, but I am not fully aware of them or what they are.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Yes, access is based and managed through access requirements and the period needed. Vendors must complete forms that the IT manager must approve.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Reliability, isolation, and durability within the organisation

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

Yes, but I am not fully aware of them.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

IQ 7: Do you know of any information and ICT infrastructure security risks when outsourcing ICT?

If yes, what information and ICT infrastructure security risks do you know of?

Yes, risk of information being accessed by unauthorised individuals.

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

IQ 8: Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

Yes, risk management exercise carried out annually in the ICT department.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

IQ 9: Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

Yes, policies, guidelines, standards, contracts, and audit reviews are done to measure the ICT security success rate of ICT vendors.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

IQ 10: Does the ICT department spend money on ICT infrastructure security?

If yes, what is the average spending in terms of the percentage turnover?

Yes, not aware of the figures

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside Transnet?

IQ 11: What ICT services does the ICT department outsource?

IAAS – Infrastructure as a service (Neotel)

SAAS – Software as a service (Anti-virus, T-Systems)

IQ 12: *Why does the ICT department outsource these ICT services?*

This is a business decision to achieve economies of scale (cost vs benefits of outsourcing).

IQ 13: *Are criteria used to select suitable ICT vendors?*

If yes, what criteria are used?

Yes, but not fully aware of it.

If no, why are there no criteria used?

IQ 14: *Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

Yes, through Active Directory. Major vendors usually apply for [an] AD account. They access the systems via Citrix with the AD account. Smaller vendors usually have to be onsite to access the systems.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

Yes, this is based on the requirements of their tasks.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

Yes, policies, procedures, and incident response guidelines are in place should these risks arise.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

Yes, information security awareness campaigns

If no, why do you think the training programmes are not needed?

SRQ 2.2: **How does the ICT department ensure they do not become dependent on their ICT service providers?**

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

If no, why does the ICT department not have any plans in place?

No, the service provider is responsible for providing an alternative service.

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: *Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

Yes, Cobit, King III, and ITIL

If no, why do you not use any ICT framework/s?

IQ 21: *Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Yes, guiding the ICT department in implementing best practices

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

Yes, monthly, quarterly, and yearly review and assessments

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

Yes, vendor management processes includes sub-contractor rules.

If no, why are there not processes/procedures in place?

APPENDIX B9: INTERVIEW ANSWERS OF PARTICIPANT 9

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

How information can be used to threaten or compromise one's credibility or the ability of someone to take information and cause problems for an individual or organisation.

IQ 2: How important is information risk management to the business?

Information risks management is of [the] utmost importance. Information in its simplest form can pose risks in many ways that could have implications ranging from legal and financial to goodwill defamation.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Yes, however, the processes are covered by agreements or policies and are not enforced or reviewed with the strictest nature. While it may exist, it would seem more to be a paper exercise and no control of how it is monitored. There is very little encryption and access control of information copying.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

If no, why do the process/es not include any type of access for ICT vendors?

Vendors having access to Active Directory have access to global email address lists. Restriction is not always specific and granular, and sometimes seems to be cumbersome to breakdown, hence larger [sic] access is given. Vendors, once onsite, have access to too many resources to be able to access information, be it electronic or in the form of paper trail documents lying around.

The issue here would be that the organisation is too large, and security awareness and focus is to some extent very pre-mature or in early stages of development.

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

[It is] the loss of intellectual property and business process models that give the company its competitive edge of doing business over its competitors

IQ 6: *Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?*

If yes, how do the methods work?

If no, how does the ICT department determine the impact of information risk?

Currently, it seems like ICT would accept the non-disclosure agreements, and trust with the vendors as acceptable.

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

IQ 7: *Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

The access of external parties onto the networks; this could be in the form of APNs, VPNs, or even Wi-Fi. There is a need to understand the outsourced company's policies in terms of patch management, antivirus, and access controls, as a hack on their side could allow infiltration on our side that could lead to [an] information leak.

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

IQ 8: *Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

We have managed firewalls, intrusion detections, application processes for external vendors to gain access into the networks and Active Directory, which have to be approved at a security council.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

IQ 9: *Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

In the past, there have never been major issues with regard to security breaches until two years ago; hence, there was no real drive to put these measures in place. Of recent, there are procedures and protocols being drawn up for security; they are setting up architecture councils and security councils to address these, however, they are still in infancy stages hence the measurement tools and matrices are still to be implemented in my opinion.

IQ 10: Does the ICT department spend money on ICT infrastructure security?

If yes, what is the average spending in terms of the percentage turnover?

Very small, it is seen as a Group cost to secure external links and security is basically done at a firewall level and thereafter at a patch/antivirus level.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/threats from inside and outside Transnet?

IQ 11: What ICT services does the ICT department outsource?

Network, email, ISP, Active Directory

IQ 12: Why does the ICT department outsource these ICT services?

Very small, it is seen as a Group cost to secure external links and security is basically done at a firewall level and thereafter at a patch/antivirus level.

IQ 13: Are criteria used to select suitable ICT vendors?

If yes, what criteria are used?

We follow a procurement process where vendors are rated on BBBEE status; if they meet the criteria of the requirement; best financial price; if they provide any supplier development improvements in the country.

If no, why are there no criteria used?

IQ 14: Does any of the ICT vendors have access to your systems or networks?

If yes, how do ICT vendors access the systems and networks?

They make use via our LAN, WAN, WI-FI, APN, VPN and have an account on our Active Directory. If they access any of the systems internally, they have a user account created based on an approval process.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: Are there different levels of access to the systems and networks for ICT vendors?

If yes, on what criteria do you base the levels of access granted?

If no, why do you not have different access levels to systems and networks?

Not necessarily, as the reason for the vendor could have various requirements, from being a support person to a full-on heading up a development project which they would require full-on access.

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

They are escalated at Group level and then pushed down to the OD level for rectifying. A timeframe is given to fix the vulnerability depending on the seriousness of the risk. There is a ranking scale in terms of high, medium, and low.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

To a minimal extent; travel as [part of] the company is on cost cutting strategies, and travel for such a nature is cut, and it is not effective holding such awareness campaigns over a video conference.

If no, why do you think the training programmes are not needed?

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

In the case of networks and Active Directory – 10

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

If no, why does the ICT department not have any plans in place?

There has been a process of due diligence that took place to transition to a new vendor; however, the current vendors are so entrenched into the organisation that breakaway is very costly and the handover/transition period is very long. The organisation has to plan a buy-back option of infrastructure before it can move to other service providers so as not to lose business productivity.

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: *Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

If no, why do you not use any ICT framework/s?

Not any that I am aware of other than the normal procurement processes.

IQ 21: *Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Yes, it can, as it would define the SLAs, the period of service, the quality of service, the hand-over period and obligations as well as the monitoring of the ICT vendor. It would allow for transparency in understanding the vendors business and identifying any threats to our business.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

If no, how do you know that ICT vendors adhere to security and compliance requirements?

At present, no. There should be a monitoring facility/SLA reporting on the vendor's security policies, procedures, their audit reports, and access to any information regarding any vulnerability within the vendor's organisation in terms of security.

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

This is stated in the procurement/tender award documents and the sub-contractor is seen as one with the ICT Vendor.

If no, why are there not processes/procedures in place?

APPENDIX B10: INTERVIEW ANSWERS OF PARTICIPANT 10

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

Information risk relates to the risk when Information falls into the wrong hands. Information risks are critical to me as senior information security analyst.

IQ 2: How important is information risk management to the business?

Very important; information risks are discussed at various forums as well as being part of the risk register.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

ICT vendors can request access via the normal user account management process and it will be approved for a period of time.

Process works as follows:

A user request form is filled in and sent to the line manager (in this case the manager responsible for managing the vendor) and gets approved. It then goes to the relevant business process owners for approval. Once all approvals have been completed, the system administrator creates the access. Admin access, for example, also needs to be approved by Group security.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

From read access to admin access

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

The vendors not complying with Transnet's information security policies and procedures

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

As part of Transnet's risk management process, a risk analysis is performed. All project risks, including outsourcing, are considered and documented.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

IQ 7: Do you know of any information and ICT infrastructure security risks when outsourcing ICT?

If yes, what information and ICT infrastructure security risks do you know of?

Vendor management and vendor monitoring might not be adequate. Events performed by vendors might not be reviewed or illegal activities might not be picked up. Vendor compliance to Transnet policies and procedures might not be monitored.

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

IQ 8: Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

Service level agreements and vendor management are in place. Also regular audits of vendors, e.g. audit of T-Systems and Neotel by Transnet Internal Audit (TIA) take place on an annual basis.

There is an audit scope, which is normally based on the Transnet Minimum Control Framework (IT). The vendor processes, e.g. backup process; if they manage our backups, the vendor will be audited and reported on.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

IQ 9: Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

Vendors report on a weekly basis on certain security compliance, e.g. compliance to information security standards of vendors that managed infrastructure; however, [I am] not sure if they are reporting on every aspect of information security.

Example: The vendor, e.g. T-Systems, provides compliance of servers they manage. There is also a tool called McAfee ePolicy Orchestrator, which has agents installed on servers and provides feedback. Transnet can check the tool to make sure their reporting is accurate.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

IQ 10: Does the ICT department spend money on ICT infrastructure security?

If yes, what is the average spending in terms of the percentage turnover?

Not sure of the percentages; however, Information Security has a budget of a couple of million each year.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/threats from inside and outside Transnet?

***IQ 11:** What ICT services does the ICT department outsource?*

Desktop support at some Transnet divisions, e.g. Transnet Group, is outsourced. The management of certain services such as network (Active Directory) servers hosting, are outsourced.

***IQ 12:** Why does the ICT department outsource these ICT services?*

Lack of internal capacity; some services are inherent, e.g. network, that was part of Transtel.

***IQ 13:** Are criteria used to select suitable ICT vendors?*

If yes, what criteria are used?

Procurement process and evaluation criteria depending on the request for service

If no, why are there no criteria used?

***IQ 14:** Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

Yes, depending on the vendor; some access via Citrix, others like T-Systems are part of the network/Active Directory listing.

If no, how do ICT vendors support their services if they do not have access?

***IQ 15:** Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

Depending on the role, vendors could have anything from read only to administrator access.

If no, why do you not have different access levels to systems and networks?

***IQ 16:** Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

- Yes, as per incident response categories. Incidents (e.g. failed log in attempts—could be a possible hack/attack; virus activity, etc.) are logged on the T-systems help desk. Categories are based on business risk, for example, Level 1 priority incident (show stopper) needs to be resolved in a much shorter time frame (e.g. 2 hours) compared to a level 4 (no immediate impact on business) of 48 hours
- Example of dashboard with incidents logged

TRANSNET IT SECURITY OPERATIONS SCORECARD 19/01/2015						
Ref	Critical Security Control	Transnet IT Risk Universe Naming Standards	Risk Description	Security Tools & Procedures	Analysts' Comment	Action Required From: Status
1.	Continuous Vulnerability Assessment and Remediation	Reliability of operating systems and network devices	Attack through exploitation of inherent OS, Database and Application vulnerabilities on systems	1.1 Nessus Perimeter and DMZ Daily Scans 1.2 McAfee Vulnerability Manager Internal Monthly Scans	No material threats detected • We have 18% decrease in high vulnerabilities for period of October-November 2014 • December scan results not published • January 2015 scan scheduled	n/a n/a Month-Month Web-Device
2.	Patch Management	Reliability of operating systems and network devices	Exploitation of operating systems and software vulnerability by malware, hacking attacks thereby increasing the risk of data loss	2.1 Microsoft System Centre Configuration Manager	Information contained in the report is not reliable due to recent database corruption currently being resolved within the SCCM rebuild and SIP programme	Transnet & T-Systems SCCM Director Web-Device
3.	Account Monitoring and Control	Logical trespassing	Unauthorised use of system and application accounts (creation, use, dormancy, deletion)	3.1 Active Directory Account with suspicious high login failures and lockouts 3.2 AIX systems with suspicious authentication failures	AD Account(s) Detected per OD: • T- SYSTEMS: USVD Ref# (I3816821 and I3814027) • TFR: USVD Ref# (I3816847) No material threats detected	OD: IMS n/a Day-Day
4.	Controlled Use of Administrative Privileges	Data integrity	Misuse, assignment, and configuration of administrative privileges on computers, networks, and applications	4.1 Active Directory's Unmanaged Computers container 4.2 Accounts with non-Expiring Passwords (including service accounts) 4.3 Privileged Account Monitoring (including domain administrators)	No material changes from last week; however, the values per OD remain extremely high No changes from last week; however, the values per OD remain high No material threats detected	OD: IMS OD: IMS n/a Web-Device Web-Device
5.	Controlled Remote Access	Logical attacks	Uncontrolled use of wireless networks, access points, and wireless client systems to the enterprise network	5.1 Access Point Nodes 5.2 Virtual Private Networks	No material threats detected No material threats detected	n/a n/a Day-Day
6.	Malware Defences	Malware	Installation, spread, and execution of malicious code at multiple points in the enterprise	6.1 Microsoft Email Traffic Volumes and Threats (1 st defence) 6.2 Scanmail for Exchange email Volumes and Threats (2 nd defence) 6.3 MS Forefront and-poll: protection for servers and workstations (last defence)	No material threats detected Scanned for Exchange Mail Signature files using ICT from updated email-signature area No material threats detected	n/a Architecture Council IC218422 n/a Day-Day
7.	Maintenance, Monitoring, and Analysis of Audit Logs	Logical attacks	Deficiencies in security logging and analysis, enabling attackers to hide their location, malicious software, and activities within the enterprise network	7.1 Iscaler Traffic Volumes and Advanced Threats Detector 7.2 CISCO ASA Firewall	No material threats detected High density inbound connections on proxy & email flows (I3816842) T-Systems: USVD Ref# (I3816821)	n/a n/a Day-Day

TRANSNET IT SECURITY OPERATIONS SCORECARD 19/01/2015				
Priority	Transnet IT Risk Universe Naming Standards	Risk Description	Security Tools & Procedures	Analysts' Comment
	Reliability of operating systems and network devices	Attack through exploitation of inherent OS, Database and Application vulnerabilities on systems	1.1 Nessus Perimeter and DMZ Daily Scans 1.2 McAfee Vulnerability Manager Internal Monthly Scans	No material threats detected • We have 18% decrease in high vulnerabilities for period of October-November 2014 • December scan results not published • January 2015 scan scheduled
High	Reliability of operating systems and network devices	Exploitation of operating systems and software vulnerability by malware, hacking attacks thereby increasing the risk of data loss	2.1 Microsoft System Centre Configuration Manager	Information contained in the report is not reliable due to recent database corruption currently being resolved within the SCCM rebuild and SIP programme
High	Logical trespassing	Unauthorised use of system and application accounts (creation, use, dormancy, deletion)	3.1 Active Directory Account with suspicious high login failures and lockouts 3.2 AIX systems with suspicious authentication failures	AD Account(s) Detected per OD: • T- SYSTEMS: USVD Ref# (I3816821 and I3814027) • TFR: USVD Ref# (I3816847) No material threats detected
High	Data integrity	Misuse, assignment, and configuration of administrative privileges on computers, networks, and applications	4.1 Active Directory's Unmanaged Computers container 4.2 Accounts with non-Expiring Passwords (including service accounts)	No material changes from last week; however, the values per OD remain extremely high No changes from last week; however, the values per OD remain high

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?

If yes, what programmes do you have in place and how does it work?

User awareness training in place for all users; this, however, does not cover vendors.

If no, why do you think the training programmes are not needed?

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

IQ 18: On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?

8

IQ 19: Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)

If yes, what plans does the ICT department have in place?

Yes, from December 2014 Transnet got [a] contract in place. Neotel manages [the] network and Transnet owns infrastructure with critical spares, making Transnet less dependent.

Should anything happen to vendors such as buy out for some reason, new vendors can come in and manage [the] network based on [a] contract agreement.

Not sure for all ICT vendors

If no, why does the ICT department not have any plans in place?

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?

If yes, what ICT framework/s do you use and why do you use it?

IT general control framework based on COBIT and ITIL; also makes use of ISO27001.

Transnet has adopted the ISO 27001 as the information security framework. However, there is also a governance framework (minimum control framework), based on COBIT and ITIL, that is in place and covers certain information security controls. Transnet also mapped the gaps not covered in the Minimum control framework to ISO27001.

If no, why do you not use any ICT framework/s?

IQ 21: Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Frameworks provide controls to ensure risks associated with vendors are effectively managed and monitored. However, if the control is not enforced, it will not operate adequately.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

***IQ 22:** Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

Regular audits (annually) of high-risk ICT vendors (e.g. T-Systems/Neotel)

Believe that service level agreements should also cover adherence to information security policies and procedures; not sure if this is in place for all vendors.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

***IQ 23:** Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/ procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

Not sure if these exist specifically for sub-contractors of primary vendors. However, this would fall under the same procedure/process as for primary vendors. The only difference is that sub-contractors should be the responsibility of the primary vendor and the primary vendor will be held accountable/liable for any misconduct.

If no, why are there not processes/procedures in place?

APPENDIX B11: INTERVIEW ANSWERS OF PARTICIPANT 11

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

Information risks to me mean the possibility of accessing information not for outside consumption.

IQ 2: How important is information risk management to the business?

Very certain; information may and could have serious consequences to the organisation if viewed by "competitors".

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Yes, we do have processes that are outlined in our different SOPs (document that I will give you).

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Yes, vendors have different access, such as read and write, but one can never cover or close all the gaps that go with it; for example, Neotel, our network infrastructure provider, has full access to our entire network; for other vendors, Citrix access is enforced and in our particular case, SCADA access is fully controlled at local level.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Gaining intimate knowledge of the business and the risk of viewing information that could be potentially damaging to the organisation.

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

Yes, a risk impact assessment is done when [there are] any access or changes to system that may have a potential impact on production and security.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

IQ 7: Do you know of any information and ICT infrastructure security risks when outsourcing ICT?

If yes, what information and ICT infrastructure security risks do you know of?

I am not party to any of the discussions and assessment information and ICT infrastructure; this takes place at Group level.

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

IQ 8: Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

I am not part of the discussion as mentioned in the previous question.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

IQ 9: Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

I really do not know, to be honest. Transnet Group deals with that kind of things.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

IQ 10: Does the ICT department spend money on ICT infrastructure security?

If yes, what is the average spending in terms of the percentage turnover?

A specific department deals exclusively with ICT security, but I do not know what the spending amount is.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside Transnet?

IQ 11: What ICT services does the ICT department outsource?

Several services are outsourced such as:

- Network infrastructure
- Management information system regarding iron ore management
- SMS system
- Active Directory and e-mail systems
- Print services

IQ 12: Why does the ICT department outsource these ICT services?

I guess this has been a combination of lack of internal expertise and others. It does make sense to outsource certain functions where vendors have the knowhow and knowledge that we do not have internally.

IQ 13: Are criteria used to select suitable ICT vendors?

If yes, what criteria are used?

Certainly, there is quite a strict Procurement process in conjunction with a detailed SOW from ICT. An adjudication committee is normally set up where both technical and administrative and compliance criteria are stipulated. The outcome of the committee is based on a scoring basis such as cost, BEE, technical specifications, and experience.

If no, why are there no criteria used?

IQ 14: Does any of the ICT vendors have access to your systems or networks?

If yes, how do ICT vendors access the systems and networks?

Yes, some have direct access because of the nature of their services provided, such as network infrastructure and/or control of our Active Directory. Others need to follow software authentication through firewalls and other software such as Citrix.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: Are there different levels of access to the systems and networks for ICT vendors?

If yes, on what criteria do you base the levels of access granted?

Yes, there are different levels and they are assigned depending on the services they will be providing to us.

If no, why do you not have different access levels to systems and networks?

IQ 16: Are there any measures in place to deal with ICT security risks/threats at the different levels?

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

This is controlled at Group level, and at local level, we do receive reports regarding "traffic" through our firewalls giving us an insight of what may potentially be a threat, and how often the attempts are made.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

***IQ 17:** Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

We do have briefings every now and then but I think we do not do enough.

If no, why do you think the training programmes are not needed?

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

***IQ 18:** On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

8

***IQ 19:** Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

We will never be able to replace all but we certainly do have contingency and disaster plans in place.

If no, why does the ICT department not have any plans in place?

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

***IQ 20:** Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

I do believe we do have framework/s in place but do not know what they are and how effective they are.

If no, why do you not use any ICT framework/s?

***IQ 21:** Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Not sure, this is all at Group level.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

***IQ 22:** Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

There are vendor management department/s but I have no knowledge on the how. Locally, we set and request the access levels to vendors we deal with directly.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

***IQ 23:** Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

There are, but [I am] not sure how effective they are.

If no, why are there not processes/procedures in place?

APPENDIX B12: INTERVIEW ANSWERS OF PARTICIPANT 12

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

I would say it refers to the exposure of our information; this can be in the form of hacking or employees who sell the information.

IQ 2: How important is information risk management to the business?

Information risks management is most important to us as it is seen as an asset to the business.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Yes, we do have processes in place; these processes are included in our service level agreements (SLAs).

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Most ICT vendors have full access as they own the systems and network infrastructure.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Leakage of confidential information to our competitors

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

If no, how does the ICT department determine the impact of information risk?

I am not sure; this is controlled at HQ level (nationally).

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

***IQ 7:** Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

Yes, network breaches (I cannot give more information).

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

***IQ 8:** Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

Yes, we have an ICT security department that deals with matters, and also local Group security.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

***IQ 9:** Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

No, this is controlled at HQ with SLAs if I am correct.

***IQ 10:** Does the ICT department spend money on ICT infrastructure security?*

If yes, what is the average spending in terms of the percentage turnover?

Yes, but not sure—this is done at HQ level.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/threats from inside and outside Transnet?

***IQ 11:** What ICT services does the ICT department outsource?*

Others include CCTV system maintenance and installation of fibre cables.

***IQ 12:** Why does the ICT department outsource these ICT services?*

This is not our core functions. We export and import goods.

IQ 13: *Are criteria used to select suitable ICT vendors?*

If yes, what criteria are used?

This is done through a tender process that our procurement department handles. We provide them with specifications such as what services we needed, etc. They will then go out on tender for three quotes. Procurements will look at different factors such as cost, experiences, and reputations of ICT vendors.

If no, why are there no criteria used?

IQ 14: *Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

Yes, they access systems and the network via Citrix, remote desktop, onsite, APN, or they have an account on AD.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

Yes, this is determined by the type of service they provide, for example, some will only have read access and some will have read and write access.

Some ICT vendors need to contact the ICT department before they can access our systems.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

Yes, I am not sure how as this is done by our Governance department at HQ.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

Yes, we have programmes or email awareness campaigns that deal with infrastructure security risks but it does not focus on infrastructure security risks associated with outsourcing of ICT.

If no, why do you think the training programmes are not needed?

SRQ 2.2: **How does the ICT department ensure they do not become dependent on their ICT service providers?**

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

If no, why does the ICT department not have any plans in place?

No, the network or infrastructure is too large and the biggest portion of the network belongs to the ICT vendor.

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: *Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

This is done at group level but I know we follow King III that includes COBIT.

If no, why do you not use any ICT framework/s?

IQ 21: *Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

To be honest, I am not sure; I did not look at it in detail. I just know we adopt frameworks for better management of the ICT environment.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

If no, how do you know that ICT vendors adhere to security and compliance requirements?

This is done at Transnet Group Level; I am not sure.

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

Yes, supervision of workmanship and quality control of work

If no, why are there not processes/procedures in place?

APPENDIX B13: INTERVIEW ANSWERS OF PARTICIPANT 13

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

Information risks are the risk that the use of information presents to the business. Due to the "value" of the information, there is a chance that incorrect information will result in bad decisions, unavailability may result in paralysis, or information leaks could damage corporate reputation or have other legal repercussions.

IQ 2: How important is information risk management to the business?

Depends on the amount and type of information and the reliance the business has on it. For a large corporation like us, information risk management will be extremely important.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

There are. Procedural and administrative controls (including policies and standards) outline how external entities can access Transnet's information resources. If a request is made for access, this is assessed based on business requirements and governance and security requirements.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Yes, [the] access type will be determined on business requirements.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Vendor not adhering to requirements and vendor lock-in (i.e. leaks due to poor vendor security and vendor not supplying information of sufficient integrity or usability).

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

Yes, risk analysis of outsourcing is conducted as part of the project management and business requirements.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

IQ 7: Do you know of any information and ICT infrastructure security risks when outsourcing ICT?

If yes, what information and ICT infrastructure security risks do you know of?

- Vendor lock-in
- Incompatibility of technologies and processes
- Vendor cannot supply spares/replacements on time, resulting in prolonged outages or vulnerabilities
- Vendors may not be fully competent with security—this could result in misconfigurations and vulnerabilities
- Vendor may not follow corporate processes, resulting in decreased security or availability
- Weak SLAs

The company is still accountable for information even though it has been outsourced to a vendor

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

IQ 8: Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

Procedural and administrative controls are in place. Risk analysis and management is conducted as part of the project life cycle.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

IQ 9: Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

Rating performance for compliance of security requirements; I am not exactly sure – I know it is there. For example, when developing a new project, there will be critical success factors that need to be delivered. Specific details of how the rating is done could vary between different systems. I have not dealt with it sufficiently to comment more. Penalties can be introduced based on delivery of projects, including adherence to security requirements.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

IQ 10: Does the ICT department spend money on ICT infrastructure security?

If yes, what is the average spending in terms of the percentage turnover?

Yes, not sure

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/threats from inside and outside Transnet?

IQ 11: What ICT services does the ICT department outsource?

Network management, server management, help desk

IQ 12: Why does the ICT department outsource these ICT services?

Not sure

IQ 13: Are criteria used to select suitable ICT vendors?

If yes, what criteria are used?

Criteria are developed during the business case and according to the RFP, etc.

If no, why are there no criteria used?

IQ 14: Does any of the ICT vendors have access to your systems or networks?

If yes, how do ICT vendors access the systems and networks?

Yes, they manage it. They also have logons to perform specific duties.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: Are there different levels of access to the systems and networks for ICT vendors?

If yes, on what criteria do you base the levels of access granted?

Yes, based on (and limited to) the functions they required to perform.

If no, why do you not have different access levels to systems and networks?

IQ 16: Are there any measures in place to deal with ICT security risks/threats at the different levels?

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

Yes, risk analysis is conducted during the project lifecycle, and risks/threats are addressed accordingly.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?

If yes, what programmes do you have in place and how does it work?

Yes, information security awareness roadshows are conducted to generate awareness. Articles are distributed in internal publications and by email.

If no, why do you think the training programmes are not needed?

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

IQ 18: On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?

8

IQ 19: Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)

If yes, what plans does the ICT department have in place?

Yes, DR, BCP, etc.; currently, if Neotel or T-Systems experience problems, we are affected. There are plans to change the structure of the networks, which will reduce reliance on the vendors. I am aware that if a specific datacentre goes down, we do lose access to some of the applications. I cannot speak to the specific plans if that happens; I have not seen anything regarding that.

If no, why does the ICT department not have any plans in place?

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?

If yes, what ICT framework/s do you use and why do you use it?

COBIT, ISO 27001/2

If no, why do you not use any ICT framework/s?

IQ 21: Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Yes, a framework ensures a common baseline and consistency to ensure a minimum level of security.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?

If yes, how does the system work?

That depends on what exactly is being monitored. Some compliance issues are monitored weekly, some daily, some have monthly updates. There are automated tools that help with the monitoring, which allow it to be done more often (daily/weekly).

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

I am not aware of any specific processes/procedures for sub-contracting. The vendor is ultimately responsible and accountable for delivering according to requirements—they must take the risk of sub-contracting. I suppose any restrictions will be included in the contract/SLA.

If no, why are there not processes/procedures in place?

APPENDIX B14: INTERVIEW ANSWERS OF PARTICIPANT 14

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

"Information landing in the wrong hands"—example, a Transnet user has access to information and systems via his company supplied laptop, it gets stolen and information can get leaked that way.

IQ 2: How important is information risk management to the business?

Very important as all information available to the outsource company is "for your eyes only" and not public knowledge.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Question excluded from interview.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Question excluded from interview.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Sharing tender information with competition/other outsource companies.

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

I am sure there is but I am not involved in that specific detail.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

***IQ 7:** Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

Companies who qualify need to have the infrastructure in place to comply with information risks identified by Transnet. For example, their computer standards should include and not be lower than Windows 7 Enterprise, 64-bit version with Service Pack 1 for 64-bit version—to not allow any kind of virus threats to flow through or allow hacking. Sometimes their machines do not comply—that is seen as an infrastructure security risk.

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

***IQ 8:** Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

One that I know of is keeping information in iCloud Space where security measures are very high. You need four kinds of security clearance to be able to view specific project details.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

***IQ 9:** Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

Question excluded from interview.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

***IQ 10:** Does the ICT department spend money on ICT infrastructure security?*

If yes, what is the average spending in terms of the percentage turnover?

20%

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/threats from inside and outside Transnet?

IQ 11: *What ICT services does the ICT department outsource?*

Printer maintenance and support

IQ 12: *Why does the ICT department outsource these ICT services?*

Because renting a printer on maintenance contract is more cost effective than employing a printer specialist.

IQ 13: *Are criteria used to select suitable ICT vendors?*

If yes, what criteria are used?

Criteria include name brands, trusted suppliers, good track record for maintenance, more cost effective per page billing.

If no, why are there no criteria used?

IQ 14: *Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

Only have access to Fault Logging System; allowing them to reduce their response times.
They should have their own equipment, which comply with the standards to enable them to access the Transnet network. All users should sign a policy document to get a contractor User ID and password to be allowed access to the Transnet network.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

Yes, access granted to only a selected team with a requirement that at least one member of the team should be onsite.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

Not sure

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

Question excluded from interview.

If no, why do you think the training programmes are not needed?

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

IQ 18: On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?

Question excluded from interview.

IQ 19: Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)

If yes, what plans does the ICT department have in place?

Not sure

If no, why does the ICT department not have any plans in place?

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?

If yes, what ICT framework/s do you use and why do you use it?

Question excluded from interview.

If no, why do you not use any ICT framework/s?

IQ 21: Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Question excluded from interview.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?

If yes, how does the system work?

Question excluded from interview.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/ procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

- Users that are not part of Transnet, their computers will have specific policies sent and forced through Active Directory (GPO), restricting them to only have access to Google Chrome and only to [the] Fault Logging System—they will not be able to [access] any other programme on the computer except that
- Transnet Computer Policy
- Transnet Internet Policy
- Transnet Document Communication Equipment Policy

If no, why are there not processes/procedures in place?

APPENDIX B15: INTERVIEW ANSWERS OF PARTICIPANT 15

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

If you look at information as an asset and the fact that it has value, you can then apply all kinds of risks. The asset can be made unavailable or the asset can be stolen. Any of the risks can have a negative effect on the information asset.

IQ 2: How important is information risk management to the business?

It is very important because the company has an entire Risk department. There are risks managers and risks GMs. Part of the risk functions include the information risks or your IT risks. They then put it into a risk register. So they maintain a risks register and they constantly look at emergency risks. Every month we have a Risiko; in that Risiko all the managers are part of that Risiko and all the managers are asked, "do you have any emergency risks you want to put on the risks register?" The company takes it very seriously and rightly so.

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Yes, there is; the main thing around it is that there are now external parties that are onsite and they [are] coming into the business. The main thing we have in our policy is they must be accompanied at all times. They generally go onsite to work in the server room. If they go into the server room they have to sign the register; another rule is that they are accompanied at all times by ICT personnel.

From outside they do have access, if you look at Neotel now. It is their switches, believe it or not, so they have access to it and they can log onto it because it is their switches; so that area is very difficult because we do not know what they can do because they are logging on remotely.

If it is physical access they are accompanied, and the other thing is obviously they will not have the admin IDs like we have. So, we won't let them work with their own IDs; we will sign on. In other words, if they come on as an admin account we will sign them on; then they will do whatever they do while we stand there. From outside they do have access, especially if it comes to things like switches. To me, that is always the big the risk.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Key suppliers have full access because they are managing our AD domains, our DCs, our domain controllers against AD rights, and they are managing our exchange servers. Between those two key suppliers, you basically have access to everything.

I am probably not the best person to ask as to what is the security arrangement that Transnet will have in place with T-Systems, but I can bet your bottom dollar that It is probably along the lines of detail login onto the servers. People need to be trained ahead of time before they get granted

access, and access must be handled in a full, proper sign form kind of process in a structured formalised manner. So, if T systems is hiring 50 people, we need to have details of that persons because those guys are going to work on our servers.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

The highest risk probably is putting in controls. We can probably put all these controls in place to make sure that [the] vendor is not doing anything bad. We can make sure that there is access control, there is authorised access control.

We can put in place login on the machines. We can put in maybe a scanner that looks at behaviour; so, it looks at what the guys are doing on a daily basis, especially when we run it and check that this person is doing something out of the ordinary. You can put all that stuff in place but the biggest risk for me is still the person.

We can put all the good stuff that I just mentioned in place but we will now have people belonging to the 3rd party organisation that is walking around on the outside knowing the admin username IDs and passwords for exchange in AD and in my opinion, the weakest link is the people.

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

I do not know if it is a specific method, but we will have methods because based on our experience, we will understand the value of an information resource. We will be able to quantify what is each risk associated with that information resource and then be able to establish a risk register.

A risk register consist of the risk, the likelihood of that risk, what are the chances of this happening. What is the impact of that risk? The risk register will be placed on the table whenever we have our Risiko and when you come with a new emergency risk.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

IQ 7: Do you know of any information and ICT infrastructure security risks when outsourcing ICT?

If yes, what information and ICT infrastructure security risks do you know of?

On the infrastructure front, if that is outsourced, the first risk regards to security is the physical location of this thing; this thing is now [that] the servers are not held onsite, they are held at who knows where. That will be the first one if it comes to infrastructure.

A further thing with security and infrastructure is that when it comes to infrastructure, there is the risk that the infrastructure can potentially be hacked.

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

***IQ 8:** Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

We will probably have all kinds of controls in places and that controls will be written into the contract, I am sure, to say you will have your patches run, you will have your updates done; you will have the latest anti-virus. All the latest patches, all the good stuff are there; there are intruder detections systems.

Maybe I should skip this question because I do not really know what they have in place to reduce and manage the risks.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

***IQ 9:** Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

I would say they probably do have but I am not sure about it. It is something that will happen at a group level. If it were me, I would certainly put a framework together of your security concerns and then obviously when your contract is signed for outsourcing.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

***IQ 10:** Does the ICT department spend money on ICT infrastructure security?*

If yes, what is the average spending in terms of the percentage turnover?

I do not know; the Group will know that.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/threats from inside and outside Transnet?

***IQ 11:** What ICT services does the ICT department outsource?*

The entire network, the user authentication [AD]/authentication system, email, domain controllers [DC], Infrastructure

IQ 12: *Why does the ICT department outsource these ICT services?*

You outsource it generally because of the costs. If you had to insource that [the services], you would have to buy the hardware on which all those services/machines run; you would have maintenance done on that hardware. So you have that hardware, you [are] buying the hardware; so it is a capital outlay plus you got an operational apex cost to maintain that hardware and then probably the most important thing is your labour cost.

So, I think the biggest reason for wanting to outsource is the fact that it is cost driven. There is a smaller element which then basically means that you can free up because, remember now, you got all that labour, hardware and stuff—you need to have all kinds of SOPs in place, how the equipment must be operated and all of that. You need SOPs. You need the government's framework around it.

IQ 13: *Are criteria used to select suitable ICT vendors?*

If yes, what criteria are used?

I think the Transnet procurement policies are generally very well defined. I think that they are open and transparent and very often what will happen is they follow the procurement process whether its general RFI (request for information), RFP (request for proposal), and then it goes potentially out for tender. The tender process is very open, well publicised, very structured.

Transnet is a unit organisation, they send out 100% of tenders every year.

If no, why are there no criteria used?

IQ 14: *Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

Yes, they do. Physically they will go to the plant and we will allow them in based on their access cards. They will also have remote access via remote tools. You must remember that Neotel Support sits in India and they [are] logging into switches to fix problems.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

Yes, there will be different levels of access depending on the level of outsourcing. If it is fully outsourced, they run it, so they will have admin rights. We as Transnet might not have the same access as them.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

In terms of AD, Neotel, and Exchange, I cannot really answer that question. This lives at Group level and is fully outsourced. I do not know what they have in place there.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

***IQ 17:** Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

If no, why do you think the training programmes are not needed?

No, we do not have it at our level; [it is] not something we do here. This is done at HQ and I am sure they have people appointed to do it.

SRQ 2.2: How does the ICT department ensure they do not become dependent on their ICT service providers?

***IQ 18:** On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

10. We are completely at their mercy.

***IQ 19:** Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

I cannot answer that question and I do not know. I do not want to speculate.

If no, why does the ICT department not have any plans in place?

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

***IQ 20:** Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

Difficult to answer that question; I do know Transnet Group chief security officer and [am] pretty sure he would have put in place, but I am not sure.

If no, why do you not use any ICT framework/s?

***IQ 21:** Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

I am really not sure about it as I mentioned in the previous question.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

The answer is that I do not, but again, I am sure that Group and HQ will have something in place. This will usually be audited by our internal and externally auditors.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

I am not necessary sure that we will contract with sub-contractors, for example, if we sign with Neotel, they will be responsible for everything and they must ensure that sub-contractors adhere to contractual agreements.

If no, why are there not processes/procedures in place?

APPENDIX B16: INTERVIEW ANSWERS OF PARTICIPANT 16

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

It is the risk of your company information being accessed by unwanted parties.

IQ 2: How important is information risk management to the business?

Extremely important

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Question excluded from interview.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Question excluded from interview.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Hacking of the client's information

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

We have various protected firewalls and DMZ areas in place. Should any outside company need to link to Transnet services, there is a process in place to give the necessary approval; they then have to logon via a DMZ in order to gain access to the network. Electronic logs are kept of all traffic/connections.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

***IQ 7:** Do you know of any information and ICT infrastructure security risks when outsourcing ICT?*

If yes, what information and ICT infrastructure security risks do you know of?

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

Not sure; cannot provide any further details.

***IQ 8:** Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?*

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

Yes, [there are] various access control regulations in place where access to devices on the network gets logged with any change made.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

***IQ 9:** Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?*

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

Question excluded from interview.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

***IQ 10:** Does the ICT department spend money on ICT infrastructure security?*

If yes, what is the average spending in terms of the percentage turnover?

Yes, but not sure how much.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside Transnet?

***IQ 11:** What ICT services does the ICT department outsource?*

Board room management services

***IQ 12:** Why does the ICT department outsource these ICT services?*

It is not one of our core offerings to our clients, so it makes sense to outsource those services.

IQ 13: *Are criteria used to select suitable ICT vendors?*

If yes, what criteria are used?

- Reliability
- BEE Status
- Years of operating
- Business licensing

If no, why are there no criteria used?

IQ 14: *Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

If no, how do ICT vendors support their services if they do not have access?

No, they do not have any access. They send technicians to site if needed as we do the first line of support.

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

If no, why do you not have different access levels to systems and networks?

No, they do not have access.

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

There is an escalation process in place, so should a threat/risk be discovered, it will be isolated and referred to our security team.

There is also intrusion detection enabled on the network that will alarm the security team of possible threats/risks.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

Question excluded from interview.

If no, why do you think the training programmes are not needed?

SRQ 2.2: **How does the ICT department ensure they do not become dependent on their ICT service providers?**

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

Question excluded from interview.

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

Yes, we have different vendors for the same services.

If no, why does the ICT department not have any plans in place?

SRQ 2.3: How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?

IQ 20: *Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

Question excluded from interview.

If no, why do you not use any ICT framework/s?

IQ 21: *Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Question excluded from interview.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

Question excluded from interview.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/ procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

Yes, they have to adhere to the same standards we have agreed to with Transnet. Our technicians oversee them and job cards will not be signed off unless we are satisfied with their work.

If no, why are there not processes/procedures in place?

APPENDIX B17: INTERVIEW ANSWERS OF PARTICIPANT 17

RQ 1: WHAT INFORMATION RISKS DOES THE ICT DEPARTMENT MANAGE WHEN OUTSOURCING ICT PROJECTS?

SRQ 1.1: What type of access do the ICT vendors have to Transnet's information and systems?

IQ 1: What does the term 'information risks' mean to you?

Any possible (non-controlled) effect on the network that carries some form of risk

IQ 2: How important is information risk management to the business?

Highest priority

IQ 3: Are there process/es in place for ICT vendors to gain access to Transnet's information and systems?

If yes, what process/es are in place?

Question excluded from interview.

If no, why are there no process/es in place?

IQ 4: Do the process/es include the type of access for ICT vendors?

If yes, what type of access do the process/es include for ICT vendors?

Question excluded from interview.

If no, why do the process/es not include any type of access for ICT vendors?

SRQ 1.2: What is seen as the highest information risk when outsourcing ICT projects?

IQ 5: In your opinion, what is the highest information risk when outsourcing?

Without proper governance in the execution of work and/or changes on the network could result in devastating consequences for the business.

IQ 6: Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?

If yes, how do the methods work?

Yes, the proper administrative (change) controls and related approval authorities in both Neotel and Transnet are mandatory before any changes can be made. There are also committees (e.g. the Transnet architectural committee) that would need to approve certain design changes and/or additions. It is part of the governance administration when preparing for change controls on the network. The possible service impact would be listed on the change control request.

If no, how does the ICT department determine the impact of information risk?

SRQ 1.3: What strategies does the ICT department have in place to manage information risks associated with ICT outsourcing?

IQ 7: Do you know of any information and ICT infrastructure security risks when outsourcing ICT?

If yes, what information and ICT infrastructure security risks do you know of?

Yes, any work on the network carries with it some element of risk. This could be service affecting, loss of data, data integrity compromise, application functionality, etc.

If no, why do you think it is not necessary to know of information and ICT infrastructure security risks when outsourcing ICT?

IQ 8: Does the ICT department have methods in place to reduce and manage these information and ICT infrastructure security risks?

If yes, what methods does the ICT department have in place to reduce and manage these ICT security risks?

Yes, a clear governance process is followed to manage any changes.

If no, why does the ICT department not have any methods in place to reduce and manage these ICT security risks?

SRQ 1.4: What does the ICT department do to ensure that ICT vendors adhere to the strategies that are put in place to manage information risks when outsourcing ICT projects?

IQ 9: Does the ICT department have criteria in place to measure the ICT security success rate of ICT vendors?

If yes, what criteria does the ICT department have in place to measure the ICT security success rate of ICT vendors?

Question excluded from interview.

If no, why is it that the ICT department does not have any criteria in place to measure the ICT security success rate of ICT vendors?

IQ 10: Does the ICT department spend money on ICT infrastructure security?

If yes, what is the average spending in terms of the percentage turnover?

Yes, [it is] not possible for me to say, but to confirm that the Neotel Data Center is mandated by the compliance of the highest Tier (4) DC.

If no, why does the ICT department not spend any money on ICT infrastructure security?

RQ 2: HOW CAN THE ICT DEPARTMENT PROTECT THEIR INFORMATION THROUGH THE USAGE OF INFRASTRUCTURE RISK MANAGEMENT AGAINST ICT SECURITY THREATS WHEN OUTSOURCING ICT?

SRQ 2.1: How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside Transnet?

IQ 11: *What ICT services does the ICT department outsource?*

Very few services in IT, however, there are services that are secondary to our core focus, which we outsource to selected vendors, such as boardroom services (we outsource to Ubuntu Video Conferencing and Audio Visual).

IQ 12: *Why does the ICT department outsource these ICT services?*

It makes business and financial sense.

IQ 13: *Are criteria used to select suitable ICT vendors?*

If yes, what criteria are used?

Yes, there are many, such as BEE, financial stability, range of services, logistical coverage, experience, and track record.

If no, why are there no criteria used?

IQ 14: *Does any of the ICT vendors have access to your systems or networks?*

If yes, how do ICT vendors access the systems and networks?

Neotel provides consumer services for voice and data and therefore open our networks to our subscribers; fully controlled access.

If no, how do ICT vendors support their services if they do not have access?

IQ 15: *Are there different levels of access to the systems and networks for ICT vendors?*

If yes, on what criteria do you base the levels of access granted?

Only controlled access is provided to certain vendors.

If no, why do you not have different access levels to systems and networks?

IQ 16: *Are there any measures in place to deal with ICT security risks/threats at the different levels?*

If yes, how does the ICT department deal with the ICT infrastructure security risks/threats at the different levels?

Yes, fall back processes, multiple data backup locations, admin, physical security measures (CCTV, firewalls, guards, etc.), business continuity services, disaster recovery services.

If no, why does the ICT department not have measures in place to deal with ICT infrastructure security risks/threats at the different levels?

IQ 17: *Do you have training programmes in place to make employees aware of the infrastructure security risks associated with ICT outsourcing?*

If yes, what programmes do you have in place and how does it work?

Question excluded from interview.

If no, why do you think the training programmes are not needed?

SRQ 2.2: **How does the ICT department ensure they do not become dependent on their ICT service providers?**

IQ 18: *On a scale of 1 to 10, how dependant is the ICT department on ICT service providers?*

Question excluded from interview.

IQ 19: *Does the ICT department have any plans in place to replace ICT vendors immediately if something goes wrong? (Business continuity and disaster recovery plans)*

If yes, what plans does the ICT department have in place?

Yes, contingency plans are a part of the DR process strategy.

If no, why does the ICT department not have any plans in place?

SRQ 2.3: **How can the implementation of an ICT framework/s protect Transnet's information against ICT infrastructure security threats when outsourcing ICT functions?**

IQ 20: *Do you make use of any ICT framework/s to protect business against ICT infrastructure security threats when outsourcing ICT functions?*

If yes, what ICT framework/s do you use and why do you use it?

Question excluded from interview.

If no, why do you not use any ICT framework/s?

IQ 21: *Do you think ICT frameworks can help the ICT department against information and ICT Infrastructure security threats when outsourcing ICT functions?*

If yes, how does the ICT framework/s help ICT department against information and ICT infrastructure security threats when outsourcing ICT functions?

Question excluded from interview.

If no, why do you think the ICT frameworks does not help ICT department against ICT information and infrastructure security threats when outsourcing ICT functions?

SRQ 2.4: **How does the ICT department ensure that ICT vendors adhere to their security and compliance requirements?**

IQ 22: *Does the ICT department have a system in place to check if ICT vendors adhere to security and compliance requirements?*

If yes, how does the system work?

Question excluded from interview.

If no, how do you know that ICT vendors adhere to security and compliance requirements?

IQ 23: *Are there processes/procedures in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?*

If yes, what processes/ procedures are in place to ensure that sub-contractors adhere to the same rules of your primary ICT vendor?

All contractors needs to have proof of compliance certification to Neotel as well as the Transnet rules and regulation (onsite)

If no, why are there not processes/procedures in place?

APPENDIX C: CONSENT LETTER OF COMPANY TO CONDUCT RESEARCH

A Division of
Transnet SOC Ltd
Registration Number
1990/000900/30

Kingsmead Office Park
Stalwart Simelane St.
Durban
4001

P.O. Box 10124
Marine Parade, Durban
South Africa, 4065
T +27 31 308 8333



MEMORANDUM
www.transnet.net

To: Karl Sockwa, Chief Executive, Transnet Port Terminals

From: Delton Basson, Chief Administrator, Transnet Port Terminals Saldanha

Date: 3rd December 2014

SUBJECT: Permission to conduct Research at Transnet Port Terminals

PURPOSE:

The aim of this submission is to request permission for conducting research at Transnet Port Terminals

BACKGROUND:

I am a student at Cape Peninsula University of Technology (CPUT). As part of completing my **Master of Technology (MTech) degree**, I am required to conduct research. My supervisor is Dr Andre de la Harpe, from the Centre for CIO Research in Africa (CenCra) and also a lecturer at CPUT.

The title of my research is: "Managing information risks through the usage of infrastructure risks management in information communication technology outsourced projects at a transport organisation in South Africa."

DISCUSSION:

The context of the study is:-

It is unclear how to manage Information Communication Technology (ICT) Infrastructure risks when outsourcing ICT projects, exposing organisations to ICT security risks (Hamlen & Thuraisingham, 2013; Herath & Kishore, 2009; Urbach & Würz, 2012).

A handwritten signature in black ink, appearing to be "D Basson".

RECOMMENDATION:

It is recommended that this request for conducting research at Transnet is approved.

Requested by:

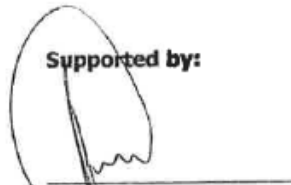


Delton Basson

Chief Administrator, ICT, TPT Saldanha

Date: 3/12/2014

Supported by:



Fernando Gonçalves

ICT Manager, TPT Saldanha

Date: 3/12/2014

Recommended by:



Velile Dube

General Manager: Western Cape, TPT

Approved / Not-Approved by: *




Dumisani Khuzwayo

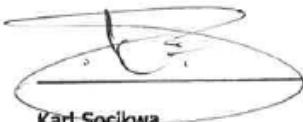
General Manager: Human Resources, TPT

Date: 4/12/2014

Date: 10/12/2014

* I WOULD RECOMMEND THAT DR ACKERMANN SHOULD ALSO HAVE AN INPUT, AS CUSTODIAN OF ICT PROCESSES. 

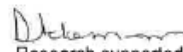
Approved / Not-Approved by:



Karl Socikwa

Chief Executive, Transnet Port Terminals

Date: 18/12/14


Research supported
12/12/2014

The aim of this study is to explore how the selected organisation can manage infrastructure risks when outsourcing their ICT projects by following a recommended framework by the researcher.

Based on the data collection method for this study, a total of 15 participants will be interviewed to share their views on this topic. The interview will consist of semi-structured questionnaires and audio recording. Participants will have the right to walk out of the interview at anytime, if they feel uncomfortable with the questions asked. Throughout the research process including the data collection and data analysis process ethics will be considered.

The outcome of this research will propose a framework that will help the selected organisation to manage Infrastructure risks when outsourcing ICT projects.

FINANCIAL IMPLICATIONS:

There is no financial implications for Transnet

BUDGET IMPLICATIONS:

There are no budget implications.

APPENDIX D: EXAMPLE OF ANALYSIS OF INTERVIEW DATA

Research Question 1	What information risks does the ICT department manage when outsourcing ICT projects?		
Research Question 1.1	What type of access does the ICT vendors have to Transnet's information and systems?		
Interview Question 1.1.1	What does the term "information risks" mean to you?		
Answers	<i>Participant 1</i>	<i>Participant 2</i>	<i>Participant 3</i>
	Used to exploit a vulnerability of IT assets and assets.	Threats to organizations information	Threats and v
	Harm to the system by stealing info	and system	while dependi
Interview Question 1.1.2	How important is information risks management to the business?		
Answers	<i>Participant 1</i>	<i>Participant 2</i>	<i>Participant 3</i>
	Identifying risks to the business more important	Crucial to management of business	Extremely imp
	Resolving risks less important to business		
Interview Question 1.1.3	Is there a process/es in place for ICT vendors to get access to Transnet information and systems?		
Answers	<i>Participant 1</i>	<i>Participant 2</i>	<i>Participant 3</i>
	Completing of user access forms to access systems	Signing of non-disclosure agreements	Access requ
	Access directly to corporate network or remotely via a secure Citrix server or VPN	Subscribing to ICT policies	Signing of nor
Interview Question 1.1.4	Does the process/es include the type of access of ICT vendors?		
Answers	<i>Participant 1</i>	<i>Participant 2</i>	<i>Participant 3</i>
	Yes,3 Types (Read,write and full access)	Yes,Access in need-to-know basis	Yes, Access :
	Access is based on requirements per user.	Least privilage enforced for vendor access	
Research Question 1.2	What is seen as the highest information risk when outsourcing ICT projects?		
Interview Question 1.1.5	In your opinion what is the highest information risk when outsourcing?		
Answers	<i>Participant 1</i>	<i>Participant 2</i>	<i>Participant 3</i>
	Ownership or intellectual property of data	Loss of intellectual property	Disclosure/Th
Interview Question 1.1.6	Does the ICT department have methods in place to determine the impact of information risks when outsourcing ICT projects?		

A	B	C	
Interview Question 1.1.10 Answers	Does the ICT department spend money on ICT infrastructure security? <i>Participant 1</i> No, Relies on Transnet group for resolving infra security	<i>Participant 2</i> Yes, 12% of percentage of turnover	<i>Participant 3</i> Yes ,Amount unk
Research Question 2	How can the ICT department protect their information through infrastructures risk management against ICT security threats when outsou		
Research Question 2.1	How does the ICT department deal with ICT infrastructure security risks/ threats from inside and outside the Transnet??		
Interview Question 1.1.11 Answers	What ICT services does the ICT department outsource? <i>Participant 1</i> AD,Network, Server Enviroment,Perimeter defence,Email and Exchange	<i>Participant 2</i> Security Services and AD	<i>Participant 3</i> Compliance & M Antivirus & Patcl Managing of IT s
Interview Question 1.1.12 Answers	Why does the ICT department outsource these ICT services? <i>Participant 1</i> Used to do it self, but sold to other companies Cost Saving	<i>Participant 2</i> Specialised functions and financial reasons	<i>Participant 3</i> Cost vs Benefits
Interview Question 1.1.13 Answers	Is there a criteria used to select a suitable ICT vendors? <i>Participant 1</i> Yes,determined by busniness requirements Procurement process in place	<i>Participant 2</i> Supply chain strategy	<i>Participant 3</i> Procurement prc
Interview Question 1.1.14 Answers	Does any of the ICT vendors have access to your systems or networks? <i>Participant 1</i> Yes, They own the network and services	<i>Participant 2</i> No, Access is granted as exception	<i>Participant 3</i> Access remotely Access are alwa
Interview Question 1.1.15 Answers	Is there different levels of access to the systems and networks for ICT vendors? <i>Participant 1</i> Yes, If we own systems we give read and write access Vendors provide service they have full, give use read and write	<i>Participant 2</i> No, Vendor access granted on exception basis	<i>Participant 3</i> Yes, Full access Based on role of

APPENDIX E: SUMMARY OF INTERVIEW RESPONSES

Interview Question 1

- It is clear there is no one single definition
- Participants 1,6 – Exploit vulnerability of IT assets; harm system
- Participants 2,3,9 – Threats to organisational information and systems
- Participants 4,5,10,11,12,16,17 – Inappropriate/unwanted access of data
- Participant 6 – Weakness in control
- Participant 7 – Unintentional and intentional attacks on systems of data
- Participants 8,13 – Incorrect/misleading information
- Participant 14 – Any risk/negative impact on information assets
- Participant 15 – Non controlled effect on network that carries risk

Interview Question 2

- Majority stated information risk management is very important or crucial
- 13 participants agreed and one disagreed

Interview Question 3

- Yes, processes are in place
- Different processes mentioned
- Participant 6 – Not always enforced
- Participant 8, not fully aware of what it is
- Participant 15 – Do not know when they log is the biggest risk

Interview Question 4

- Majority said Yes
- Participant 9 said No/Disagreed
- Depends on access required
- Read to write

Interview Question 5

- Participants 1,2,9 – Ownership and intellectual property
- Participants 3,6,12 – Disclosure of confidential information to 3rd parties
- Participants 4,16 - Unauthorised access and hacking
- Participant 5 – Influence on supplier base and change business model
- Participants 7,17 – Information exploited, exposed, or shared and sold to competitors
- Participants 10,13 – Vendors not complying with information security and requirements
- Participant 11 – Gaining intimate knowledge of business
- Participant 14 – Human factor
- Participant 15 – Proper governance of work

Interview Question 6

- 11 said Yes – Participants 1,2,3,7,8,10,11,13,15,16,17
- 6 said No – Participants 4,5,6,9,12,14
- Participants 1,2,3,7,10,11,13 – Risk meetings and assessments per project
- Participants 8,11,14,17 – Not aware or sure what they are

- Participant 15 – Administrative controls
- Participants 16 – Firewalls and DMZ
- Participants 4 – Overall risk per project
- Participant 5 – Use judgement
- Participant 6 – Working on mechanism
- Participant 9 – Work on trust
- Participant 12 – Not sure

Interview Question 7

- Majority said yes
- 1 said Not sure – Participant 16
- Participants 1,5,9,12,14 – Core systems host by other company; breach them breach us
- Participants 2,6 – Data exfiltration
- Participants 3,4,6,8 – Unauthorised access; lack of escalation procedures; theft of information
- Participant 4 – Viruses and malware
- Participant 7 – Intentional or unintentional attacks on systems
- Participants 10,13,17 – Vendor management and monitoring not adequate; Illegal activities not reviewed or picked up; compliance not monitored
- Participant 11 – Yes, but not part of discussion, at Group level
- Participant 13 – Incompatibilities of technology and processes
- Participant 14 – Outsourcing is first risk
- Participant 15 – Application dis-functionality, loss of data

Interview Question 8

- 16 participants said Yes
- Four methods in place
- Participants 1,6,10 – Internal and assurance audits
- Participant 2 – Data protection strategies implemented
- Participants 3,8,13 – Risk management process with mitigation plan
- Participants 4,7,16 – Access management process and procedures
- Participants 5,9 – Firewall; antivirus; SLA meetings; log files on systems
- Participant 6 – No direct mechanism for dealing with risk of infra outsourcing
- Participants 7,9 – Network monitoring tool; monthly vulnerable assessments; penetration testing
- Participants 12,14 – not sure (ICT Security department at Group level deals with it)
- Participants 15 – Government processes
- Participants 17 – Four types of clearances to view project details

Interview Question 9

- 6 said Yes – Participants 1,2,3,7,8,10
- 4 said No – Participants 6,7,9,12
- 7 said Not sure – Participants (4,5,9,13,14)
- Participants 1,2,3 – SLA agreements
- Participants 4,5,11,12,13,14 – Manage at Group; not sure
- Participant 6 – Security team and processes not mature enough
- Participants 7,10 – Vendors required to provide periodic reporting
- Participant 8 – Audit reviews

- Participant 9 – Protocols now drawn up for security, starting process

Interview Question 10

- Majority said Yes
- 2 said No
- All gave different percentages and some do not know as this happen at Group level

Interview Question 11

- Several services are outsourced
- Participants 1,2,4,5,7,9,11,13,14 – AD; Network infrastructure; Perimeter defense; Email and exchange
Participants 3, 10 – Compliance and Monitoring ICT services; Management of IT systems and workstations in some ODs.
- Participants 5,12 – CCTV maintenance
- Participant 6 – Network and server management
- Participant 8 – IAAS and SAAS
- Participant 12 – Installation of fibre cables
- Participant 17 – Printer maintenance and support

Interview Question 12

- Participants 1,2,9,14 ,15, 17 – Cost saving; used to do it self
- Participant 2 – Specialised functions
- Participants 3, 8 – Cost vs benefit of outsourcing
- Participants 4,5,9,10, 11,12,16 – Shortage of skills and expertise; non-core function
- Participant 5 – Vendors stay ahead of technology; believe it should be in-house and make it core
- Participants 6,7 – Transnet strategy; building capacity in-house
- Participant 10 – Inherit services
- Participant 13 – Not sure why they do it

Interview Question 13

- Yes
- All mentioned a well-documented procurement process
- Participants 1,2,3,6,7,11,14 – Procurement process
- Participants 4 ,5,9,10 – Number of evaluation criteria
- Participant 8 – Do not know what the process is or entail
- Participant 12 – We provide specifications
- Participant 13 – Criteria developed during business case and based on RFP
- Participants 15,17 – Criteria include financial stability and track record
- Participant 16 – Reliability; operating status

Interview Question 14

- 14 said Yes, 3 said No
- Participant 1 – They own network and services
- Participant 2 – No, access granted as exception
- Participant 3 – Via Citrix and logged all times
- Participant 4 – Vendors connect directly to network
- Participant 5 – Remote desktop; longer chain bigger risks

- Participants 6,9,12,14 – VPN, APN, Citrix and LAN (remote access tools)
- Participant 7 – Via access management process; vendor is given a password and username
- Participant 8 – AD Account; Citrix
- Participant 9 – WI-FI
- Participant 10 – Citrix; some part of network
- Participants 11,13 – Direct access (own it) they manage it; Citrix
- Participant 15 – Open to subscribers, but fully controlled
- Participant 16 – No access; send technician to site
- Participant 17 – Fault logging systems

Interview Question 15

- 14 said Yes, 3 said No
- Participant 1 – We own, give read and write; vendors own, they have full access and we read and write
- Participant 2 – No, access granted on exception basis
- Participants 3,5,8,10,11,12,13,14 – Full access to read only; based on vendor role and contract
- Participant 4 – Per application with motivation for access
- Participant 6 – Full access most services/systems; most environments outsourced
- Participant 7 – Based on access required and approved by management; different roles in different systems
- Participant 9 – No, vendors can support and also own the system, then require full access
- Participant 15 – Controlled access to certain vendors
- Participant 16 – No access
- Participant 17 – Only to selected team

Interview Question 16

- 14 Yes, 3 No
- Participants 1,4,6 – Scan for vulnerabilities and changes; rely on SLA and Group security
- Participant 2 – Constant access monitoring
- Participant 3 – Logged on risk register; priority and mitigation for each risk
- Participant 5 – Telling me is risk
- Participants 6,7 – Penetration testing; security assessment audits
- Participant 7 – Access management processes; virus protection software; networking monitoring tools
- Participant 8 – Policies in place; incident response guidelines
- Participants 9,16 – Escalated from Group to OD level; timeframe given to fix; ranking high, low, or medium
- Participant 10 – Per incident response category
- Participant 11 – Controlled at Group level; only get reports
- Participants 12,14,17 – Not sure, at HQ and Group level
- Participant 13 – Risk analyses conducted
- Participant 15 – Fall back processes, multiple back up locations

Interview Question 17

- Majority said Yes
- Participant 1 – No, seen as money waste
- Participants 2,7,8,13 – Information awareness programmes
- Participants 3,4,6,10,12 – Information security awareness programmes; outsourcing and vendor risks not included
- Participant 5 – Workshops on desktop and Internet security; Group deals with security
- Participant 9 – To minimal extend; cost cutting strategy and travel
- Participant 11 – Have briefings but not enough
- Participant 14 – No, done at HQ level

Interview Question 18

- Participant 1 – score 6
- Participants 2,5,9,12,14 – score 10
- Participants 3,4,7,8,10,11,13 – score 8
- Participants 6 – score 9

Interview Question 19

- Majority said No
- Participant 1 – No, long contracts; no exiting condition; build dependency on vendor
- Participant 2 – Yes, internal resourced, upskilled
- Participant 3 – Unsure, cannot answer
- Participant 4 – No, short term plan
- Participant 5 – No, cannot answer; bigger risk handover
- Participant 6 – No, there is none; not enough resources
- Participant 7 – No, but independent assurance in place
- Participant 8 – No, service provider responsible for alternative service
- Participant 9 – No, very costly breakaway and handover long; organisation must have buy back option
- Participant 10 – Yes, contract in place, Dec 2014; vendor manages network, Transnet owns infrastructure; new vendor goes onsite and manages network; not for all vendors
- Participant 11 – Yes, do not know how effective they are
- Participant 12 – No, biggest part of network and infrastructure belongs to vendor
- Participant 13 – Yes, cannot speak of specific plan if happens
- Participant 14 – Do not know and do not want to speculate
- Participant 15 - Yes, contingency plan part of DR strategy
- Participant 16 – Yes, different vendors for same system
- Participant 17 – Not sure

Interview Question 20

- Majority said Yes
- Participants 1,3 – IS 27001,9000; Quality Management Systems
- Participant 2 – 27001/2; COBIT; adopt worldwide standards
- Participant 3- Service delivery; IT risk governance and security
- Participant 4 –ITIL; COBIT; customised internal framework for EIMS/ICT
- Participant 5 – ITIL; not sure which ISO

- Participants 6,12,14 – Not sure
- Participant 7 – ISO, COBIT, ITIL; need to comply with it
- Participant 8 – COBIT and ITIL
- Participants 9,11,12 – Do not know what they are
- Participant 10 – ISO 27001 as information security framework; governance framework based on COBIT and ITIL; maps gaps not covered in minimum control framework
- Participant 13 – COBIT; ISO 27001/2

Interview Question 21

- Majority said Yes
- Participants 1,4 – Yes, base to build on; guide what is required from vendor
- Participant 2 – Yes, common consistency and acceptance
- Participant 3 – Yes, outline control to secure ICT environment
- Participant 5 – Yes, guidance; no need to re-invent wheel; standards to follow
- Participant 6 – Yes, integrate previous learnings and experience; best practice
- Participant 7 – Yes, controlled environment structures to comply with
- Participant 8 – Yes, Guidelines for best practice implementation
- Participant 9 – Yes, help identify threats
- Participant 10 – Yes, controls to effectively manage and monitor risks associated with vendors; if not enforced will not be adequate
- Participants 11,14 – not sure, at Group level
- Participant 12 – Do not know; better management of ICT environment
- Participant 13 – Yes, ensure common baseline and minimum level of security

Interview Question 22

- Majority said Yes
- Participant 1,2,3 – Internal audits
- Participant 4 – No, on exception basis; investigate if there is
- Participant 5 – Contract manager responsible; won't work if they do not comply
- Participant 6 – SLA steering committees; *ad-hoc* audits and assessments
- Participant 7 – Procurement vendor management process
- Participant 8 – Monthly, quarterly and yearly reviews and assessments
- Participant 9 – No, should be monitoring facility
- Participant 10 – Regular audits for high risks vendors; not sure if in place for all vendors
- Participant 11 – Do not have knowledge of how; locally we deal with them
- Participants 12,14 – Not sure, done at Group level
- Participant 13 – Yes, depends what monitored; some issues monitored daily, weekly, monthly; automated tools

Interview Question 23

- 12 said Yes; 2 said No; 3 said Not sure
- Participant 1 – No, does not include sub-contractors, we measure primary and not sub
- Participants 2,3,4,5,7,8,9,15,16 – Condition in primary contract
- Participant 4 – No other tool
- Participant 6 – No, end-user deal with supplier; bypass security
- Participant 10 – Not sure if it exists
- Participant 11 – Yes, but do not know how effective it is

- Participant 12 – Yes, supervision of workmanship
- Participant 13 – Not aware of any specific process or procedures for subs
- Participant 14 – Not sure, sub responsibility of primary
- Participant 15 – Policies in place