RISK MANAGEMENT FOR PORT MANAGEMENT INFORMATION SYSTEMS

by

NTEMBEKO JAFTA

A TREATISE SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE[1]:

MASTER IN BUSINESS ADMINISTRATION

DEGREE IN THE

FACULTY OF BUSINESS AND ECONOMIC SCIENCES

AT THE

Nelson Mandela University

SUPERVISOR: DR JESSICA FRASER

2018

[1] See Appendix C

DECLARATION[2]

I, Ntembeko Jafta, Student Number 205045928, hereby declare that the treatise for the Master in Business Administration is my own work and that it has not been previously submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

_____

NTEMBEKO JAFTA

[2] Turnitin report on Appendix D.

ACKNOWLEDGEMENTS

Thank you to all who have supported me towards the successful completion of this study. Special thanks to the participants in the study for their prompt responses, and for providing me with the data needed to complete this study.

To my parents and my in-laws: thank you for your support, motivation and understanding throughout my MBA journey. Most especially to my wife, Nwabisa Bianca Jafta: thank you for always believing in me. You always knew what I needed, and what to say when I felt like giving up. You are truly the best!
To my friends: I appreciate your encouraging words and support when at times the task seemed impossible to complete. You gave me strength to push through.

A special thank you to my supervisor, Dr Jessica Fraser, for her guidance and supervision. Thank you for your patience and understanding, for encouraging me towards quality and excellence at all times. I will carry your teachings with me through all my future endeavours.

To the friends that I gained in the MBA programme: I could not have asked for better people to walk this journey with me. You made the journey enjoyable. I know that I have gained lifetime friends. Special appreciation to Ms Yolisa Sonti for her support and encouragement.

Most of all I acknowledge and thank God, without whom this project would not be possible. I acknowledge your blessings, and for giving me the mind, body and strength to learn, explore and go beyond my limits.

ABSTRACT

Port Management Information Systems (Port MIS) are systems that support port managers in the facilitation of port activities. However, little is known about the system and the risk that it presents. Much information is exposed, and security needs to be strengthened. Port MIS helps managers to make decisions relating to the activities that enable effective management and leadership of the port. Inadequate and poor risk management would lead to loss of business and potential loss of human life. This research study focused on the subsystems that make up Port MIS. There is limited research on port management, and more specifically the risks involved in such national assets. The study explored the purpose of such systems and how they contribute to the whole system. The findings and recommendations would benefit port managers both nationally and internationally as globalisation becomes the basis of world trade and economies.

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

CHAPTER 1: INTRODUCTION AND PROBLEM STATEMENT

1.1 INTRODUCTION

The sea has always been a major means of trade between countries, resulting in the establishment of ports all over the world. Ports are important in the facilitation of the importing and exporting of goods to and from a country, and South Africa (SA) is no exception. This can been seen by the number of ports that SA has across the coastline of the country. Transnet (Pty) LTD, a parastatal of the government of South Africa, operates eight commercial ports. The South African ports are not very different to any developed country's ports, since they also utilise information systems. Information systems, such as the Port Management Information System, help to ensure effective communication to avoid time being wasted (Abbes, 2015).

Port Managers use the port Management Information Systems for communication and to avoid wasting time using manual procedures. The literature review conducted revealed that Management Information Systems (MIS) have no single theoretical background, similar to that of the Port Management Information Systems (Port MIS) which also does not have any notable definition. These terms refer to a broad class of conceptual frameworks that have been developed to understand and explain the design, use, administration and concerns of information systems for management use (Majchrzak and Markus, n.d.). There are, however, risks to blindly relying on such systems and if they are not continuously monitored and assessed, they have the potential to cause much damage.

A seaport, traditionally a place of articulation among transportation systems, is logically a place for the convergence of numerous information flows, all of which are contained within the Port Management Information Systems. In addition to the requirement for security and speed; reliability on delivery time and frequency of service are of fundamental importance to all port users. This becomes an obligation that management needs to provide (Abbes, 2015).The Port MIS needs to have security features that include management of risk, amongst other aspects. This is critical as it has such a high volume of information that flows through it, making it vulnerable to exposure and negative interference.

Chapter One of this study on the Port MIS provides the problem statement that forms the crux of the investigation. The research objectives follow, addressing the purpose of the study. These objectives are rephrased into questions which interrogate the research problem. More light is shed on the research objectives through the research methodology, and through an overview of how the literature review was conducted. A glossary of terms is also provided to give perspective on the terms used in this treatise. Chapter One closes with an outline of forthcoming chapters and an overview of the content presented.

1.2 STATEMENT OF THE PROBLEM

Port MIS are associated with Management Information Systems. They are used specifically at sea ports for the purpose of supporting management. Management Information Systems are computer information systems that collect and process information from different sources in an organization, assisting management at all decision-making levels (Al-mamary, Shamsuddin & Aziati, 2014).

The Port MIS helps the managers of a port to make informed decisions by collecting information from different levels of the organisation. The Port MIS provides management with an opportunity to evaluate their vulnerability to risk, thus assisting management with their decision-making (Kumar & Singh, 2015). Security was identified as a concern because of inflow of information from many sources. The result is that port terminals have an increasing dependency upon technology, and automation has clearly brought considerable economic benefit. However, this dependency also introduces vulnerability. Any loss of availability, integrity and confidentiality related to critical systems or data has the potential to cause significant business disruption, with consequent financial loss. As the sophistication of malignant targeted attacks increase, so must efforts to contain and respond to the threat (Marsh, 2014).

The above threats to MIS confirm the need to have all risks and vulnerabilities managed. This applies to the operations of a port and its systems as well. A proposed solution is Risk Management, which is defined as the process of identifying and assessing risk, and to apply methods to reduce risk to an acceptable extent (Serpella, Ferrada, Howard & Rubio, 2014). Thus, in order to have the port activities operational

despite the prevalent potential risks, the Risk Management of Port Management Information Systems should be investigated and updated on a regular basis. Such Risk Management is the focus of this study.

The research problem stated is explored by seeking answers to a set of research questions.

1.3 THE RESEARCH QUESTIONS

The above-mentioned problem statement led to the following research questions:
RQ1: What are the risks that apply to information systems such as the Port MIS?
RQ2: What are prevalent risk assessment methods?
RQ3: What are the effects of risk on Port MIS and subsystems?
RQ 4: What is the importance of risk assessment?
RQ5: What is the importance of risk management?
RQ6: Do all eight ports in South Africa attach the same level of importance to risk assessment for their Port MIS?
RQ 7: How can a risk management strategy be standardised for all eight ports?

1.4 THE RESEARCH OBJECTIVES

The primary objective of this study is to explore the effect of managing risk within Port Management Information Systems.
The secondary research objectives for this study follow:
RO1: To understand the role of Port MIS and subsystems, and the risks they face.
RO2: To investigate risk assessment methods.
RO3: To determine the effects of risk prevalent within information systems such as the Port MIS.
RO4: To investigate the importance of risk assessment methods.
RO5: To explain the importance of Risk Management Systems such as the Port MIS.
RO6: To conduct a survey to evaluate how port users perceive risk management.
RO7: To determine the standardisation of a Risk Management Strategy for Port MIS that would be applicable to all eight ports.

1.5 THE METHODOLOGY OF THE STUDY

To achieve the above-mentioned primary objective, the following methodology was used:

(i) An extensive literature review was conducted on risk management strategies, Port Management Information Systems and the risks prevalent to such information systems.

(ii) A questionnaire (see Appendix B) was developed to measure the above-mentioned variables.

(iii) The questionnaire was emailed to personnel who use Port MIS across the ports of South Africa.

(v) The responses from the sample group were recorded and the empirical results analysed.

(vi) Based on the results, conclusions were drawn; recommendations for port managers suggested and gaps for future research identified.

1.5.1 The research study approach

The study was conducted using a mix of both qualitative and quantitative methodologies. The qualitative study included the literature review on both Risk Management and Port MIS. The review covered the use Port Management Information Systems and subsystems and their associated risks. The review also included the role played by Port MIS in supporting the management team in their decision making. The study investigated the benefits of Risk Management methods on Port MIS. The quantitative study included the questionnaire sent to the respondents on how they managed risks relating to Port MIS.

1.5.2 Sampling design

This study focused on Transnet Port Management information system end users. The users included lower to mid-level managers who interact with Transnet's Port Management Information System. A sample of at most 30 users around the country were targeted by the questionnaire, which was sent internally to Transnet (Pty) Ltd Respondents had to reply via an e-mailed link. They had to complete the online questionnaire and their responses were automatically recorded.

1.5.3 The measuring instrument

The questions on the questionnaires were measured against the Likert Scale, where the respondents had to give a response ranging from “Strongly disagree to Strongly agree” on statements which probed the research questions.

1.5.4 Data analysis

The data collated from the respondents was summarised and analysed using descriptive statistical methods to find the most common responses to the research questions. Further analysis was done to find relationships within the findings that helped to better understand the research objectives.

1.5.5 Ethics clearance

The completed Ethics Clearance form was submitted to the Nelson Mandela University Business School for their approval. The group of respondents did not qualify as a vulnerable group, such as schoolchildren, thus a full ethics clearance did not apply. The approved Form E is attached as Appendix A.

1.6 TERMINOLOGY/ ACRONYMS

IT	Information Technology
AIS	Automatic Identification System
DOS	Denial of Service
DR	Disaster Recovery
FM	Facilities Management
FPIC	Fixed Priced Incentive Contracts
GAM	Guaranteed Annual Minimum
ICT	Information Communication Technology
IP	Intellectual Property
IS	Information Systems
ISMS	Integrated Ship Management Systems.
MIS	Management Information Systems
NRTSAPD	Near Real Time Statistical Asset Priority Driven
Port MIS/PMIS	Port Management Information Systems
VBS	Vehicle Booking System
VPIC	Variable Priced Incentive Contracts

1.7 OUTLINE OF THE STUDY

Chapter 1

Chapter 1 presents a brief outline of the study. The management question or problem, and the basic research methodology are reviewed. The study approach, which includes both qualitative and quantitative methods, was also introduced.

Chapter 2

Chapter 2 includes the literature review on risk management of information systems, such as Port Management Information Systems. An in-depth review of available research studies was done on the benefits of understating risk to Information Systems like the Port Management Information Systems. The focus was on their impact on systems and how they should be addressed as a management problem.

Chapter 3

Chapter 3 focused on subsystems that make up the Port MIS as a system. Each subsystem was independently reviewed to identify what it contributed to the overall system.

Chapter 4

Chapter 4 discusses the research methodology and approach adopted for this study.

Chapter 5

Chapter 5 presents the data analysis that was conducted to address the research questions. Statistical methods were applied to the data collected from the respondents to see if there was any correlation between the research objectives and the findings.

Chapter 6

Chapter 6 is a summary of the study and presents an overview of the management question, literature review, research methodology and the data analysis. The management question is addressed and recommendations are made. The future prospects of research gaps are identified and discussed.

1.8 SUMMARY

Chapter 1 identified the concepts of Port MIS and the risks prevalent to such systems. The secondary research questions and objectives related to the primary research purpose, questions and objectives were provided. The methodology was clarified, and the qualitative and quantitative nature of the study. Chapter outlines followed, giving a holistic perspective of the study.

CHAPTER 2

PORT MIS RISK MANAGEMENT

2.1 INTRODUCTION

In every country that has a coastline, there is always a port or ports for the import and export of goods. The port will have managers using information systems to support its operations. This study is about the management information systems that support the operations of the port. However, management information systems as part of organisations pose risks that have to be managed.

Risk Management of Port Management Information Systems (Port-MIS) is the focus of this study. Port-MIS and what it is used for are briefly discussed. Common risks in information systems such as Port-MIS are explored, as well as how the risks should be assessed and how to identify the types of risks that exist. The study goes on to identify different types of risk assessment methods that are predominantly used on information systems such as Port- MIS. The chapter closes with a summary of the benefits of Risk Management for Port-MIS.

2.2 OVERVIEW OF PORT-MIS

Management Information Systems (MIS) is a term used to describe a specific category of information system that serves middle management. The systems serve to give middle managers knowledge of the operations of the business (Laudon & Laudon, 2010). Port Management Information Systems (Port-MIS) is a kind of management support information system that helps with the arrival/departure processes of ships (Park et al., 2005). Čišić & Tijan (2011) see it as a system that the Port Authority needs in its operations. It provides information that allows for the supervision of the overall activities of the seaport, enabling managers to make well-timed and accurate decisions (Čišić & Tijan, 2011).

Port MIS is defined as an “electronic system that handles administrative procedures of vessel and cargo movements, inside the port ” (Keceli, Choi, Cha, Aydogdu & Kim, 2008). The computerised system has five major modules, namely Cargo Control, Vessel Control, Port Facilities, Billing and Statistics as depicted in Figure 2.1 below.

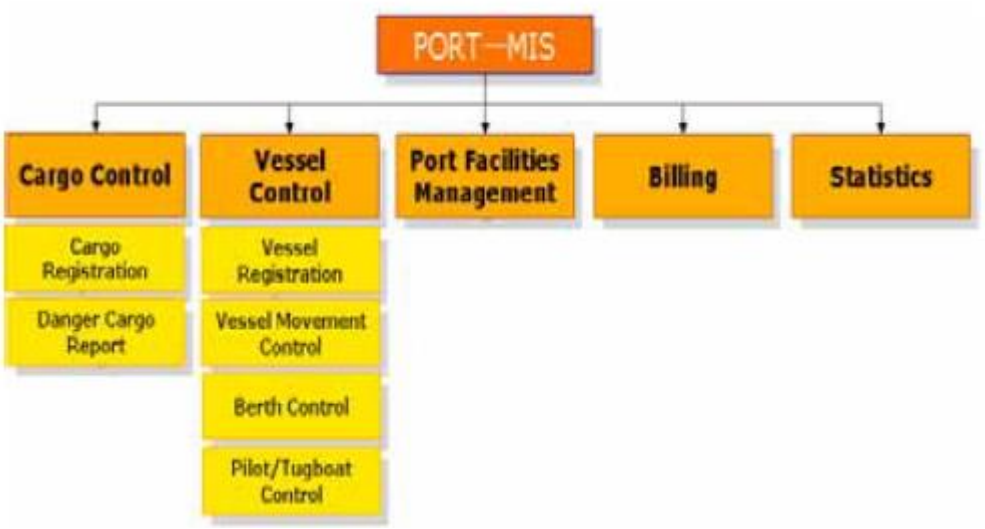


Figure 2.1: Port MIS overview

Source: (Keceli et al., 2008:167)

From the definition, it is evident that a Port MIS is a critical system to the operations of the port, and thus risk associated with it must be managed. It is also critical in supporting the operations performed by managers. It provides the statistical activities about the operations at the port. Port MIS has cargo registration details, as well as information of the cargo being carried by the vessels. This information needs to be protected from risks. Port-MIS has therefore to have risks assessed and managed in case of risks that might threaten it. Managers have to ensure that their division has effective processes in place to handle the risks.

The literature review exposed that organisations allocate a larger budget for Information Technology (IT) security because of the greater threat posed by IT. This confirms the importance of Port-MIS risk management, and why the active practice of risk management methods would aid port managers to classify the controls desirable to conserve IT to counter risk (Tohidi, 2011). Risk management is clearly critical, hence the huge funds that are allocated to them.

The nature of risk need to be understood, what forms they come in and how they endanger Port-MIS. The next section discusses these factors.

2.3 THE NATURE OF RISK

In order to discuss the nature of risk, one has to first understand what risk is. According to the Oxford dictionary, risk is defined as: “A person or thing regarded as a threat or likely source of danger” (Oxford University, 2016b). Wiesche et al., (2013) defined risk in information systems, which would include Port MIS, as “any threat that may lead to the improper modification, destruction, theft, or lack of availability of IT assets” (Wiesche, Keskinov, Scherman, & Kremar, 2013). The definitions show that risks are threats that lead to undesirable consequences, such as danger to and destruction of the assets of an organisation.

Risks are known to be internal or external. Internal risks are known as Endogenous Risk. External risks are known as Exogenous Risk. Their nature is classed into these two categories.

Exogenous Risks refers to those risks that an organisation has no hold over and are not caused by activities within an organisation. Unanticipated tragedies such as floods and earthquakes are Exogenous risks (Chou & Chou, 2009). Nehari–Talet et.al. (2014) saw Exogenous Risks as those over which organisations have no control, and which are not a result of internal activities. Hurricanes and earthquakes are worthy examples of Exogenous Risk. While there is approximate control on the amount of damage these examples can cause by choosing specific construction standards, there is actually no control over the existence of such unexpected events (Nehari Talet, Mat-Zin, & Houari, 2014).

Endogenous Risk arises from within the organisation. An example would be unanticipated resistance by users, vagueness concerning the cost of workers’ turnover, the risk of commitment escalation and repair costs in the long execution process (Rajnoha, Kádárová, Sujová, & Kádár, 2014). Chou and Chou extend on the same explanation of Endogenous Risks, by saying they refer to those risks that are reliant on actions inside the organisation. They are also risks that enter an organisation through outsource contracting. Outsource contracting also falls under Endogenous Risk (Chou & Chou, 2009).

The distinction found between the two natures of risk was that Exogenous Risk are risks from natural causes; the organisation expects them but has no control over when and how they would happen. Endogenous Risk comes from within the organisation; they result from association and processes inside the organisation, including outsourcing. The above risks are likely to happen on the Port MIS, hence the justification for this study. The next section discusses the risks in Port MIS.

2.4 RISKS IN PORT MIS

Port MIS is a management information system, as already defined. A Management Information System (MIS) is described as an information system used in management and business (Kitagaki & Hikita, 2007). MIS on its own is an information system built specifically for business and management.

Information systems are made up of many components. Figure 2.2 discusses the components of the information system.

Data	Input that the system takes to produce information
Hardware	A computer and its peripheral equipment: input, output, and storage devices; hardware also includes data communication equipment
Software	Sets of instructions that tell the computer how to take data in, how to process it, how to display information, and how to store data and information
Telecommunications	Hardware and software that facilitate fast transmission and reception of text, pictures, sound, and animation in the form of electronic data
People	Information systems professionals and users who analyze organizational information needs, design and construct information systems, write computer programs, operate the hardware, and maintain software
Procedures	Rules for achieving optimal and secure operations in data processing; procedures include priorities in dispensing software applications and security measures

Figure 2.2: Components of an Information System (IS)

Source: (Oz, 2009:15)

The Port-MIS as an information system has data, hardware, software, telecommunications, people and procedures as explained above. The above

components of the system are at risk of threats, as is the system itself. It is thus essential to identify all potential threats to an organisation that uses Port-MIS.

Threats to Port-MIS may originate within and are termed Insider Threats. Insider Threats are individuals or people who have access to the system, or who used to have access to the system, and their purpose is to cause harm to the organisation (Bertino, 2012). Such threats to Port MIS are risks that needs to be managed. Threats to assets exist within, and yet can come from external sources at times. This motivates organisations to install innovative software systems and hardware for guarding against possible attack from outsiders and insiders.

Organisations form numerous information security policies and procedures to help against risks. These policies help to decrease and prevent planned or unintentional actions of staffs that could either deteriorate the efficiency of the hardware and/ or software protection systems that could reduce their usefulness (Hu, Dinev, Hart & Cooke, 2012).

IT threats on the information technology assets of an organisation are clearly a valid concern. However, in the study of IT, risk addresses different matters when extended to software projects, IT security, outsourcing of information systems, e-commerce and inter-organisational systems, to mention a few other components of IS (Wiesche et al., 2013). This means that risks within information systems are broad, and not limited to a specific type of system. The only typical form of system deployment (as outsourcing) has already been mentioned. This study looks into the Risk Management of Port MIS, whether it is outsourced systems or an inter-organisational system.

According to Sherer (2004), there are different types of risks from an information systems technology perspective. He outlines the different risks as follows:

- Technical risks that have to do with information systems.
- Project risks that are relevant to the development of the system.
- Organisational/ Political risks that have to do with the organisational structure or politics.
- Financial risks.
- Systematic disaster risks (Sherer, 2004).

The malicious damage caused by people from within differs from the individuals that have access to the system. The Insider Threats differentiation is outlined in Table 2.1 below, which illustrates how to identify each threat.

Name	Distinguishing Indicators/Anomalies
Saboteur	• Indicators: URL; File; Logon • Anomalies: File accesses in relation to peer group in LDAP
Intellectual Property (IP) Thief-Ambitious Leader	• Indicators: URL; File; Printer; Login; Email • Anomalies: File accesses and email communication graph in relation to peer group (manager) in LDAP
Intellectual Property (IP) Thief-Entitled Individual	• Indicators: URL; File; Printer; Login; Email • Anomalies: File accesses compared to peer group (technical) in LDAP
Fraudster	• Indicators: Login; processes; files; and URL • Anomalies: Email and URL compared to groups (non-technical)
Careless User	• Indicators: File, Email, URL, Process • Anomalies: Processes run compared to user and LDAP (function) group
Rager	• Indicators: Email, IM, Login • Anomalies: sentiment and topics in emails sent

Table 2.1 : Insider Threats Scenario

(Senator et al., 2013:3) & (Goldberg, Young, Reardon, Phillips, & Senator, 2017:2650)

A ‘Saboteur’ is an individual or group who is likely to cause interruptions on the shared resources of a computer network (Samson, 2015)**.** The distinguishing indicators are anomalies such as URL, file and logon, along with file accesses with relation to peers (Senator et al., 2013)**.**

A ‘Fraudster’ is an individual inside the organisation who uses IT for personal gain or to compel criminality. Fraudsters are not the only threat, because there are also thieves. Within the arcade of thieves would be an Ambitious Leader and an entitled thief: The Ambitious Leader would be responsible for organising other insiders to get admission to all parts of the Intellectual Property (IP) being embezzled. They are also

a cause of great loss, based on how much proper planning goes into their actions. Their actions are usually for the following reasons:

- 43% of the time it is for the creation of a new organisation.
- 43 % of the time it is for liaising with a rival business.

(Moore et al., 2011)

The thieves are a threat because of what they could do with the Intellectual Property (IP) that they steal. This could mean that an organisation has to be very careful with their IP. Users of the organisation's IT resources have to be as careful. Careless users could lead to the loss of IP if there are thieves amongst them, or if a thief is intent on stealing IP. The careless user is an insider who is not knowingly deceitful, but is an individual who disregards corporate IT policies, thus exposing the business to risk.

A 'Rager' is an insider who has outbreaks of robust or threatening language usage in mail/Webmail/IM when corresponding with anomalies in other activities, indicating a potential fundamental change in behaviour. A particular detector specification is found in the emails as an indicator of such behaviour (Nehari Talet et al., 2014)**.** The above threats are different type of IS threats that can arise from its components.

Telecommunication threats are those made to the infrastructure that is used to communicate within the port and Port-MIS infrastructure. The threats come in the form of terror attacks, technological threats, criminal attacks and general threats (Agubor and Chukwudebe, 2015).

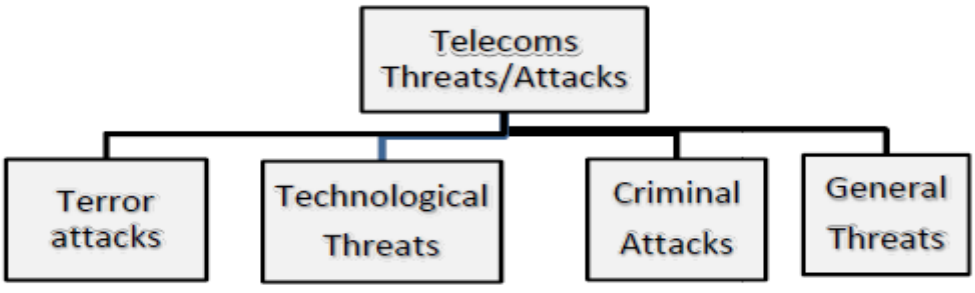


Figure 2.3 : Telecommunication threats /attacks

(Agubor & Chukwudebe, 2015:125)

The above Figure 2.3 are attacks that would likely be on the Telecommunication system of the Port MIS.

‘Terror attacks’ are broad in scope, and could be understood to be an act of war. The definition of terror attacks relating to IS are best described as the intention to conduct the act and to influence or intimidate the government or population; having some form of political, religious or ideological motive or purpose, and the cause of harm, death or bodily injury (Al Mazari, Anjariny, Habib, & Nyakwende, 2016).

‘Technological attacks’ are focused on the user’s computer or internet connection by someone other than the person using the computer. They are focused on pharming, with the intent being to attack system reconfigurations (Chaudhry, Chaudhry & Rittenhouse, 2016). Telecommunication systems face such risks and the ideal would be to change the systems’ configuration.

‘Criminal Attacks’ are best described as a cyber-crime that is not carried out for a political or national security purpose, such as most instances of internet fraud, identity theft and intellectual property piracy (Hathaway et al., 2012).

‘General threats’ are attacks on routing protocols which include replaying, spoofing or altering routing traffic (Raymond & Midkiff, 2008). Changing traffic of the intended data could be a means of depriving the original receiver of the message intended for them. These are threats that pose a risk to an Information System (IS) like the Port-MIS. These can go undetected unless mechanisms are put in place to detect the threats.

Different techniques can be used to detect threats. Table 2.2 has a summary of the different approaches to detect threats on the Port MIS system. Each approach has its own pros and cons. The summary includes which approaches should be used to detect threats to Port MIS.

Classification of approaches	Pros	Cons
Intrusion-detection-based approaches	A large pool of existing techniques	• Not as efficient for large amounts of log across multiple systems • High rate of false positive • Only detect specific attacks • Do not detect insider intrusion that do not leave traces
System-call-based approaches	More difficult for intruders to intrude without leaving evidence	• Number of false alarms is too high to deploy in practice • Variations in access behavior of users weaken their effectiveness
Data-centric approaches	Minimize the actual amount of data that needs to be processed	• It is not clear how to partition data into clusters that may have hidden patterns
Honeypot approaches	Provide early warning or deter attacks; useful in detecting new exploits	• Simply moving a honeypot from an external network to the internal network will not detect malicious insiders. A new strategy to deploy honeypots is required.
Dynamical-system-theory-based approaches	Detect insider malicious threats before an attack occurs	• Accuracy of user profiles is crucial
Anti-indirect-exfiltration approaches	Identify potential developer actions which may result in long view threats	• Evaluation of the effectiveness of these approaches are currently unavailable • Impact on normal operation unavailable
Visualization approaches	Visually identify unusual patterns as insider threats	• Difficult to process large amounts of data • Analyzing and understanding insider threats after applying visualization techniques is difficult

Table 2.2 : Threat Detection Approaches

Source: (Zeadally, Yu, Jeong, & Liang, 2012:8)

The above assumes a system within the organisation. It does not include the system within the other company's premises. The next section discusses the system at the other company. This leads to the risk of outsourcing of the Port MIS.

2.5 RISK OF OUTSOURCING PORT MIS

Outsourcing of information systems has experienced considerable growth in recent years as it has become an elementary strategy of the IS field. Analysts foresee that outsourcing will be ongoing, as the motive for outsourcing is that an organisation partners with another strategic organisation that can provide them with IT systems to help their business. They then offer them incentives for taking the risks (Gonzalez, Gasco & Llopis, 2006).

It is likely that an information system like the Port-MIS would be outsourced to another company. Both organisations would form strategic partners who would be compensated for their purpose and role.

The outsourcing company can offer two key categories of incentive contracts to another establishment or business. The contracts offered by the outsourcer are found to be no changing Fixed Price Incentive Contracts (FPIC) and changing Variable Price Incentive Contracts (VPIC), (Chou & Chou, 2009). In an FPIC, a pre-arranged price is rewarded to the service provider, who takes on responsibility for all the potential cost overruns. A service provider can participate in opportunistic bargaining. This means that it may burden the customer to recompense the overruns if they hold the unique advantage of being the only service provider, and when the option of switching is not possible (Zhang & Xu, 2017).

An FPIC is a kind of contract where the charges for information handling are definite, but the information processing costs remain inexact (Osei-Bryson & Ngwenyama, 2006).The contracts both have an enticement and a penalty endowment. The contracts may vary in management of the risks if the vendor under-performs. It should be noted that this is in itself a risk that an organisation takes when it underperforms (Chou & Chou, 2009). Information systems, such as the Port-MIS, are open to risk and ambiguity when they outsource their projects, which limits the gamble of outsourcing becoming a success. This is in addition to service and management related risk matters (Osei-Bryson & Ngwenyama, 2006).

Significant loss of control over the performance of activities by an organisation is another result of it contracting out its information processing operations. There are two basic risks associated with this loss of control: these are known as shirking and opportunistic bargaining. A deliberate underperformance while claiming full payment is known to be ‘Shirking’, and comes in a variety of forms. In essence, it involves a vendor or an agent doing less work than mandatory, less work than contracted for, and less work than compensated for. Shirking refers to the agent's commitment to work hard, which would not be the same as the client’s. The absence of information available to the outsourcer makes it challenging or difficult to ascertain shirking (Aron, Clemons, & Reddi, 2005).

Opportunistic bargaining refers to a merchant's capability to ask for higher than market prices. Exposure to opportunistic bargaining is when an outsourcer is tied-into a vendor inclusively, and would have to pay substantial charges to change to an alternative. To minimise shirking risks, the outsourcer can participate in checking and managing mechanisms. The two are accomplished by outsourcers setting up a unit within the organisation that manages the relations concerning the vendor and end-users. This is done to observe the vendors' performance and manage the risks of the outsourced project (Osei-Bryson & Ngwenyama, 2006).

The next section discusses how risks are assessed.

2.6 RISK ASSESSMENT

Risk analysis methods can be quantitative or qualitative. Quantitative risk analysis methods analyse risk using mathematical and statistical tools (Alberts & Stevens, 2003; Karabacak & Sogukpinar, 2005). According to Karacback & Sogukpinar, quantitative measures as a method of risk analysis are not appropriate for current information security risk analysis. Compared to the past, current information systems have a more complex structure. Compound scenarios are difficult to solve, and the calculations that come as a result of this are complex (Karabacak & Sogukpinar, 2005).

Qualitative risk assessment methods are based on decision, instinct and the knowledge of the assessor. The use of assessments by assigning the likelihoods and consequences of risk are more flexible when dealing with diverse situations of risk (Lo & Chen, 2012). The risk analysis methods could be computer or paper based (Karabacak & Sogukpinar, 2005).

Alberts & Stevens (2003) suggest that an organisation should comprehend and protect its information security needs by applying a risk analysis method called OCTAVE. OCTAVE is labelled as a risk based strategic assessment and planning technique for security that is self-directed. This means that within the organisation there should be an initiative to set its security strategy (Alberts & Stevens, 2003) .

The OCTAVE method is different from other approaches, as depicted in the Table 2.3 below. It is an analysis approach that looks at the organisation's risk analysis from within the organisation.

OCTAVE	Other Evaluations
Organization evaluation	System evaluation
Focus on security practices	Focus on technology
Strategic issues	Tactical issues
Self direction	Expert led

Table 2.3 : Octave vs Other Approaches

(Alberts & Stevens, 2003:4)

The Near Real Time Statistical Asset Priority Driven (NRTSAPD) Risk Assessment method explores risk analysis over a period. The method considers critical elements when assessing the risks of the information system. The method is valued because it offers an advantage over other risk assessments in that it gives management a quick, easy to use and simple risk assessment methodology. It is based on an organisational mission critical asset priority (Pak, 2008).

The NRTSAPD as a quantitative method works through various elements in relation to risks. It gives them weights to determine the level of risk that the organisation is exposed to, and views their impact on the overall risk assessment calculation outcome. The calculation has the elements presented below.

Pak (2008) focuses on the following elements in his calculations:

1. Frequency of the Attacks – This element accounts for 10% and is the most critical. It accounts for the number of attacks that were made on the system.
2. Probability of being attacked again - This element accounts also for 10%. An assessor can give a score founded on the present environmental situations and how likely a threat would be repeated within an organisation.

3. Total Replacement Value - The monetary value element refers to the amount of harm a threat could do to the information system of an organisation. The factor weighs 20% of the assessment calculation.
4. Exposure Rating - The element of the assessment calculation has a risk factor of 5% and it is about assessing the likelihood of a threat on a Likert Scale of 1-5.1 will mean low, and 5 will be a high risk factor.
5. Estimated Risk Rating - A risk factor of 5% is given for this risk assessment calculation. The assessment is done on a scale of 0 -100. This is used to evaluate the risk when identified, its vulnerability and how it can be minimised further.
6. Impact Category Level - The Impact Category Level on Denial of Service (DOS), Modification, Disclosure or Destruction is evaluated on a scale of 1 to 4. The impact categories of Denial of Service, Modification, Disclosure or Destruction contribute to 10% of the weighted risk assessment analysis. When a threat is realised, its impact on the organisation is categorised by the nature of the attack. If the attack was to cause a DOS, the impact score of 1 is assigned.
7. Number of Customers Affected - The number of customers affected also contributes to the total risk calculation on a weighted risk factor of 10%. When a security incident occurs, the organisation should be concerned over its customers' ability to access the business processing network. The larger number of customers affected, the more serious is the impact of the threat.
8. Incident Response Time - The Incident Response Time to act on a reported incident is measured on a scale of (1-10), and contributes a weighted risk factor of 5% to the total calculation. The response team reacts to a security incident to contain and mitigate it. The longer time the response team takes to mitigate the incident, the more critical will be the impact to the business mission.
9. Business Impact level - The Business Impact Level to the organisation's business mission can be measured as low, medium or high. This is used on a weighted risk factor of 25%. When a threat agent exploits vulnerabilities, the organisation can experience a severe impact on the organisational business goals. The impact on the organisational assets depend on its criticality to the organisational business goals (Pak, 2008).

Pak's assessment model gives a perspective of what the whole organisation could be exposed to and the effect on the overall risk levels. This could be utilised to look at

the risk of the organisation holistically, without leaving to chance the internal and external stakeholders. Port-MIS can be assessed using such a method without having an expert on the systems risk factors.

2.7 OVERVIEW OF RISK MANAGEMENT AND PORT MIS

Management is “The process of dealing with or controlling things or people; the responsibility for and control of a company or organisation ”(Oxford University, 2016a). Risk is seen as anything that has the potential to cause damage or danger to organisational assets (Oxford University, 2016b).

Ntouskas and Polemi (2010) define Risk Management as a continuous process of recognising examining, handling, monitoring and reporting on the active risks of an organisation. Risk Management is seen as an important administrative and governance goal of an organisation, aimed at protection of the organisation within and outside from risks that would affect the achievement of its goals negatively (Ntouskas & Polemi, 2010).

Risk management is a process comprising the following steps: risk identification, risk analysis, risk planning and risk monitoring (Höst & Lindholm, 2007). It provides an actual method of assessing safety through risk assessment, mitigation and evaluation. Existing risk management methods are well recognised. However, it requires more precise and detailed understanding of the IT security territory along the establishment background (Ekelhart, Fenz & Neubauer, 2009)**.**

Risk management is known to be an organised method. It is a process of handling security through risk assessment, then devising plans to manage and mitigate risk using managerial resources. Strategies include giving the risk to a third party or hiding the risk. This could include limiting the negative consequences of the risk, and accepting some or all of the consequences of a particular risk. Risk could be the result of security threats, property value threats, threats that influence probability, property exposure to threats, threat influence on property or organisations and prevailing security threats (Jackson, 2008).

Risk can be limited by enforcing one or more controls on a specific step in the processes of the business. Controls could be a specific technology that limits access

to an organisation's premises; it could also be a procedure to complete a specific task in the organisational information assets. They are significantly different in reliability in terms of preventing fraudulent activities from system to system within an organisation. The controls are generic in their approach, which means they should be customised to each unique organisational set of systems (Rolland, Ulmer & Patterson, 2014).

Effective use of risk management processes would assist managers to recognise the controls needed to sustain IT factors. However, for this reason a significant number of organisations assign enormous funds for IT security (Tohidi, 2011). Risk management is costly to an organisation, but is critically needed.

Figure 2.4: Corporate IT Risk Management Model

Source: (Spremiü, 2012:300)

Spremiü (2012) presented Figure 2.4 as a holistic model for management corporate IT risks. The model includes business drivers, corporate governance policies, procedures and operational risks. According to Spremiu (2012), the following is an explanatory summary of a Corporate IT Risk Management Model:

- Business drivers have to be in line with corporate objectives; they should be regulatory requirements that are approved by the highest corporate structures. The lack of such support could put the organisation at great risk.
- Corporate governance policies for managing IT risks are obligatory in all business echelons, and approved by the corporate executive structures. They entail the establishment of various committees responsible for plans used for regulatory compliance and adoption of the industry best practice.
- Procedures for managing IT risks on a business unit level, or functional level, should follow standards and norms set by international regulatory bodies.
- Operational activities must be guided by management procedures and governance policies that characterise the defence mechanisms against threat, with the intention to increase the level of defence on attacks and threats to IT resources (Spremiü, 2012).

2.8 DISASTER RECOVER AND RISK MANAGEMENT

Disasters happen all the time. However, numerous establishments are caught unaware or they make unrealistic assumptions about disasters. The reasons they submit are known as the myths that organisations make. Disaster comes in different formats or types. Some known disaster types are presented below (Landry & Koger, 2006).

i) Natural Disasters

Natural disasters happen. They cannot be predicted or prohibited from happening. Known examples are hurricanes, floods, tornadoes, earthquakes and snow storms. Their capabilities destroy a massive amount of physical assets. These disasters will not happen at all business locations, but only in specific areas of the world.

ii) Technical Disasters

Technical disasters are events that occur from hardware or software failure. Software failure resulting in information damage is the most important loss through technical disasters. The natural disasters cause some physical damage to the organisation, like the hardware needing to be replaced after the event.

iii) Human-Made Disasters

Human disaster is destruction caused by an employee, former employee or an external person. The idea is to do both physical and information destruction. Some reasons for causing such disaster is through employee negligence, or perhaps corporate sabotage by another organisation. Trained or untrained employees can accidently, or deliberately, abolish physical resources while capturing incorrect information. This can cause costly errors that will be detrimental to the organisation's success. In corporate sabotage, a competitor could be causing the destruction of an opponent's physical location, or by launching cyber-attacks that could lead to information theft or loss (Vuong, 2015) .

Despite the above known disasters, organisations still make assumptions about how to recover. Landry & Koger (2006) outlined the myths surrounding the management of threats for an organisation, especially one like the Port MIS.

Myth 1: The only disasters to plan for are natural disasters.

Threats such as tornadoes, floods, blizzards, fires, earthquakes, tropical storms, hurricanes, mudslides, tsunami and volcanic eruptions do happen. There also needs to be a plan for the loss of human life as well.

Myth 2: A mock test really tests disaster recovery.

Any plan that has never been fully tested is useless: so the Port MIS recovery plans need to be regularly tested.

Myth 3: Attacks and hacks are only external threats.

Endogenous threats, as explained, are employees within an organisation that can be the source of deliberate or unplanned attacks on corporate assets. Endogenous threats are overwhelming. Exogenous threats are rooted in the quick access to local internet resources like the intranet, and the fact that most organisations feel relaxed about the use of the computer stations by their employees. The Port MIS has to have restrictions, as well as within the organisation.

Myth 4: Untested disaster recovery (DR) hot sites.

DR sites are places to work from in case of disasters, and employees were found to be not aware of these places. Employees should be made aware of such sites before they work on them during a disaster. A familiar environment is important.

Myth 5: Conference rooms are adequate disaster recovery sites.

Conference rooms are not workplaces, and are not prepared like workplaces. Such zones are not equipped to handle workers' many communication lines, power and internet needs. A secondary well-equipped site that can manage the requirements for the work environment needs to be set up before disasters.

Myth 6: Disaster recovery can be implemented later.

The planning and building of Disaster Recovery sites are usually put off for later development to help save the cost and time associated with them. However, it should not be delayed as the system production time has the capability to draw all the resources towards it, and the DR planning might fail to materialise.

Myth 7: Equipment will be available during and after the disaster.

It should be noted that there would be no time to move all the resources during a disaster. All the equipment will thus not be available. A plan has to be devised before disaster strikes.

Myth 8: Back-ups work.

Not all backups work according to the assumption that they would during a disaster. A strategy for a back-up plan needs to be concluded during the planning stages, and it should be implemented.The plans and implementation need to be tested before a disaster really strikes.

Myth 9: Disaster recovery can be planned individually.

Centrally coordinated planning for disaster recovery is necessary. The greater and more compound the business, the more empirical it becomes. It has to be a centralised process for all DR plans. Each separate division should not be duplicating similar practices.

Myth 10: Everyone knows what to do.

Roles should be clearly identified and communicated before a disaster. The reporting structures should be defined and lines of command, with their substitutes, should be identified as well. Movement to a new site should be easily done and users should be aware of an alternative site too (Landry & Koger, 2006).

2.9 SUMMARY

A Port MIS is a critical information system that supports middle management to make decisions about the operations at a port. The system, like any other information system, is exposed to many risks. Such risks have the potential to cause more damage. The environment has to be analysed and preventative action taken to prevent such damage.

Threats to an Information system exist within and outside any organisation, and they pose risks. These risks should be minimised and assessed, using validated techniques and methods to determine their danger to the organisation's survival. Risk assessment methodologies have advantages and disadvantages associated with them. However, there is no single method to assess risks. The solution is to use best industry practices such as OCTAVE, but with the supervision of an individual who is an expert in the analysis of the risks posed in that environment.

When identified, the risk needs to be managed. It is highly likely that all risks can be eliminated. Managing risks can help the organisation to improve. However, there are

huge costs needed to minimise risk exposure. The techniques of analysing risk can help if an individual who is appointed to assess the company follows its strategies.

CHAPTER 3

PORT MANAGEMENT INFORMATION SYSTEMS

3.1 INTRODUCTION

Chapter 3 presents a literature review on Port Management Information Systems (PORT MIS), along with port functions, port operations and port users. It reviews PORT MIS subsystems that support the port business functions. The ports are a gateway for the arrival and departure of a number of passengers and a range of goods. This is a result of global trade that has rapidly grown. This has led to a huge increase of growth in trade of goods distributed by the maritime sector (Klopott, 2013). They help the growth of exports and imports exchange, and play a role in how PORT MIS is implemented.

Chapter 3 explains who the role players are. The focus is on subsystems that make up Port MIS - what they serve to accomplish, along with their business functions and the departments that use them. A brief overview of the system and its importance to the ports is included.

3.2 PORT-MIS FUNCTIONS OVERVIEW

A presentation by the Korean Maritime Institute outlined the main functions of Port MIS, as depicted in Figure 3.1 below:

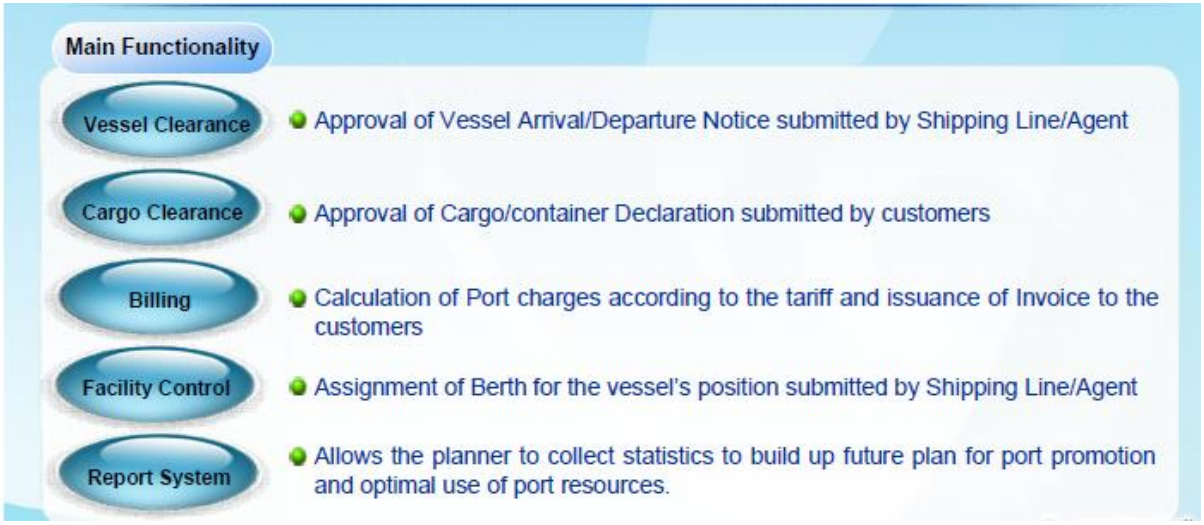


Figure 3.1: Port MIS Functions

Source : (Kim, 2013:4)

The above PORT-MIS functions provide the following benefits:

- Smooth management of vessel arrival/departure and cargo handlings by transferring and using information about vessel, cargo and port facilities through information systems.
- Avoiding unforeseen coincidences by monitoring vessel movements (arrival/departure, berthing) and port facilities through management information.
- Allowing optimal use of limited port facilities by providing port management information on a real-time basis.
- Uplifting stakeholder credibility on port operations by providing paperless administration, removal of user permits/ visits to governmental organisations and fast port operation information services (Cabezas & Kasoulides, 2004).

3.3 PORT ROLE PLAYERS

In order to facilitate the movement of goods in and out of a port, there are people appointed as port operators and users. Their roles might differ from port to port. This study presents what is common to South African and Nigerian ports. Goodhope & Polytechnic (2014) outlined the personnel employed at ports through their job descriptions, as follows:

3.3.1 Port Operators and Users

- **Terminal Operators**

These are companies that own and operate terminals (Baird, 2002). In the South African context, the ports operator is Transnet (PTY) LTD.

- **Stevedores Companies**

Stevedore companies supply dockworkers and are also in charge of other welfare undertakings. Dockworkers are workers or labourers who are employed on vessels at dock. Their normal jobs encompass packing and unloading of freight, recording of loads on vessels or keeping load registers.

- **Exporters and Importers**

These are key operatives in the port system. They are the core of intercontinental trade. Without their services, no intercontinental trade can take place. Importers and exporters are companies or individuals that embark on export and import trade.

- **Warehouse Operators**

These are companies in the port that offer warehousing services for clients to store cargo, either within or close to the port premises.

- **Haulage Companies**

Haulage companies are enterprises in the port that offer transportation and logistics services. They do transportation of cargo in and out of ports to selected end-points.

- **Chandlers**

Chandlers are focused agents that supply food items to vessels that come to the dock.

- **Freight Forwarding and Clearing Agents**

These specialised companies do clearing and forwarding functions. Freight forwarding is a demanding occupation and it is of importance in supporting the logistics business (Shang, Chao, & Lirn, 2016).

- **Maintenance Companies**

These companies do ship repairs and maintenance (Goodhope & Polytechnic, 2014).

- **The Port Authorities**

The role of seaport authorities in governing the regionalisation phase will slightly differ according to the type of port utilization. Port authorities work together with numerous patrons (haulers, movers, transport operators, labour and government organisations) to identify and address concerns affecting logistics.

Port authorities concentrate largely on the general efficiency and progression of trade, rather than on the performance of particular sectors. The port authority can be a catalyst even when its direct impact on cargo flow is limited. Port authorities are known to endorse an efficient intermodal system in order to secure cargo under conditions of high competition (Notteboom & Rodrigue, 2005).

3.3.2 Government Agencies

These are government owned parastatals. Their responsibility is to prevent dangerous contamination of the marine environment and to ensure that practices are in line with international standards (Goodhope & Polytechnic, 2014**).** Government agencies are Customs Officers and Waterway Police, among others (Shang et al., 2016).

In most countries, other government agencies are involved at the border, with the Customs Office as the lead agency. These include:

- Safety agencies
- Plant, drug and food inspectors
- Immigration
- Police and security agencies
- Trading standards organisations (Ojadi & Walters, 2015).

3.4 THE PORT MIS

The role players clearly have their responsibilities in facilitating the movement and support of goods. However, there still needs to be a system that facilitates the responsibilities of all the role players. Figure 3.2 illustrates the Port Management Information System (Port-MIS), developed by the KLNet Corporation. The system has five fields of management: The Vessel, Cargo, Facilities, Billing and Statistics Management (KOSDAQ- Korea Securities Dealers Automated Quotation, 2015)**.**

Port-MIS is an information system, and like any other information system it has a structured database. Figure 3.2 illustrates what the schema of the system would be and how it serves its stakeholders. Stakeholders are those who have a vested interest in the system and are depicted outside the boundaries of the system schema. Also depicted is the information or data stored on the system by its users. The information required by stakeholders differs from function to function.

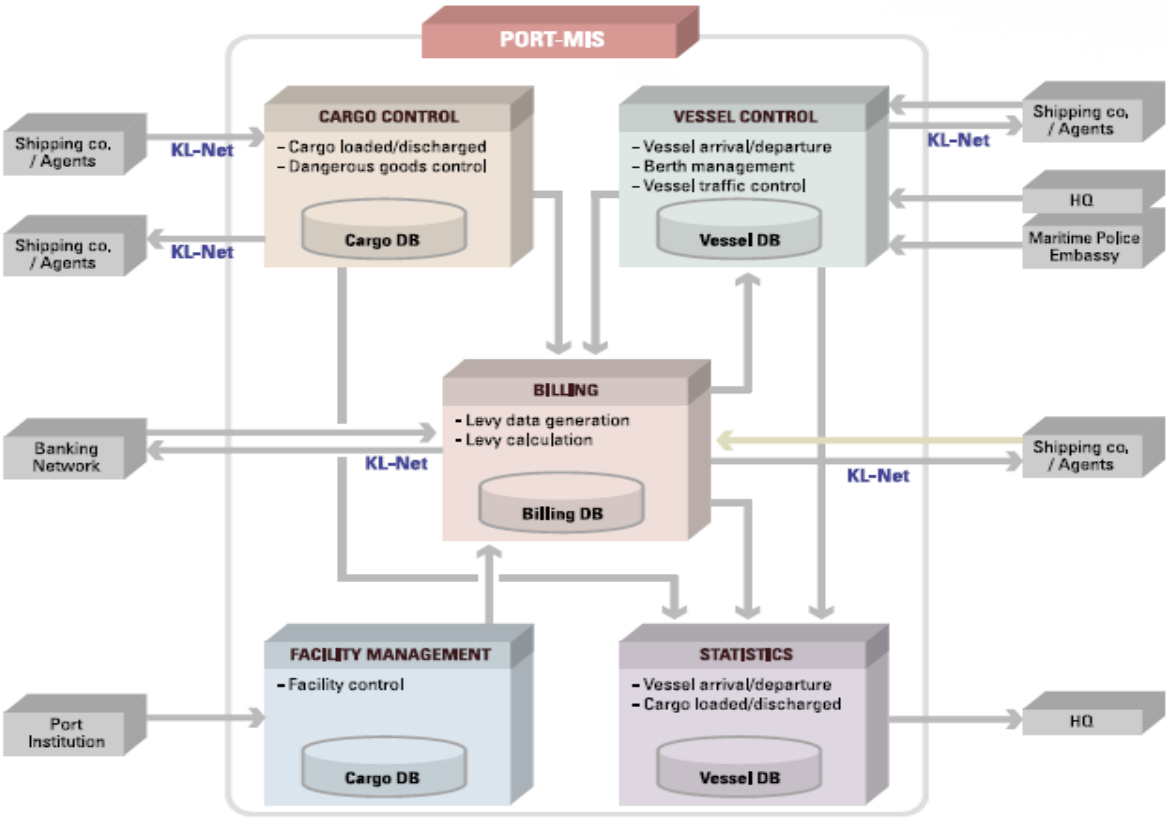


Figure 3.2: Port MIS Schema

Source : (KOSDAQ Korea Securities Dealers Automated Quotation, 2015:8)

Figure 3.2 illustrates the database schema, showing the interested stakeholders of the cargo management system. Shipping companies are likely to make requests on the system. However, the Regional Port Office is more likely to be managing the facilities when needed.

The system in Figure 3.2 depicts the Shipping companies and Regional port operators as the role players. All role players have different duties to fulfil in the port operations. These operations impact on the Port-MIS. These role players, using the Port MIS, together discuss their functions within the port.

Figure 3.2 shows the system as a control system.

However, Figure 3.3 shows the system as a management system. In addition, any researcher studying the system will have to use the term ‘management’ instead of

control. The word ‘control’ in this context has more focus on the technical and engineering related aspects of the ports, thus it has to be used with caution.

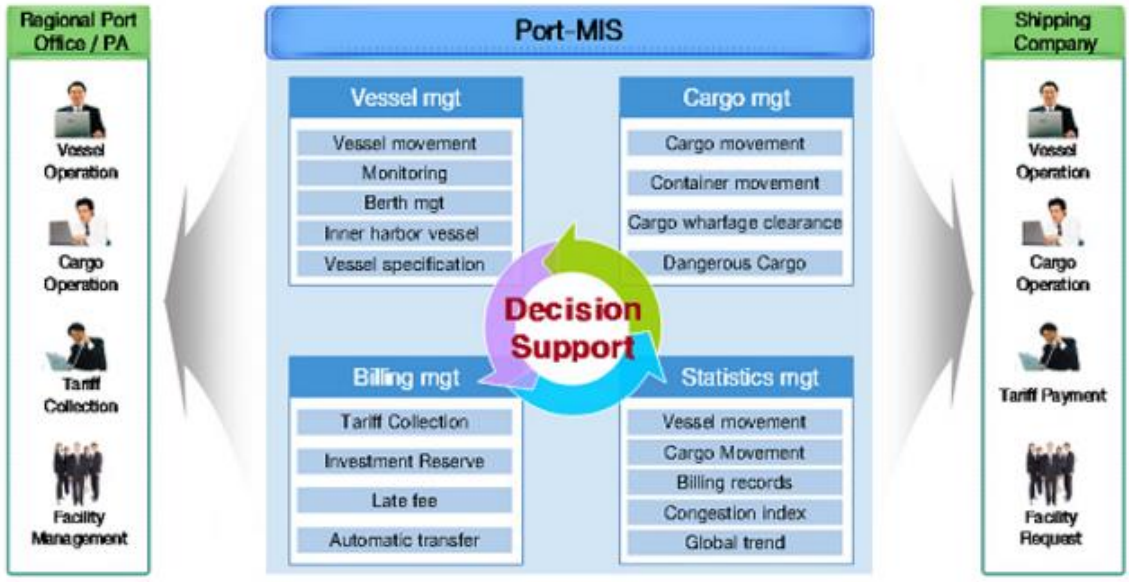


Figure 3.3: Port MIS Conceptual Model

SOURCE : http://www.klnet.co.kr/english/product/product1_1.html

The Port-MIS has sub-systems that contribute to the whole system. The sub-systems can be seen in Figure 3.3 as having a list of management functions that it has to perform. The following sections discuss these management functions and the list of goals or activities to be undertaken by each management system. The first system is that of vessel management.

3.4.1 Vessel Management

Vessel management has to do with the services offered by the ports regarding vessels. These services provide information about vessel position to all agents. They include administrative procedures, e-communication with maritime/port authorities, police, immigration, monitoring services, navigation services and vessel authentication (Dellios & Polemi, 2012). Vessel management in the ports is significant to the shipping industry, as can be seen by how many government stakeholders have an interest in information about vessels.

The shipping industry has been categorised as a high-risk industry, due to the threats that vessels and crewmembers face daily. Poor shipping management can result in

accidents that differ in scope. They comprise loss of human life, enormous marine pollution and damage to a ship or its cargo, among others. Therefore, it is very important for a ship operator or a port manager to have access to all relevant information. The information has to be effectively managed, including the berths utilised by the vessels closer to the port (Karahalios, 2014).

Berths and their management form part of the vessel management. Port MIS stores information about them. Berth management should not be careless, thus exposing vessels to risk. Carelessness in berth assignments has resulted in accidents, where deserted vessels can cost the company millions in the currency of a country (Xu, Li, & Leung, 2012).

Threats to vessels imply threats to Port MIS as well. Threats indicate the importance of the system in the operation of the ports. There are also physical threats to guard against. Physical access threats are when unauthorised parties get direct physical access to ship systems, communication systems or shore assets. It is an obvious threat as it allows these parties to introduce malware or to interfere with the system. Even trusted personnel can be a threat, either because of carelessness or because of bitterness against the company or persons in the company (Rødseth, Marinteknisk & As, 2013). If threats are not addressed properly, there could be no system to work with as an end result.

If there is no vessel management system in a port, chaos will result and vessel collision and other accidents will abound (Herdzik, 2012). This highlights the need to study such a system and how it should address the needs of Port MIS. KLNet Corporation identified some information needs that should be gathered by the Port MIS.

- Vessel Movement information

  Such information is attained from integrated ship management information systems (ISMIS). This can be used to plan distributed vessel management sub-systems, as in a ship sailing on inland rivers. This would inhibit transportation congestion and prevent accidents happening (Wu, Chen, Hu, Shi, & Mo, 2012). The purpose of vessel movement information is to manage traffic flow and protect against delays and accidents.

- Monitoring of Vessels

  Vessel monitoring is closely related to the vessel movement information, and information gathered can help to reduce fatalities that may arise as a result of unmonitored ships. The importance of vessel monitoring is to reduce fatalities that may arise.

- Berth Management Information

  Berth management information helps with the scheduling of the berths, thus decreasing the cost of ships/vessels being idle. These vessels have to be known before reaching a port, avoiding delays that may result in more cost due to delivery delays. Berths form part of the vessel management system. A major challenge facing shipping lines is the limited number of berths at seaports. If no berth is available, vessels have to delay docking. This delays delivery days, raising the cost of the operation (Herdzik, 2012).

- Inner Harbour Vessel Information and Specification

  This is similar to vessel monitoring. Vessel specification includes all details that cover the amount of explosives, toxic substances, flammables in bulk and non-gas free cargo, among others. The release of such freight has to be monitored. These vessels are obliged to display a red flag during daylight and an all-round red light at night. Some other vessels are required to maintain a half-mile separation from identified vessels.

  Within the inner harbour, vessel information required is the authorisation from the Harbour Master before any movement. This is given for indication of overtaking or separation from a specified vessel (Department of Transport, 2009). Facts are recorded about vessel specification, while the Harbour Master regulates how to act when vessels are to approach the inner harbour. All information on vessels are recorded by the Port MIS, whether they are at sea or in the port.

3.4.2 Cargo Management

Cargo management has Cargo Management Systems are about services that provide e-documentation to all proxies involved: cargo e-management, e-information about

container status, cargo authentication and monitoring services navigation services (Dellios & Polemi, 2012). The services are about cargo that is shipped in containers in most instances.

The cargo containers have been documented as major role players, which led to them being part of management systems/ departments. They have emerged as a fundamental means of transporting mass-produced merchandise in a supply chain logistics system. The need for containers arose when the undertaking of barrels, individual boxes and crates became slow and labour exhaustive at seaports (Govender & Mbhele, 2014)**.**

Containers in cargo management are of importance as most goods are transported this way. Cargo management, particularly in the maritime domain, play a vital part in the transfer of goods between seller and buyer. Despite such importance, with over 90% of the world's worldwide trade being sea based, there is actually little known about this subject (Rowbotham, 2014).

A cargo management system encompasses a lot of proxies. The interested stakeholders have their information regarding their cargo through e-documentation. However, there is little known about these systems. Figure 3.3 confirms that such e-documentation has to have information about the vessels, and this information has to come from vessel management systems. Figure 3.3 noted that information on dangerous cargo forms part of the management system.

Cargo movement and container movement are integrated as the cargo is moved in containers. Currently, the container movement in a port is totally managed by computerised software systems. There are systems for cars which are transported as cargo in containers. This system is known as the "Vehicle Booking System" (VBS). It allocates period slots for road carriers to book their time to come and pick up their containers (Pudhota, 2012). Within the container/cargo movement, the most important factor is the management of the cargo pick up and packing.

All cargo has to be paid for, and cargo wharf clearance is closely related to the Billing Management System. Clearance is part of the handling of cargo in ports, with special focus on dangerous cargo. Hazardous and dangerous goods require professional management due to their volatile and unstable nature. They can be toxic, explosive,

or flammable, and often require dedicated and specialist handling facilities at the ports during loading and unloading.

Loading onto the vessel must be done in such a way that they do not risk influencing or compromising the safety of the vessel and its crew. The dangers of the cargo have to be properly sent to the port managers, the shipping lines and the shipping agents (Rowbotham, 2014). Dangerous cargo requires delicacy when being handled as they are toxic and harmful. They have to be noted on the Vessel Management system.

Cargo management has to do with services rendered to shipping companies and other interested parties using, amongst other things, containers to move their products. How to handle dangerous cargo in containers includes, among other things, information that needs to be conveyed in an organised system.

3.4.3 Billing Management

A leading information system developer, the Klein Systems Group, states that a billing system (as a sub-system of a Port MIS) has to perform the following calculations:

- **Wharfage**
  Automated calculation of wharfage is based on customer and commodity codes, inter-modal and multi-modal transport discounts and other relevant factors.

- **Dockage & Pilotage**
  Pilotage is guiding a vessel on a river channel, for example, from the mouth of the Columbia River to Portland. Pilotage fees are charges for mooring a vessel at a wharf (Oregon State University, 1981)**.** An automatic charge calculation of dockage and pilotage is conducted, based on the length of the vessel, time and other factors. Calculation charges are for monthly, twenty-four hour days, hourly, six-hour days and many other billing options. This is also needed for vessel information management, along with vessel scheduling so that the preparation of bills can be automated and founded on vessel movement, onset time, period from anchor to berth, berth to berth etc.

- **Lease invoicing**

This is the ability to invoice automatically for rent, including a year-on-year inflationary raise in the rental amount. Rent is for the facilities offered.

- **Electronic Invoicing**

This is the ability to automatically email, fax and mail invoices to terminal operators, stakeholders, shipping lines and any other transacting parties. It should setup customer preferences for billing based on combined invoices.

- **Bunkerage Invoicing**

This is invoicing for fuel and any service charges for the bunkerage.

- **Guaranteed Contract Minimums / Guaranteed Annual Minimum (GAM) Invoicing**

This is the ability to automatically calculate short falls from agreed upon contract minimums or GAMs, and then to bill them at the pre-agreed occurrence on the quarterly, annual invoice etc. (Ignify, 2016).

- **Tariff Collection**

Customs agencies are responsible for the collection of tariffs and fees at ports of entry. This is their known duty, such as protection of intellectual property through the prohibition of forgery merchandise, the deterrence of dangerous goods from entering the country, and the prevention of illegitimate entry (Han & McGauran, 2014).

The port tariffs charged are dependent on the category of services offered to the customer, who could be an importer or an exporter. The tariff items are separated between charges to the vessel, and charges to the cargo. These charges are influenced by a variety of factors, including the nature of the merchandise handled or carried, the nature of the carrying ship used, the capacity of trade and the elasticity of demand for the product (Strandenes & Marlow, 2000).

- **Investment Reserve**

A study, titled “Russian ports to charge investment dues already in 2017” (Port Today, 2017), on investment reserves showed that the Russian Ministry of Transportation introduced special investment charges at national seaports. This

was dependent on the vessels used. The sole purpose of the investment was to support building and expansion of state-owned facilities in seaports. It is a charge imposed on all cargo vessels at their seaports (Port Today, 2017). The revenue is generated through additional charges, which can be imposed on for use of safe passage. Vessels are obligated to meet the costs intended to compensate the investment into infrastructure and superstructure to the states having control of the area (Vukić, Peronja, & Slišković, 2018).

- **Late Fees**

Late fees or demurrage are charges incurred if the time limits of ocean vessel contracts are not met (Gleim, 2009).

- **Automatic Transfers**

This transfer of information is provided by the Automatic Identification System (AIS). It includes vessel parameters such as: name, length, nationality, operation type, berth quay, company, arrival date, source port, port code, ship type, cruise transit, Lloyd code, departure date, bollards, call sign and destination port (Fernández et al., 2016).

Billing systems are pivotal to reducing cost and hardship to gather income. This has features embedded in them, such as customer or vessel contract management, rate table based tariffs, multiple inputs for a single tariff, automated billing procedures and Account Receivables. The tariffs are easy to update; complex tariffs are automatically controlled, reducing billing errors and calculation time. Contract management is automatic, reducing the time to generate appropriate discounts, special rates and manage minimum guarantees. All invoicing on the system is automated and operational data and financial data are kept synchronised (Kleinport, 2016).

3.4.4 Facilities Management

Facilities Management (FM) is a new field of study developed within engineering, as well as a new service sector that has been developing due to outsourcing of non-core competencies (such as cleaning and office management) to third party providers. It has varied definitions, and is understood to be the integration of organisational

processes in order to maintain and develop the services supporting and improving the effectiveness of the primary processes.

FM is also described as an integrated approach to operating, maintaining, improving and adapting the buildings and infrastructure of an organisation in order to create an environment that strongly supports its primary objectives. These views are implicitly based on the concept of the value chain, distinguishing between the primary and secondary activities of an organisation (Scupola, 2012).

FM can be seen as a non-primary core business of the seaport. Within the ports, the building and infrastructure refer to the storage areas and warehouses used for cargo that has to be shipped out, and cargo that has been shipped in. Ports have to provide facilities and services for vessels and freight – this includes infrastructure, building, equipment and services to ships and services to cargo (Cullinane, Song, & Wang, 2003). These are of importance to the ports, but they are not primarily the field of outmost importance to the function of a port. A system enabling FM at ports would assist with availability of its services to the relevant stakeholders.

3.4.5 Statistics Management

Port statistics have traditionally been within the realm of terminal operators, local port authorities or national associations. Largely, these entities decided what data was collected and, more importantly, how and when the data was disseminated (UNCTAD, 2014). The role of the Port Authority is to oversee and administer commercial operations within each port by regulating pricing, and supervising access to basic port infrastructure (ASH Centre for Democratic Governance and Innovation, 2011).

In a competitive environment, Information Communication Technology (ICT) systems play a strong supporting role in accompanying the evolution of port authorities and sustaining their growth strategies. Generally, the use of ICT to gain competitive advantage has become a key strategic issue amongst organisations in the fast globalising environment (Cepolina & Ghiara, 2013). Statistics management systems should help ports to be competitive. However, they are selective on what they collect to be competitive. The first information gathered would be that of vessel and cargo movement along the reports on port congestion and global trend index.

- **Vessel Movement**

Information on the movement of vessels is gathered through another system, known as the Vehicle Management System (VMS). It is similar to the VBS. It is known to offer instantaneous vessel movement tracking at a glance and anytime, and keeps the history of vessel movement (Alfayyadh, 2017). Knowing such information would be important for decision-making on the port's activities.

- **Cargo Movement**

Figure 3.4 explains cargo movement statistics as being part of port statistics. The focus is on the purpose of a port. Ports serve as sea-land interfaces for the movement of cargo and passengers. As a crucial part of multimodal transport, they are of great economic and strategic importance to the country where they are located.

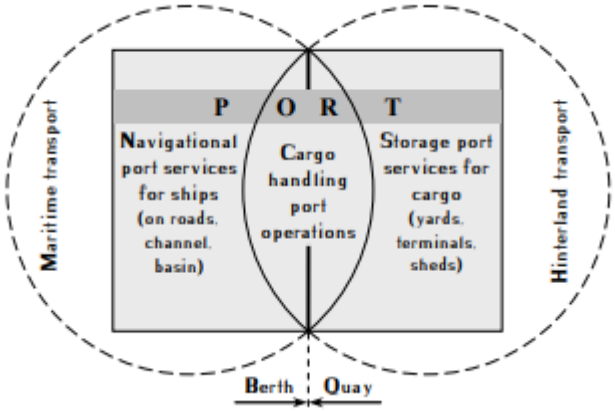


Figure 3.4: Port operations interface within the multimodal transport chain.
Source: (Ibrahimi, 2009:3)

Cargo movement statistics include performance pointers spread from port operational and financials to environmental, safety, security and trade aiding issues. However, in port operations, as seen in Figure 3.4, it has to do with cargo movement from land to sea and vice-versa. More specifically, the following cargo movement concerns are critical:

- Cargo movement consignment transportation vehicles, such as vessels, trucks and trains.
- The direct movement of cargo from ships to trains and trucks and vice-versa.
- The incidental movement of cargo between transportation vehicles and numerous storing spaces.

- The movement to storage facilities, courtyards, sheds and storerooms (Ibrahimi, 2009). Cargo movement statistics are concerned with the moving of cargo to and from land to the ports; the use of inland transportation; and inter-portal movement that encompasses movement to different storage facilities.

Statistics management includes billing records, which refers to information that is part of a billing module. A billing module is the maintenance of a precise account of terminal operations, the management of numerous types of billing codes with prices or special contracts that a port has with its business partners, as well as the issuing of invoices. The following are features of the billing module:

- Invoicing for credit
- Receipt for cash
- Payment summary
- Code management such as tariff code, invoice unit, and demurrage. Data gathering on terminal operation (Alfayyadh, 2017).

Another part of statistics information gathered in Port MIS entails the invoicing, register of cash with summary, and invoices for units serviced by the ports.

- **Port Congestion Index and Global Trends**

Port congestion is explained as the greatest time intensive dealings for the port operations management. It influences the efficiency of the port operations in an undesirable way. Port congestion occurs when the port and terminal capabilities are not adequate enough to deal with the traffic received at the port, causing waiting times. There are numerous factors that cause vessels to build-up at ports: bad weather, strikes, insufficient infrastructure, poor management etc. Ship pile-up at anchorage can also be a major safety and environmental issue for ports (Romers, 2013).

Congestion at a port is one of many factors that could be a threat to safety, and could affect the environment. Port management needs a Port MIS to help them to deal with congestion. There are different types of congestion, and management has to be given information from the statistics system on them. Such information will identify the type of congestion and the explanation for their cause:

i. Ship Berth Congestion

This results from crowding by ships waiting on the port mouth paths. The delay could be that other vessels are occupying the existing berth elected, or likely to be allocated to the up-coming traffic.

ii. Ship Work Congestion

This is a result of delays in the processing of work on loading and / or off - loading the ship, which results in slowdowns that could lengthen the interval of time that the ship had to stay in port to realise the cargo operation assignment.

iii. Vehicle Gate Congestion

This is a result of poor scheduling of landward admission to the port through trucks which are programmed arrivals at the port gate. If impediments or programming defaults occur, the system sends instantaneously queuing indications to automobiles entering or exiting the port gate for delivery or evacuation of cargo. This becomes a consequence of port gate congestion.

iv. Vehicle Work Congestion

This mainly emanates from lapses related to the packing or unpacking of trucks and vehicles. The absence of necessary apparatus to do the work of packing and unpacking, or low productivity from necessary vehicle work can cause this congestion.

v. Cargo Stack Congestion

This results from a constant stay of cargo in the storing area, over the agreed number of hours/days or above the determined capability of the cargo stacking area.

iv. Ship Entry / Exit Route Congestion

This arises when there is any incidental barricade on the naval side access paths to the port facility. Such a barricade would lead to queues and ultimately extending a ship's turn-around time at the port facility (GIDADO, 2015).

The congestion experienced is dependent on the type of factors contributing to it. They start with problems at berthing, work done on packing and unpacking of cargo along vehicles and trucks, the storage facilities not being enough to do undocking to nearest

storage facilities, the access of vehicles working on the cargo to and from the ships and the route management on entry and exit.

All of the factors discussed would be an integral part of the information that the Port MIS system would collate for port managers to execute their duties to run efficient ports.

3.5 CONCLUSION

Chapter 3 has shown that ports help to facilitate the export and import of goods. This happens with the help of port role players and the Port MIS, a system that supports five business functions. The five business functions relate to vessel management, cargo management, facilities management, billing management and port statistics management. These systems are interrelated, and share the information in one system with another.

The vessel management information gathered can be used by the statistics management to report on what types of vessels have been to the port. The information can be also used to report on cargo delivered, as it has information relating to the type of vessels used for the operation. This is another way to show that cargo management relates to the vessel management and gathers information as such.

The cargo has to be housed on delivery, thus information about what has been imported has to show what capabilities the Facilities Management department is able to store. All this cargo has to be paid for, and this relates to Billing Management. Billing management has to do with the billing that relates to the cargo delivered or exported as this is of interest to authorities as port role players. The billing is also determined according to the type of services rendered. Cargo management will be of importance in the sharing of information to automatically charge accordingly.

CHAPTER 4

RESEARCH DESIGN AND METHODOLOGY

4.1 INTRODUCTION

Chapter 4 explains the methodology of how the research was conducted and the reason for the choice of the methodology. The research design, research instruments, questionnaires for the quantitative data and sample of respondents are reviewed. A qualitative method of research was adopted.

4.2 RESEARCH DESIGN

According to Bernard (2000), research design "is the careful planning and implementation of a process of knowing, on which a priori planning of all phases of research which includes analysis and writing, can benefit one's research in several ways" (Bernard, 2000). A worthy research design is clearly well-defined, uniformity flanked by research questions and methods which will produce valid and dependable data and which can be achieved by the existing resources of conducting research (Ritchie & Lewis, 2014).

Chapters 2 and 3 addressed the theoretical perspective of the research design and briefly addressed the research questions. This research study was on Transnet Ports across South Africa. It focussed on risk assessment on Port MIS, and how management should be addressing the issues regarding risk. The study explored the value of the subsystems that make up Port MIS.

A questionnaire was constructed and sent to Transnet (Pty) Ltd. A sample of Port MIS users had to answer the questionnaires. The sample was selected out of the full population of the Port Management Information Systems (Port MIS) users. The sample included managers and subordinates who use the Port MIS. Their input complemented the theory presented.

4.3 POPULATION AND SAMPLE SELECTION

Population

Defining and selecting the population sample was guided by the following questions.

• What were the primary population or populations in your study?

The primary population of the study was Transnet (Pty) Ltd Port MIS users who happen to be middle managers. The study on Port MIS had to focus on the users who are exposed to the system risks.

• Are there subpopulations within the population that are of particular interest?

The middle managers and managers use the Port MIS to make decisions that affect operations. They make up the primary population. However, the Port MIS is fed information or data by other sub-systems. The users of the sub-systems form a sub-population, and they also need to address the risks to Port MIS.

• Would it benefit your study to include groups of individuals other than the primary population? That is, who are the key stakeholders?

The study will benefit by including the other Port MIS users, such as the subordinates that feed the system with data. They also represent all the stakeholders within the system.

• Are there specific individuals whom you should include?

The Port MIS users have to be included in this study (Bernard, 2000).

The purpose of the study was to give an overview of how risk is managed under the Port MIS. The sample included users of Port MIS at manager and staff level.

Sampling is of concern to control the success of a project. There are different procedures in qualitative research that guide the selection of respondents, as it is not about counting opinions or people. It is about exploring the range of opinions and different representations of an issue that is being investigated. Sampling in qualitative research is concerned with the richness of information and the number of participants required (O'Reilly & Parker, 2012).

For this research study, the sample was selected using purposive sampling. Purposive sampling is heterogeneous sampling, also known as maximum variation sampling. It is a deliberate strategy to include phenomena which may vary widely from each other. The aim is to identify central themes which cut across the variety of cases or people (Ritchie & Lewis, 2014).

The study sampling can be described as heterogeneity purposive as the sample was selected from the group of Port MIS manager-users, and the group of subordinate-users. These groups both have differences, where one is of managers and the latter being their subordinates. However, they use the same Port MIS and address the same problem.

4.4 RESEARCH METHODOLOGY

Research methodology is a science that defines the principles of methods to study a subject. It is for developing a process containing all the elements required, allowing descriptions, explaining and predicting a phenomenon, process or effects (Mitra & Borza, 2015). For this study, the research methodology used questionnaires to establish how the Port MIS users manage the risks relating to them.

The researcher had to use a methodology that provides a practical and accessible explanation of what is being investigated in a particular study. The following questions had to be considered:

- Why the researcher chose that focus;
- Why the study was designed by the researcher in that way;
- Why alternatives were rejected;
- What were the questions the researcher was asking, and
- How did the researcher ensure that confidence could be felt in the data gathered and in the analysis of that data (Case & Light, 2011).

Attempts to answer the above questions are addressed in the following paragraphs on positivistic, phenomenological and mixed methods.

4.4.1 Positivistic / Qualitative

A Positivistic or qualitative research study is defined as a developing, inductive, interpretive and naturalistic approach to a study. It is a reading of people, cases,

phenomena, social situations and processes in their usual settings in order to disclose in descriptive terms the meanings that people attach to their experiences of the world. It should be noted that qualitative research is not based on a single methodology and does not belong to a single discipline (Yilmaz, 2013). The Positivistic approach was chosen for this study to explore how the users of Port MIS were experiencing and addressing risk related to the systems.

It should be noted that qualitative methods have typically been used more in the study of Information Systems (IS) and in other social sciences for exploratory research in order to develop a deep understanding of a phenomenon and/ or to inductively generate new theoretical insights (Venkatesh & Brown, 2013). This is what this study will try to achieve by looking at existing theory of risk management and how it will be applied to Port MIS. There is not much research done on Port MIS, and it is thus fitting that a qualitative study be done, together with a quantitative study.

In order to achieve validity, there should be an adequate sample size of users to get the results. It is said that the quality of qualitative research, to a considerable extent, relates to sampling adequacy that should provide wisdom and maximum opportunity for transferability of findings (O'Reilly & Parker, 2012). The sample chosen came from all Transnet ports in South Africa.

The selected sample filled in the questionnaire on the premises of their companies. The reason for the latter is that some of the respondents were in displaced cities. There are potential advantages of using the online questionnaires for research, is saving in time and travel costs and greater anonymity around sensitive topics (Irvine, Drew, & Sainsbury, 2013).

The questionnaires were constructed so as to get in-depth knowledge of risk as related to Port MIS. They formed the basis of the interviews conducted. The purpose of in-depth interviewing is not to get answers to questions, nor to test hypotheses, and not to "evaluate" as it is normally used. At the root of in-depth interviewing is an interest in understanding the existed experiences of other individuals and the sense they make of that experience (Seidtnan, 2006). Untapped knowledge on Port Risk Management was sought.

4.4.2 Phenomenological Approach / Quantitative

Quantitative research is about investigating a phenomenon by collecting numerical data that is analysed using mathematically based methods, specifically statistics (Muijs, 2005). Thus, a questionnaire was distributed to Transnet Port MIS users to assess how they manage risk relating to the system they use.

The purpose of quantitative studies was for the researcher to project his or her findings onto the larger population through an objective process. Data collected, often through surveys administered to a sample or subset of the entire population, allows the researcher to generalise or make inferences. Results are interpreted to determine the probability that the conclusions found among the sample can be replicated within the larger population (Borrego & Tech, 2009).

4.4.3 Mixed Method Approach

A mixed method study involves the collection or analysis of both quantitative and/or qualitative data in a single study in which the data is collected concurrently or sequentially, is given priority, and involves the integration of the data at one or more stages in the process of research (Borrego & Tech, 2009).

Quantitative and qualitative research designs differ in terms of their epistemological, theoretical and methodological underpinnings. Quantitative research seeks to develop descriptive universal laws in social behaviours by statistically measuring what it assumes to be a static reality. It stresses the measurement and analysis of causal relationships between isolated variables within a framework which is value-free, logical, reductionist, and deterministic, based on *a priori* theories (Yilmaz, 2013).

Mixed method research studies are seen to be the meaningful merging of qualitative and quantitative approaches. They offer a completely diverse new strand of research methodology that allows researchers to get data about both the individual and the broader societal context, and conveys the results of the qualitative and the quantitative paradigms (Lisle, 2011).

4.4.4 Rationale of the Research Paradigm

For this study, a questionnaire was considered an effective method for gathering data from clients when a focus group or semi-structured number of respondents was not a possibility (Veith, 2015).

4.4.5 Design of the questionnaire

The questionnaire was designed to answer all the research questions as presented in Chapter 1.

4.5 DEMOGRAPHICS

The response profile was concerned with who the respondents were and the demographics of the aforementioned individuals. There were twenty-four (24) respondents who replied to an online questionnaire. The researcher expected that a total of 21 respondents would have made up 10% of the targeted sample in relation to the number of questions included in the survey instrument (Wegner, 2007).. The response rate was, therefore, better than anticipated. The questionnaire was distributed to Transnet employees via a third party, which makes it impossible to confirm how many users and actual employees were working on the system.

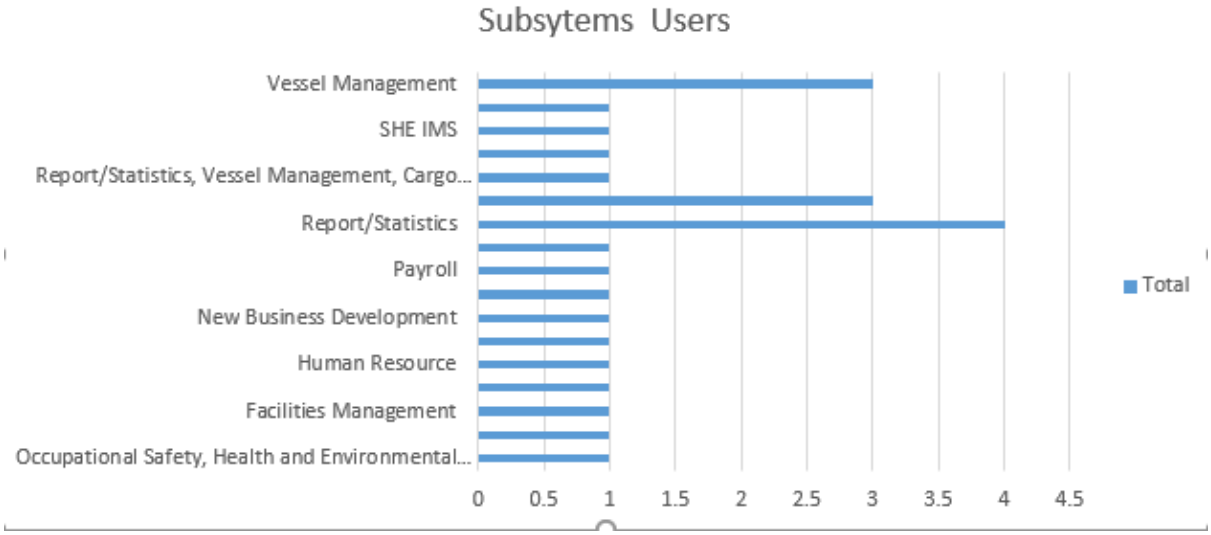


Figure 4.1: Number of Sub-system Users by department

Sub-system	Number of users = 24
Vessel Management	3
Report or Statistics/ **Vessel Management/** **Cargo Management**	8
Billing Management	1
Facilities Management	1
Other(s): **New Business Development** **Operations** **Risk Management** **Operations** **Procurement** **Payroll** **Occupational Health, Health** **and Environmental Management Systems** **Human Resources** **SHE IMS/ SHE Management**	11

Table 4.1: Number of Sub-system Users

The employees were targeted based on what is known about users of the system or from the known department complementing the system, as illustrated in the graph in Figure 4.1 above. The respondents from vessel management, report statistics, cargo management and facilities management made up (54%) of the respondents. However, none of the other respondents (46%) were excluded from the study since only the distributor of the questionnaire knew the internal use of the system in operations. The users could be working on the system with different titles, (other than what is illustrated in Figure 3.1), related to the system and thus it was assumed that a representative group of users was selected for the study.

The next section discusses the level of management occupied by the respondents.

The level of management occupied by most (66%) respondents fall within the level of senior and middle management, befitting that an MIS would be used by such end

users. Figure 4.2 gives a good illustration that both senior and middle management are both highly represented as compared to non-supervisory respondents, with the smallest number of respondents being Junior Managers.

Figure 4.2: Percentage Levels of Management

Level of Management within the organisation	**Percentage**
Junior Management	13%
Middle Management	33%
Non-supervisory staff	21
Senior Management	33%

Table 4.2: Percentage Levels of Management

The majority of respondents were from the targeted groups, thus giving the desired credibility to the sample respondents.

The next aspect was the geographic location demarcation of the respondents.

The questionnaire was targeted at all 8 ports of South Africa. The respondents include representatives from all the ports. Figure 4.2 illustrates all the 8 port respondents, including the TNPA, which is the ports' national headquarters. They have a vested interest in the operations as the head office. The most interesting aspect was that the majority of the users were from the port of Ngqurha; followed by the port of Port Elizabeth, with the rest of the respondents being from each of the other ports.

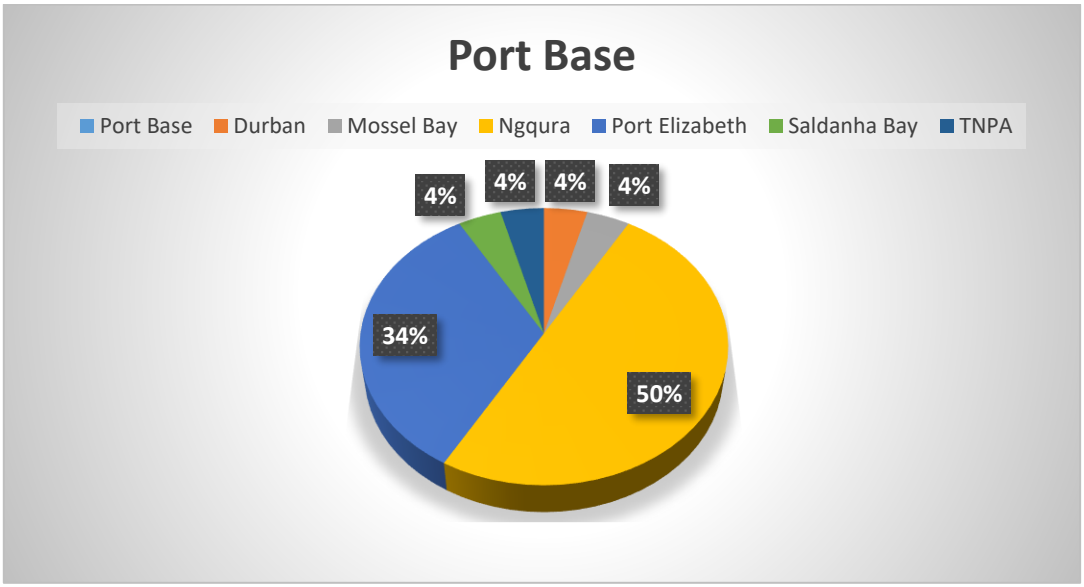


Figure 4.3: Percentages by Port Base

Port Base	**Pecentage**
Durban	4%
Mossel Bay	4%
Ngqurha	50%
Port Elizabeth	34%
Saldanha Bay	4%
TNPA	4%

Table 4.3: Percentages by Port Base

In terms of geographical location, it could be said that 84% of the respondents were from the Eastern Cape region.

4.6 MEASUREMENT CHARACTERISTICS

Measurement is the assigning of numbers to observations in order to enumerate phenomena (Kimberlin & Winterstein, 2008). This study is both qualitative and quantitative. Sampling in qualitative research is concerned with the richness of information and the number of participants required in order to enumerate the

phenomena (O'Reilly & Parker, 2012). The sample comprised of 24 respondents from an unknown population of Port MIS users, as only Transnet knows the numbers.

Knowing that a sample was used, it meant that the research measuring instrument results should be inferred to the population as whole. Therefore, the measuring instruments used must be valid, reliable and the result be generalisable. The following section addresses reliability, validity and generalisability pertaining to this study.

4.6.1 RESEARCH INSTRUMENTS

For the purpose of this study, a survey was conducted using questionnaires (see Appendix B) as a research instrument. They were distributed and administered by the researcher. A questionnaire afforded the opportunity to get insight on the topic being investigated. The other instrument used was an interview with the managers and users to gauge their understanding of risk and management.

- Questionnaires

Questionnaires are one of the primary sources of gaining data in any research study. Closed-ended (or structured) questions were used in the questionnaires for this study. They allow the reviewer to control what the question asks and get answers on only what is being probed (Zohrabi, 2013).

- Validity

Validity is defined as the extent to which an instrument measures what it purports to measure. The questionnaires and interviews had to be valid in addressing the issues of Port MIS risk management. Validity requires that an instrument is reliable as well.

- Reliability

Reliability can be measured in multiple ways, depending on the type of instrument being used. The most common forms include: test-retest; internal consistency and scorer reliability (Hagan, 2014). Reliability refers to an item being tested receiving the same responses at different times.

- Generalisability

Research results given by the instruments should be generalisable. They should represent the theory gathered and results produced. The theory is applicable to different settings not only for purposes of basic research, but also for purposes of

managing and solving problems that organisations like Transnet face in their daily operations (Chong, Techatassanasoontorn and Doolin, 2013).

4.7 ETHICAL CONSIDERATIONS

All the required ethics forms were submitted to the Nelson Mandela University Ethics Committee for ethical clearance. The ethical principles listed below were followed:

Ethical Principles

- Minimising harm.
  This research study is not likely to cause any harm to the individuals surveyed or interviewed. All the participants were free from any harm or danger whatsoever by taking part. The research is likely to be repeated by anyone without causing any harm.

- Respecting autonomy.
  The research process showed respect for people in the sense of allowing them to make decisions for themselves, notably about whether or not to participate. The respondent knew that they could withdraw at any time from the process of the study.

- Protecting privacy.
  When the research is to be made public, the respondents will be provided with descriptions and explanations of what would be publicly available. Also included would be what would not be made public. This will be to ensure that data is kept confidential.

- Offering reciprocity.
  Researchers depend upon being allowed access to data, and this may involve people cooperating in various ways: for example, giving up time in order to be interviewed or to fill in a questionnaire. The research process can also disrupt people's lives in various ways and to varying degrees when interviews are conducted.

- Treating people equitably.
  It could be argued that the various individuals and groups that a researcher comes into contact with in the course of research would hold different positions

in the organisation. It was noted that should all be treated equally and the research study would promise such. This means that no-one would be unjustly preferred or separated against from the study (Montefiore, 2012).

The treatment of the respondents is important to ensure that the study had followed proper protocols. No respondents was forced to take part if they were not willing. The researcher explained how the results would be distributed and published. This ensured that they will not be harmed in any way. Their reputation and equality was to be upheld at all times.

4.8 SUMMARY

Chapter 4 outlined how risk in Port MIS would be investigated. The research design clarified that the study would be a mixed method study using quantitative and qualitative approaches. The population and sample was identified. An overview of the research instruments and their application was provided. The chapter closed with a review of the ethics principles that were applied.

CHAPTER 5

DATA ANALYSIS AND FINDINGS

5.1 INTRODUCTION

Chapter 5 presents an analysis of the data collected from Transnet. It focuses on the empirical data collected and discusses the findings. An analysis of the responses is given based on each of the research questions. The details surrounding each response and additional factors are discussed in the context of the research questions.

5.2 DATA ANALYSIS BASED ON RESEARCH OBJECTIVES

The primary objective of this study was to explore the effects of managing risk within Port Management Information Systems. It sought to do this through set research questions.

THE RESEARCH QUESTIONS

RQ 1: What are the risks that apply to information systems such as the Port MIS?

RQ2: What are prevalent risk assessment methods?

RQ 3: What are the effects of risk on Port MIS and subsystems?

RQ 4: What is the importance if risk assessments?

RQ5: What is the importance of risk management?

RQ 6: Do all eight ports in South Africa attach the same level of importance to risk assessment for their Port MIS?

RQ 7: How can risk management strategy be standardised for all eight Ports?

Together with the above research questions were sub-questions that related to the questionnaire, which the respondents had to answer. The analysis conducted on the data collected was a descriptive statistical analysis based on The Likert Scale. Respondents had to give an answer to each statement on the questionnaire ranging from “Strongly Agree” to “Strongly Disagree.”

RQ1: What are the risks that apply to information systems such as the Port MIS?

The first research question probed the risks to information systems such as the Port MIS.

The questionnaire statements that addressed this research question were:

- Information on systems are at risk of theft by employees.
- Information on systems are at risk of theft by outsiders.
- The computer equipment can be manually stolen from its physical location.
- The system can easily be destroyed by intruders.
- Employees of the organisation can damage the company's information system internally by themselves.
- Telecommunication and IT systems are at risk from the following attacks: Terror attacks e.g. such as inter-country warfare.
- The telecommunication and IT system are at risk of the following attacks: Technological threats e.g. cyber-attacks.
- The telecommunication and IT system are at risk of the following attacks: Criminal attacks such as phone lines being damaged.
- The telecommunication and IT system are at risk of the following attacks: Criminal attacks such as cables being stolen.

Table 5.1: Information on systems are at risk of theft by employees.

	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	21%	25%	29%	21%	4%	100%
No. of Respondents	5	6	7	5	1	24

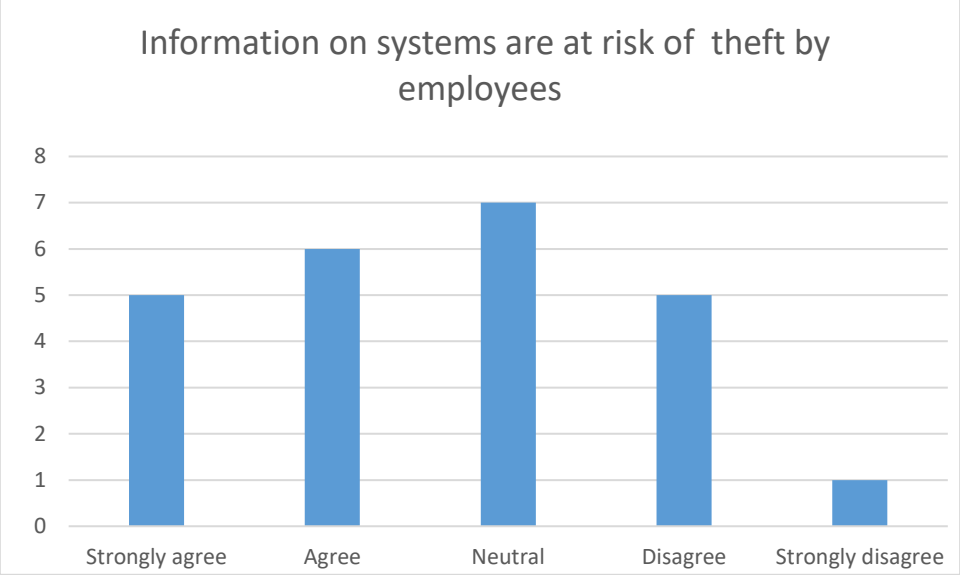


Figure 5.1: Information on systems are at risk of theft by employees.

Table 5.1 clarifies that most of the respondents (29%) were neutral to the statement. The second most did agree (25%). It should be of concern that most respondents felt that the system was at risk of theft by employees. Thieves also come in the form of individuals who are ambitious leaders, with the intention of starting their own business, or collaborating with outside companies if possible. It is necessary to have measures in place to detect their suspicious activities. The respondent company could use threat detection approaches (Refer Chapter 2: Table 2.2) and implement them to detect malicious activities by employees to minimise risk.

Table 5.2: Information on systems are at risk of theft by outsiders

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	4%	21%	29%	38%	8%	100%
No. of Respondents	1	5	7	9	2	24

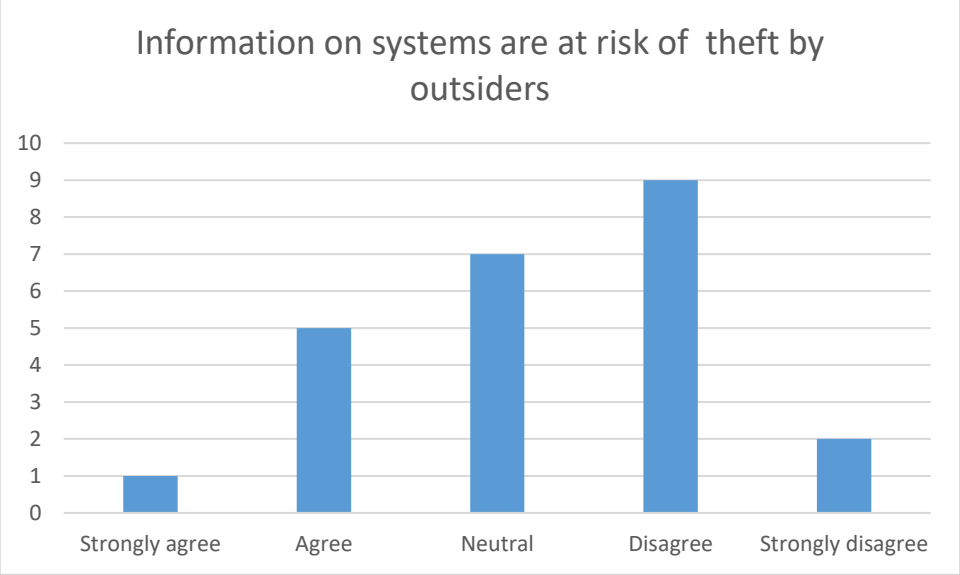


Figure 5.2: Information on systems are at risk of theft by outsiders

Table 5.2 clarifies that most of the respondents (38%) disagreed with the statement that information systems are at risk of theft by outsiders. 8% strongly disagreed. The neutral respondents (29%), combined with the number of those who strongly agreed (4%) and agreed (21%) made up 54% of the users. This surpassed 46% of the users who disagreed (38%) and strongly disagreed (8%) - that the information on systems was at risk of theft by outsiders. This reveals that there might be a possible breach of security.

Those users who disagreed (38%) and those who were neutral (29%) mean that there is a group of people who do not know whether or not the information on systems is at risk of theft by outsiders.

There should be further investigation as to why there are only (8%) that disagrees and (38%) who strongly disagrees. What did the other users feel about theft? The threats by outsiders represent an example of threats by saboteurs who may be known to individuals or groups within the company. They are likely to cause interruptions on shared resources of a computer network. The port MIS system has to be protected from such threats.

Table 5.3: The computer equipment can be manually stolen from its physical location.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	17%	33%	25%	21%	4%	100%
No. of Respondents	4	8	6	5	1	24

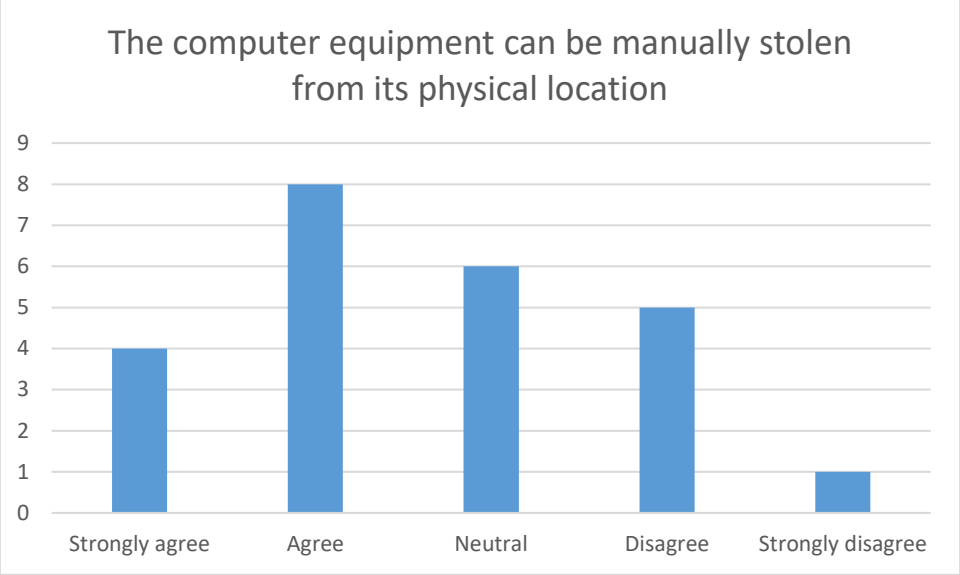


Figure 5.3: The computer equipment can be manually stolen from its physical location

Table 5.3 and Figure 5.3 show that the most number of respondents (33%) agree that the computer equipment can be manually stolen from their physical location. This means that most respondents believed that the location where the computer equipment was kept was not safe, but at risk of being broken into. Respondents that strongly agree formed 17%, and those who were neutral were 25%. The definition of risk includes theft as an undesirable effect. Therefore, it can be concluded that there is a need to protect the computer equipment against physical theft.

Table 5.4: The system can easily be destroyed by intruders

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	4%	21%	29%	34%%	12%	100%
No. of Respondents	1	5	7	9	3	24

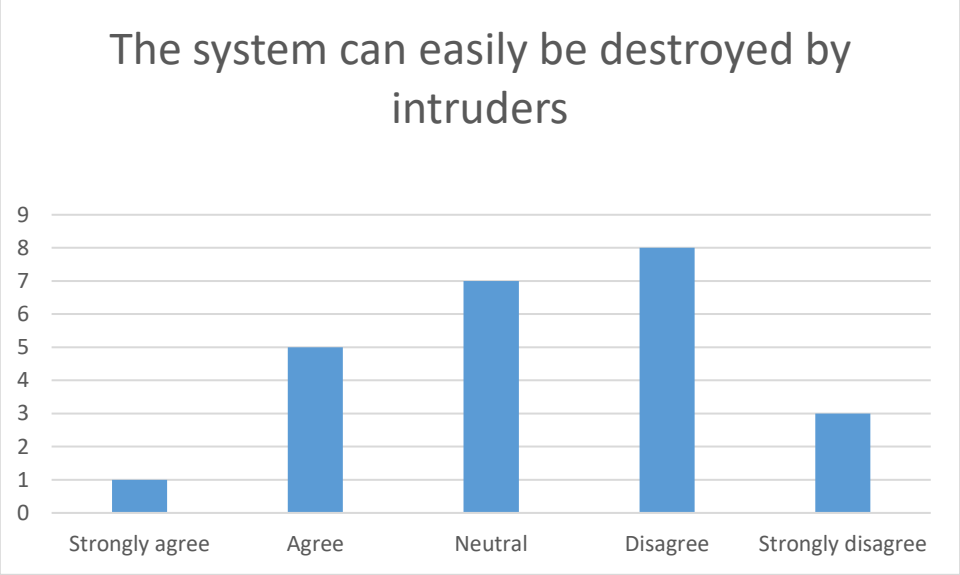


Figure 5.4: The system can easily be destroyed by intruders

The most number of respondents (34%) disagreed. The above combination of those who are neutral (29%), agree (21%), strongly agree (4%), were respondents who seem to suggest that the system could be at risk of intruders easily destroying the systems. These threats are exogenous risks, which an organisation has no hold over, and are of activities not within the control of the organisation. There needs to be a system in place to protect against intruders.

Table 5.5: Employees of the organisation can damage the company's information system internally by themselves

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	8%	46%	21%	21%	4%	100%
No. of Respondents	2	11	5	5	1	24

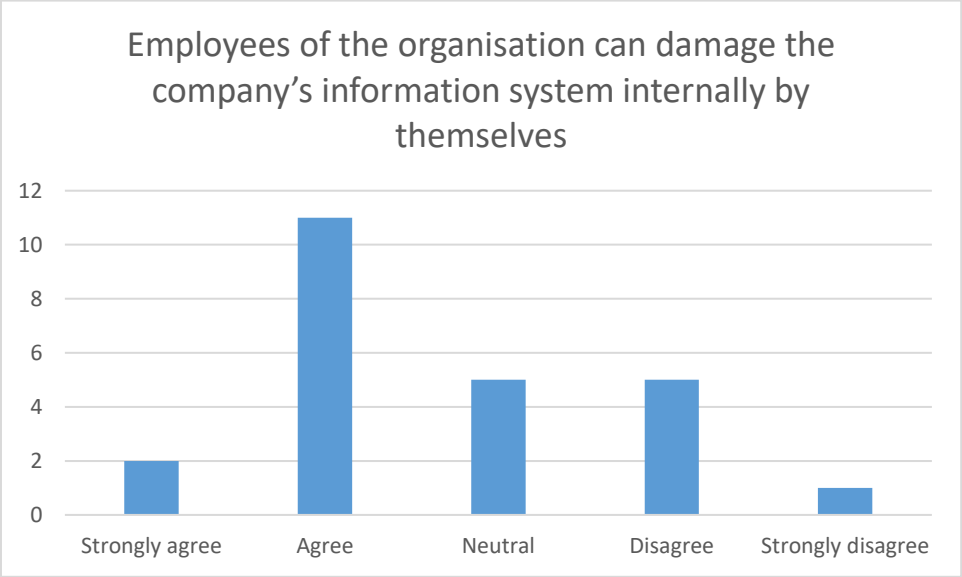


Figure 5.5: Employees of the organisation can damage the company's information system internally by themselves

The respondents who make up 54% of the sample seem to agree or strongly agree that the system is at risk of employees of the organisation damaging the company's information system by themselves. The most number of respondents (46%) agree with the statement. The neutral respondents are the same as those who disagree (21%) that there is such risk. This is a concern that more than half of the sample thinks the system is at risk of such threats.

An individual who is a threat to the company's information system is a Rager and a Saboteur. There needs to be detection or monitoring of email activities as the first step because they tend to use unacceptable language and threatening emails.

Table 5.6:The telecommunication and IT system are at risk of the following attacks:Terror attacks e.g. inter-country warfare

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	17%	33%	17%	29%	4%	100%
No. of Respondents	4	8	4	7	1	24

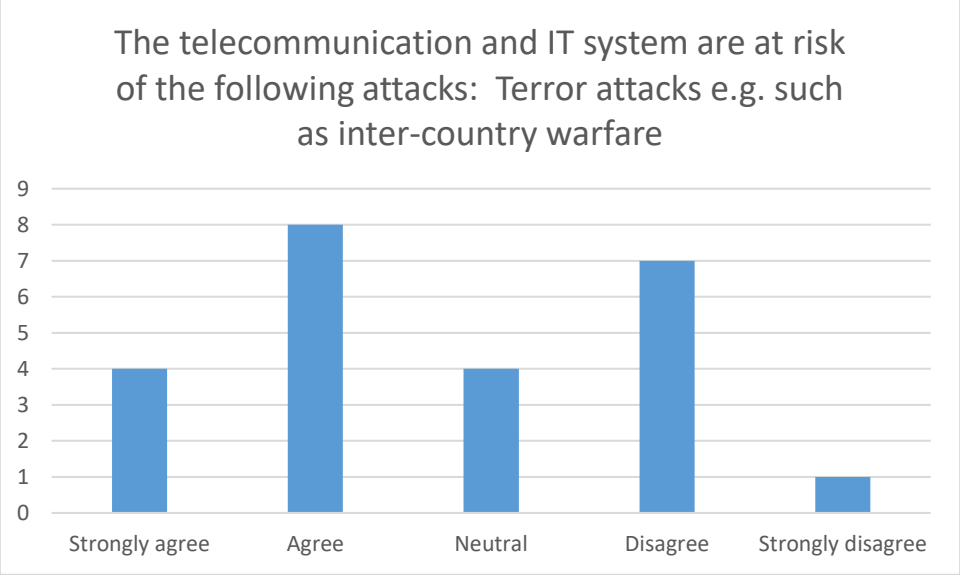


Figure 5.6: The telecommunication and IT system are at risk of the following attacks: Terror attacks eg such as inter-country warfare

Figure 5.6 and Table 5.6 show the breakdown of the respondents. The highest number of responses is from the group of respondents that agreed (33%) that the system was at risk of terror attacks. The second most group of respondents had disagreed (29%). The least number of respondents had strongly disagreed (4%).

The above responses show 50% of respondents strongly agree (33%) and agree (17%) that there are concerns regarding risk to telecommunication and IT systems of terror attacks. Those who strongly disagree (29%) and disagree (4%) are below (50%). The neutrals at 17% leave doubts as to where they stand.

Terror attacks bring undesirable effects – they are problems caused by humans. To this extent, they are equated to Human-made disasters. On the myths relating to recovery, Myth1 clearly states that plans cannot only be made for natural disasters. Thus, these kinds of disasters need to have incorporated plans. This extends to plans to replace employees should they lose their lives.

Table 5.7:The telecommunication and IT system are at risk of the following attacks: Technological threats e.g. cyber-attacks.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	29%	54%	4%	13%		100%
No. of Respondents	7	13	1	3		24

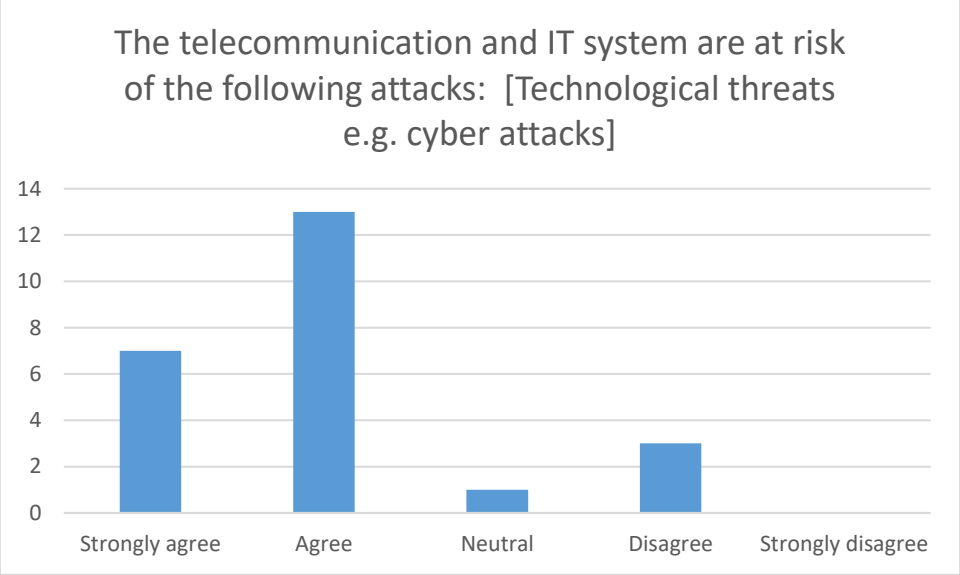


Figure 5.7: The telecommunication and IT system are at risk of the following attacks: Technological threats e.g. cyber-attacks.

The analysis of the response on technological threats seems to suggest a one sided bias with results that agree mostly than disagree with the statement. In Figure 5.7 above, the highest group of respondents agreed (54%), followed by those who strongly agreed (29%). They made up the most number of respondents in the sample on this statement. There was only one respondent (4%) who was neutral to the statement, with the second lowest being from the group that did not agree (13%). There was no one who strongly disagreed that the system was at risk of cyber-attacks. These were also very similar responses when it came to the analysis of the threat of telecommunication cables and telephone lines. The analysis has shown that over 50% of respondents agree and strongly agree that the system is at risk of threats that could hamper the system negatively.

Table 5.8: Criminal attacks, such as phone lines being damaged

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	8%	71%	8%	13%		100%
No. of Respondents	2	17	2	3		24

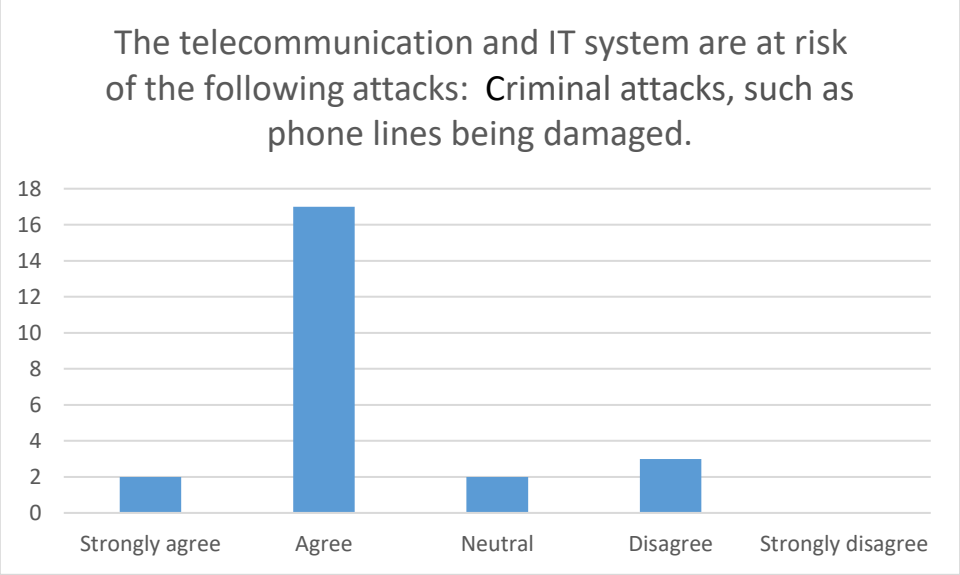


Figure 5.8: Criminal attacks, such as phone lines being damaged

The group with the highest number are those that agree (71%) that the telecommunication and IT system are at risk of criminal attacks such as to phone lines being damaged. They are followed by the few that disagree (13%) and those who are neutral and strongly agree (8%). However, the above statistics show that the number of those who agree are aware of the risks.

Table 5.9: Telecommunication and IT systems are at risk of the following attacks: Criminal attacks, such as cables being stolen.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	8%	71%	8%	13%		100%
No. of Respondents	2	17	2	3		24

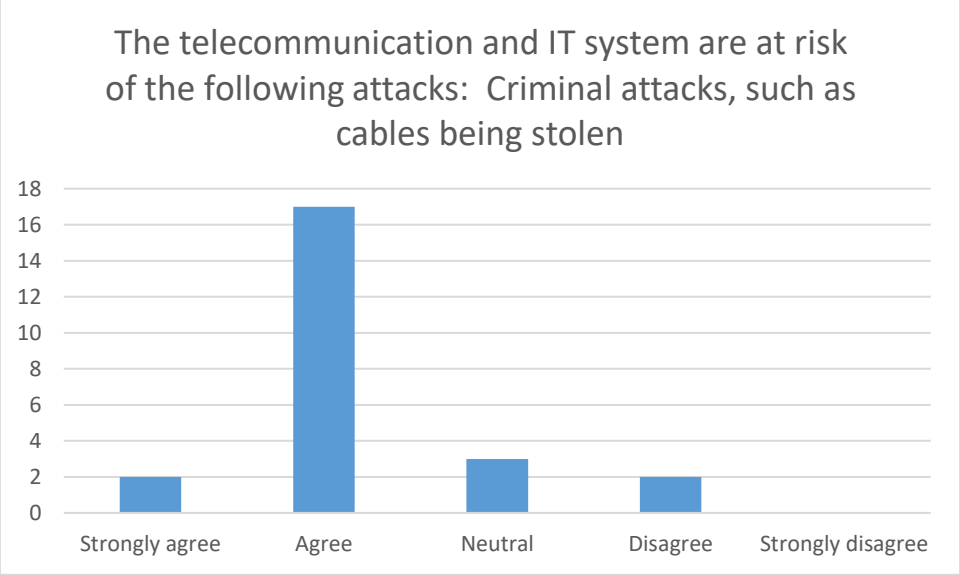


Figure 5.9: The telecommunication and IT system are at risk of the following attacks: Criminal attacks, such as cables being stolen

There was no respondent that strongly disagreed. However, there was a tie on those who were neutral and strongly agree (8%). The group of respondents who agreed (71%) that the cable in the IT systems were at risk of being stolen were more than the strongly agree respondents (8%). They make up the majority that believe that there are risks of criminal attacks, such as cables being stolen.

A mechanism is needed to support the system against all the threats that are related to Telecommunication and IT systems. These are attacks concentrated at the user's computer or internet connection, rather than the person using the computer. They are focused on pharming and the intent is to cause a system reconfiguration attack. There needs to be measures in place to control and limit such activities.

The telecommunication systems are used for the operational activities or the functioning of the Port MIS system. The systems are susceptible to such attacks and operational activities need to be guided by management procedures and governance policies. Defence mechanisms against such threats are needed.
The above is the last paragraph based on RQ1.

RQ2: What are prevalent risk assessment methods?

The second research question related to the prevalent risk assessment methods on Port MIS.

The questionnaire statements that addressed this research question were:

- There is a need for software that can automatically detect threats to the information system.
- Risk assessment methods are beneficial.
- Risk assessment methods help to minimise risks.
- There is a real time protection on the systems against threat.
- The system has protection against hackers.
- Connected to the system are only authorised users.
- Users are only limited to work on systems that affect their work.
- Software updates are done automatically to reduce the risks of threats.

Table 5.10: There is a need for software that can automatically detect threats to the information system

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	46	33%	17%	4%		100%
No. of Respondents	11	8	4	1		24

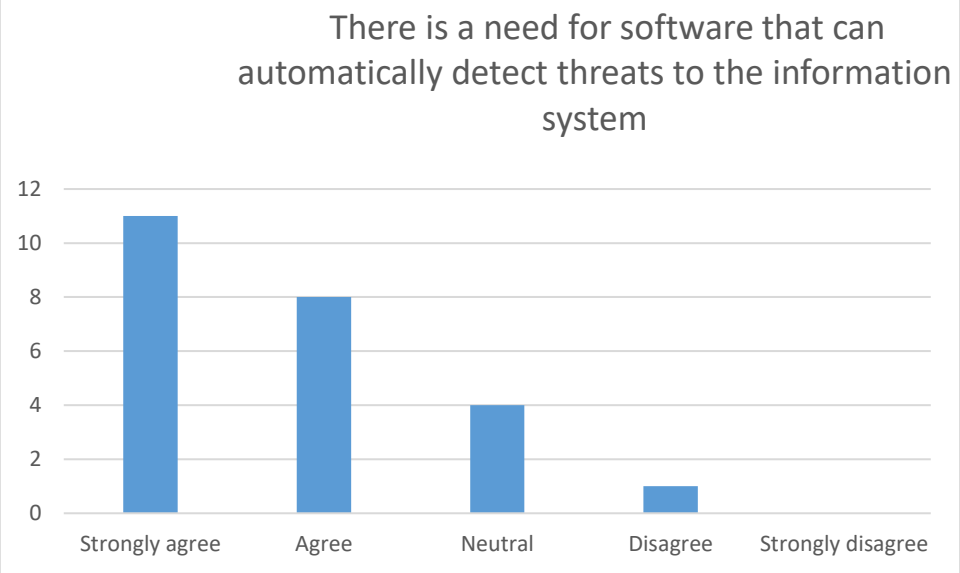


Figure 5.10: Employees of the organisation can damage the company's information system internally by themselves

Most respondents strongly agreed (46%) that there was a need for software that can automatically detect threats to the information system. The group that agreed (33%) followed this. The neutral respondents were 17%, along with those who disagreed (4%). There was no respondent that disagreed with the statement.

The above Figure 5.10 shows that the majority of respondents know that there is a need to detect threats to information systems. The few who do not know or disagree need to be aware of why IT software is needed to detect threats. It is software systems that detect threats to information. It is innovative software systems that are guarding against possible mischievous attacks from outsiders and insiders.

Table 5.11: Risk assessment methods are beneficial

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	46%	50%	4%			100%
No. of Respondents	11	12	1			24

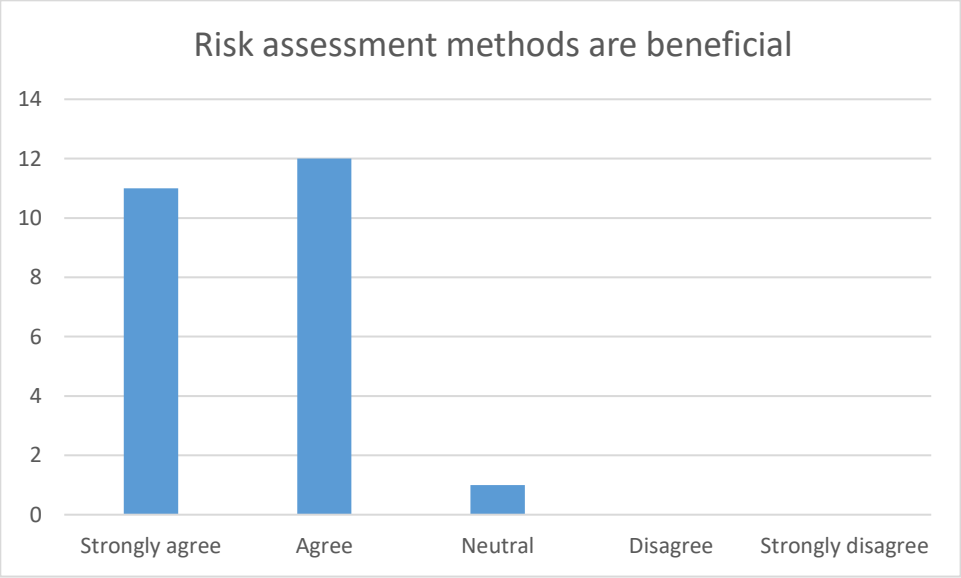


Figure 5.11: Risk assessment methods are beneficial

The most number of respondents (50%) agree as the majority that it is beneficial to have risk assessment methods. Those who strongly agree are 46%. There are only (4%) respondents that are neutral. The response indicates that the respondents know the benefits of risk assessment and feel that they are beneficial too.

This analysis shows that the majority of respondents do believe that having risk methods is beneficial. However, although needed, it is known that risk assessment as part of risk management is conducted by a person with the knowledge to assess. Risk also cannot be quantified. The method used needs to be qualitative, based on decision and instinct, which is based on the knowledge of the assessor.

Table 5.12: Risk assessment methods help to minimise risks

	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	46%	50%	4%			100%
No. of Respondents	11	12	1			24

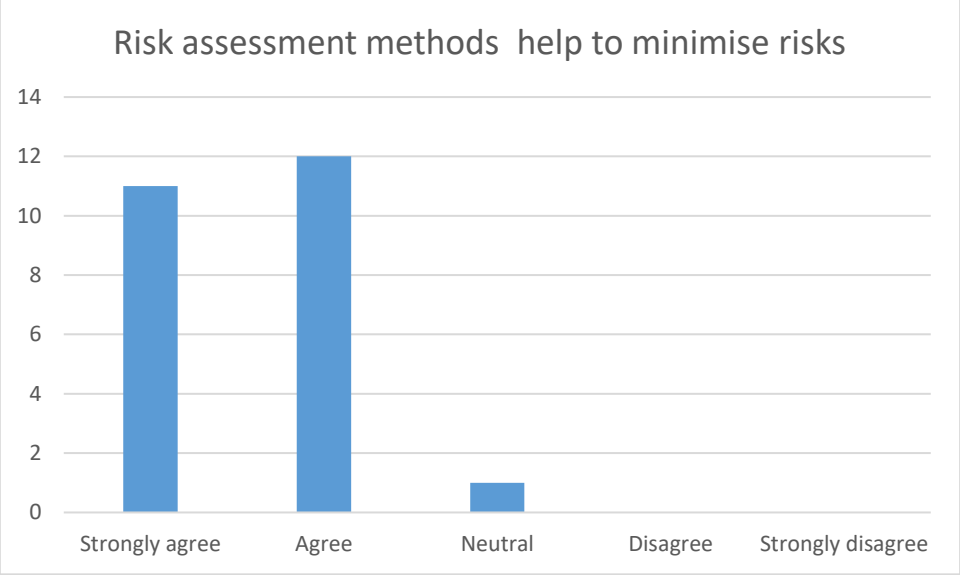


Figure 5.12: Risk assessment methods help minimise risks

The above Figure 5.12 is identical to the previous one, which gives a short analysis that the respondents also believe that risk assessment methods are both beneficial and help to minimise risks. This is confirmed by the fact the number who agree are the majority. There is only one respondent that was neutral and none disagreed or strongly disagreed.

It is known that organisations utilise risk based strategic assessment and planning techniques for security that is self-directed, such as an OCTAVE. This would mean that the organisation takes the initiative for setting its own self-directed organisational

security strategy. Self-directed means the organisation will take initiatives based on its individual needs and desires - of where it wants to be in its security detail and measures.

Table 5.13: There is real time protection on the systems against threat

	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	21%	50%	29%			100%
No. of Respondents	5	12	7			24

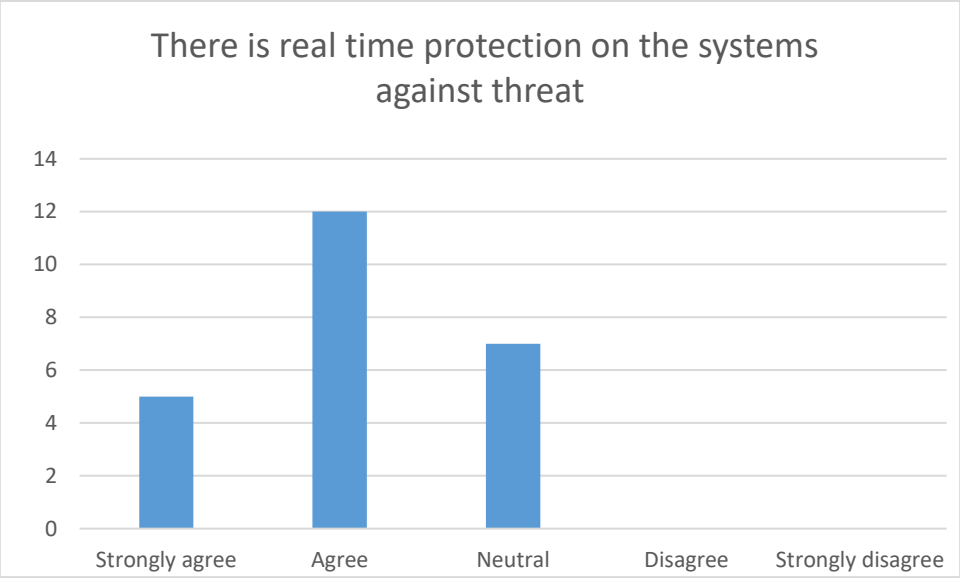


Figure 5.13:There is a real time protection on the systems against threat

Figure 5.13 and Table 5.13 show that the most number of respondents agreed (50%) that the system has real time protection against threats. However, a few strongly agreed (21%) as compared to those who are neutral (29%). A positive is that there are no respondents that disagree or strong disagree. The other observation is that there is no strong belief by the majority of the respondents about the real time protection.

A combination of 71% agree to strongly agree, believing in the need for protection in real time. Having had a look at real threats, another specific real time threat could be a hacker. This showed that there is an understanding that the system needs to have the benefits of real time information.

A methodology known as Near Real Time Statistical Asset Priority Driven (NRTSAPD) Risk Assessment methodology could be of advantage in measuring the number of

attacks on the system used for real time protection. This has elements that look into aspects and measures of probability, calculations of being attacked, number of incidents and impact on the business. This is a measuring method used to gauge the systems/software implementation against attacks.

Table 5.14: There is real time protection on the systems against threat

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	25%	42	33%			100%
No. of Respondents	6	10	8			24

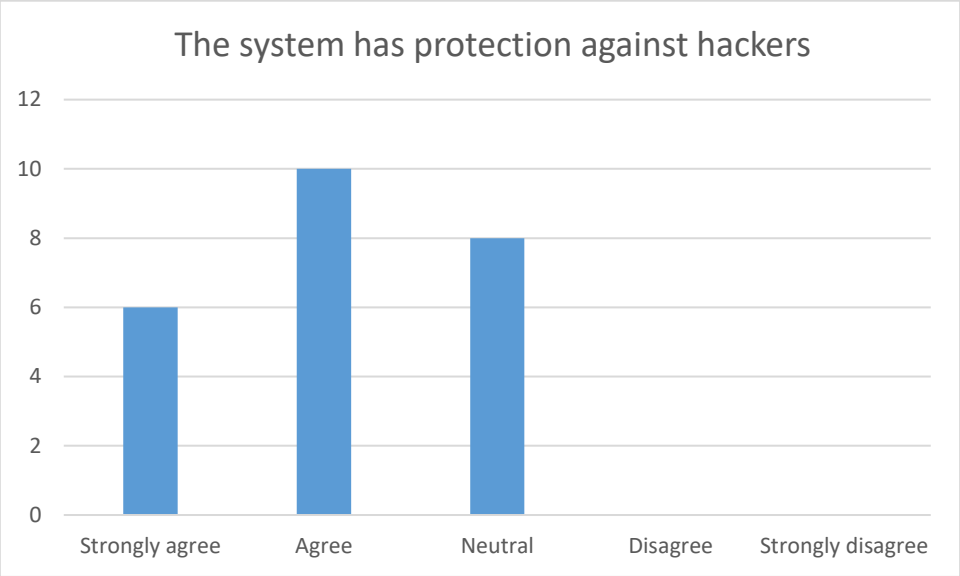


Figure 5.14: There is a real time protection on the systems against threat

The above shows that the statement that the system has real time protection is not understood in relation to hackers being real time threats. To analyse from an inside perspective on who could be a threat, there needs to be sophisticated software that will assist with real-time protection from individuals termed hackers.

Table 5.15: Connected to the system are only authorised users

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	50%	42%	8%			100%
No. of Respondents	12	10	2			24

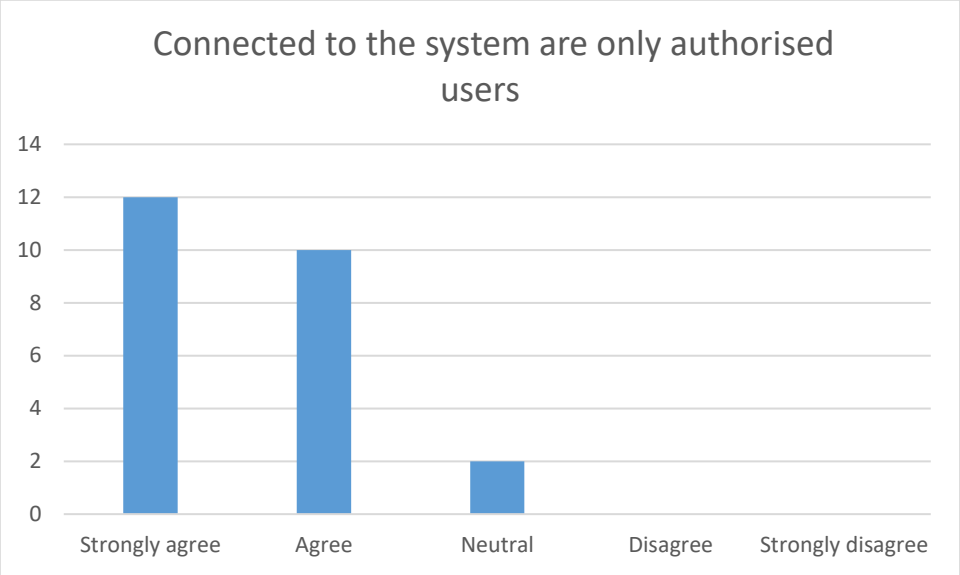


Figure 5.15: Connected to the system are only authorised users

The responses from the respondents are captured in Figure 5.15 and Table 5.15.There is an interesting revelation from the results. The number of respondents to strongly agree was 50% on the statement. They surpass the number of those that agree (42%) with a few neutrals (8%).

The majority of the respondents strongly agree and agree (92%) that connected to the system are only authorised users. There are only (8%) of users that are neutral to the statement. This shows that the only users who are connected to the system are authorised. The next statement assessed what the connected users work on. This was to better assess that the authorised users could not alter other users' systems intentionally.

Port MIS systems has only authorised users using the system. However, there is a need to be wary of careless users that could cause the loss of Intellectual Property (IP). There could be thieves with such intentions.

Table 5.16: Users are only limited to work on systems that affect their work

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	21%	71%	4%		4%	100%
No. of Respondents	5	17	1		1	24

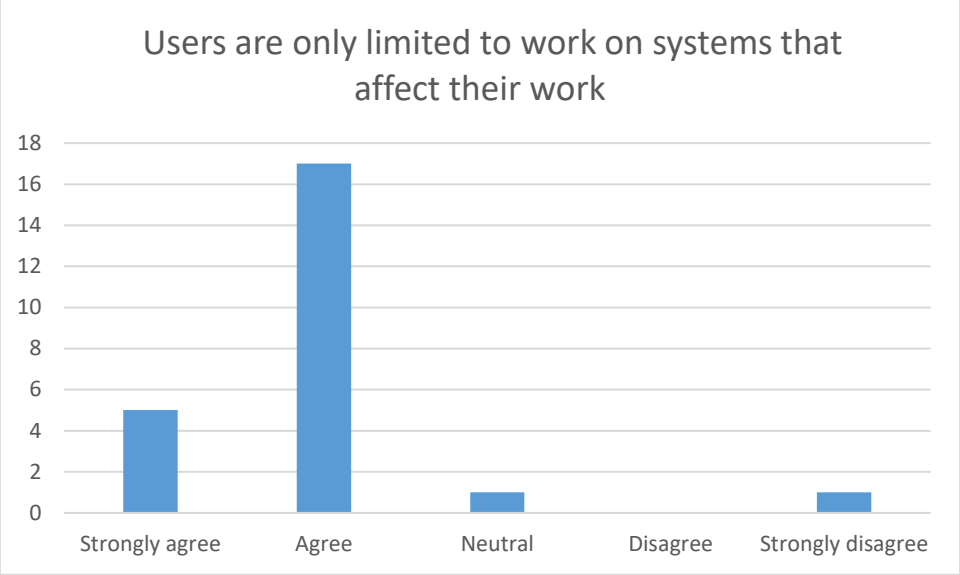


Figure 5.16: Users are only limited to work on systems that affect their work

The results show that at most they agree (71%), followed by the respondents that strongly agree (21%), that users are only limited to work on systems that affect their work. No respondent has disagreed. However, there were two respondents each (4%) that were neutral and strongly agreed.

It is safe to conclude that the majority agree and strongly agree that the systems have only users working on systems at work. However, a worry is that it was found with strong conviction that things are not all well with the majority. This could cause an alarm that there are careless users who disregard corporate IT policies, thus exposing the business to risk. There is a need to emphasise policies on the use of systems.

This leads to the last statement relating to RQ2. The statement related to software working on threats that could affect the system.

Table 5.17: Software updates are done automatically to reduce the risks of threats

	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	38%	54%	4%	4%		100%
No. of Respondents	9	13	1	1		24

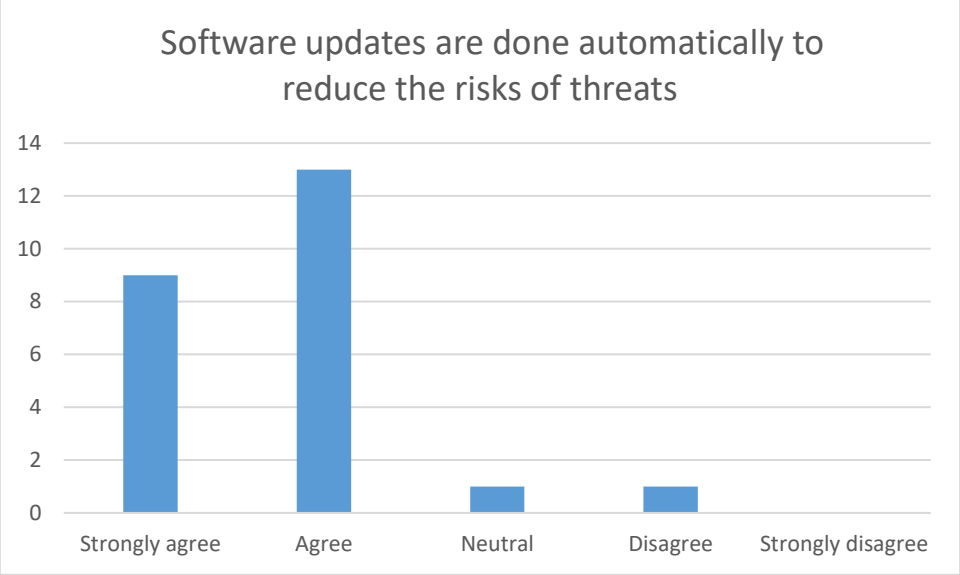


Figure 5.17: Software updates are done automatically to reduce the risks of threats

The results show that the respondents agree (54%) that software updates are automatically conducted to reduce the risk of threats. This is followed by the number of those strongly agree (38%) with the previously mentioned statement. There are only 2 other respondents who both disagreed and were neutral on this (4%). There was no respondent that disagreed with the statement. This leaves the results with the majority of respondents agreeing and strongly agreeing that software updates are done automatically to reduce the risk of threats. This analysis shows there was software that does automatic updates.

RQ3: What are the effects of risks to Port MIS and subsystems?

The third research question probed the understanding of what are the effects of risks to Port MIS and subsystems on Port MIS.

The questionnaire statements that addressed this research question were:

- External Customers' business with the organisation can be affected by the shutdown of the system.
- Data loss affects my department and the organisation as a whole.
- "Information system risks cause "poor system performance".

Table 5.18: External Customers' business with the organisation can be affected by the shutdown of the system.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	46	32	8	8	4	100%
No. of Respondents	11	8	2	2	1	24

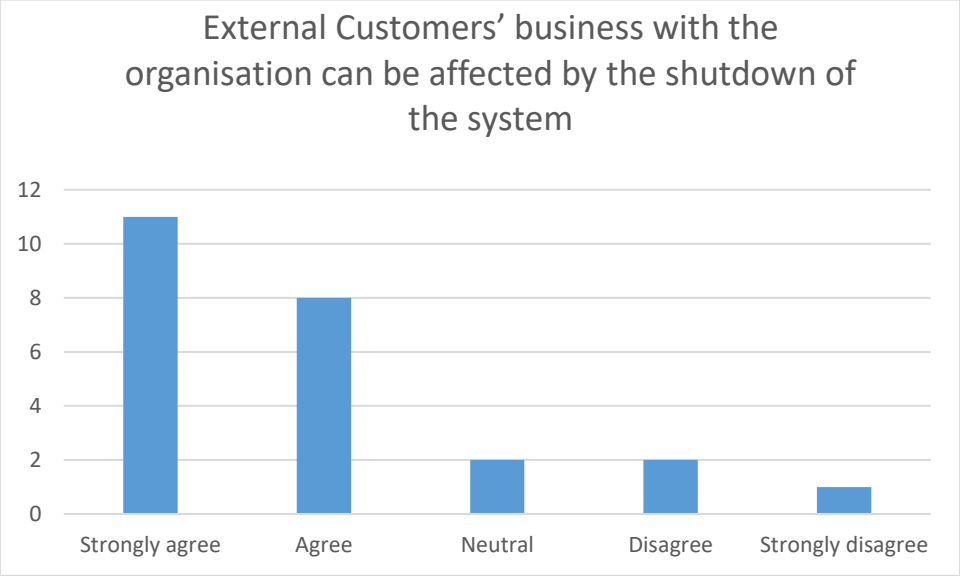


Figure 5.18: External Customers' business with the organisation can be affected by the shutdown of the system

The responses show that most respondents agree strongly (46%) that there were negative effects to external customers' business should there be a shutdown of the system. This is followed by the agree statement (32%). There is a tie on the neutral and disagree statement (8%) each, with only (4%) that strongly disagree. The majority of respondents showed an understanding of the effects of what a system shutdown can do to affect business affairs of the external customers.

This shows the importance of knowing of risk, as highlighted by Pak's (2008) assessment model. The impact of customers affected by a systems' shutdown or a security breach can have a large impact, thus it should be important to know when it happens. Managing risks help in securing business.

Table 5.19: Managing risks will help not to lose future or current business

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	54%	42%		4%		100%
No. of Respondents	13	10		1		24

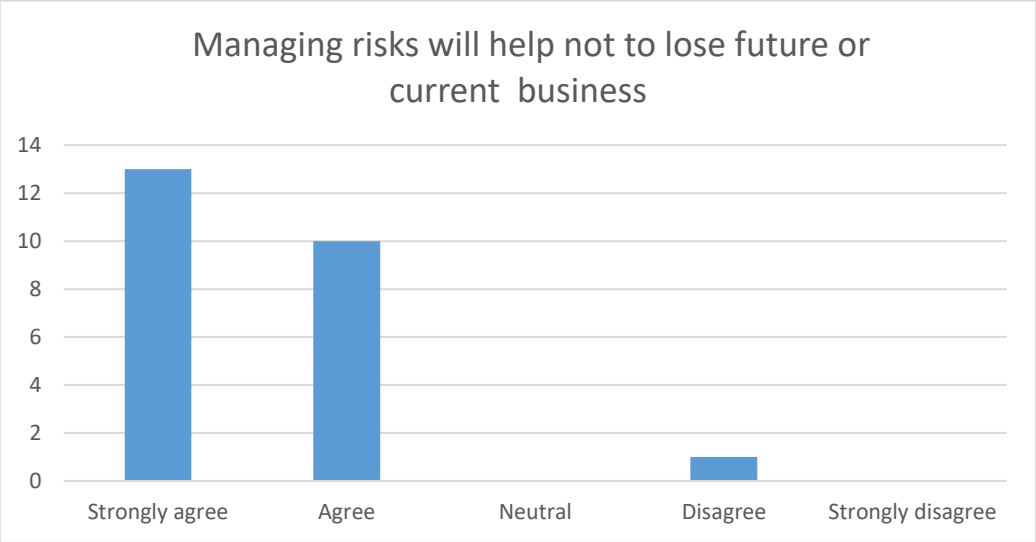


Figure 5.19: Managing risks will help not to lose future or current business

Figure 5.19 and Table 5.19 captured the responses relating to the statement on managing risks. The most number of respondents seem to strongly agree that reputation of managing risks precedes itself and helps not lose future or current business. Most respondents strongly agree (54%), followed by the number of respondents that agree (42%). There were no neutral or respondents that strongly disagree. There were only (4%) that disagreed that managing risks will help not to lose future or current business. Figure 5.18 above reveals that the majority of respondents strongly agree and agree that managing risks will help not to lose future or current business.

RQ3 included what the effects of data loss are. The next statement analyses the effects of when data is lost. This relates to both the department and whole organisation. The management of risks helps not to lose future or current business. However, there could be data loss during the process that also needs consideration.

Table 5.20: Data loss affects my department and the organisation as a whole

	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	58%	29%	8%	4%		100%
No. of Respondents	14	7	2	1		24

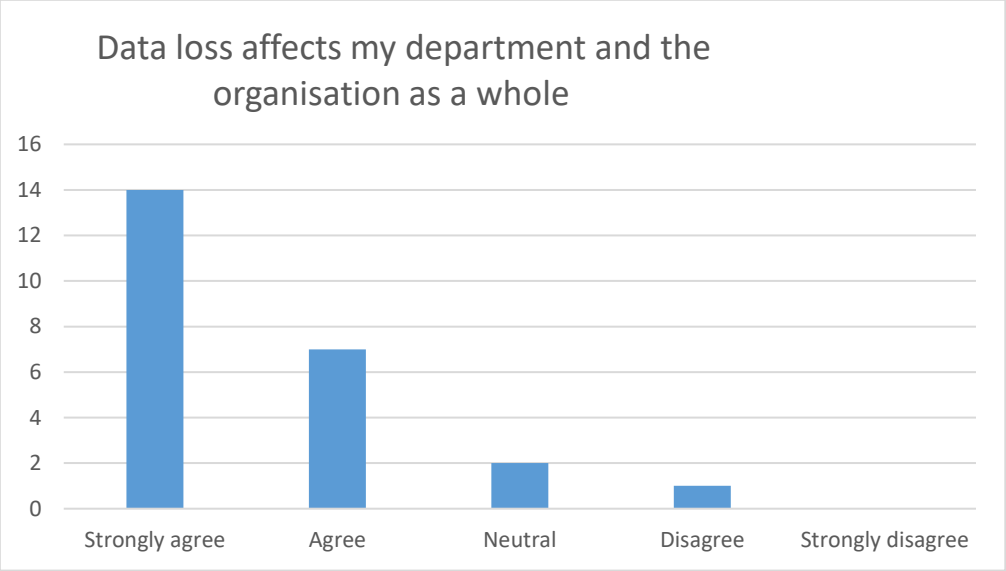


Figure 5.20: Data loss affects my department and the organisation as whole

Figure 5.20 and Table 5.20 have captured the responses on data loss. The most number of respondents seem to strongly agree (58%) that data loss has an effect on their departments and the entire organisation. This is followed by half the number that agree (29%), with (8%) that are neutral and (4%) that disagree. There was no respondent that strongly disagreed.

There is an overwhelming combination that strongly agreed and agree (88%) that data loss affects both their departments and organisation as a whole. Only a small number (12%) were neutral (8%) and disagreed (4%). There needs to be an understanding of different approaches and techniques to detect threats, as seen in Table 2.2.

Table 5.21: Information system risks cause financial risks e.g. loss of income

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	42%	46%	4%	4%	4%	100%
No. of Respondents	10	11	1	1	1	24

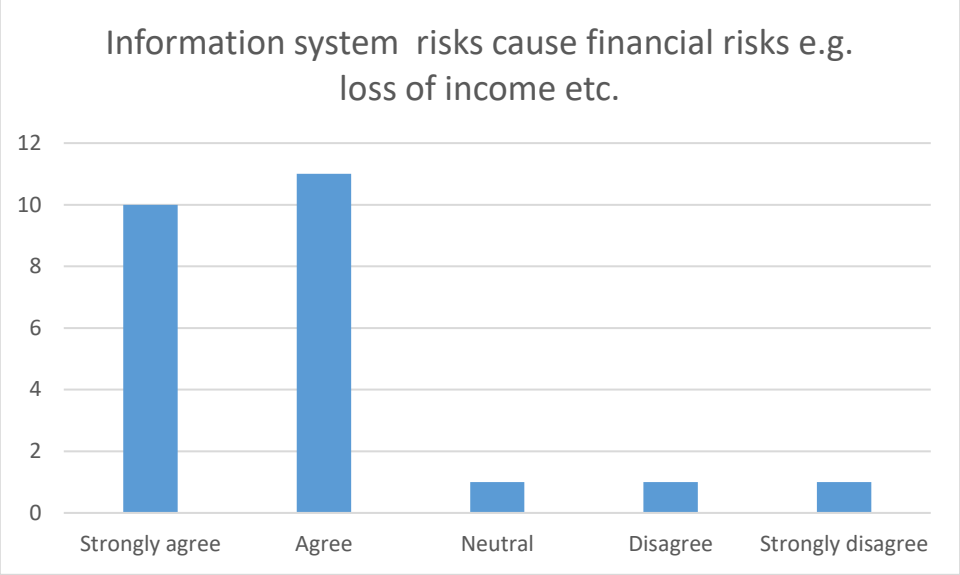


Figure 5.21: Information system risks cause financial risks e.g. loss of income etc.

The next statement of analysis looks into the effects of risk. The responses relating to the statement are captured in Figure 5.21 and Table 5.21. The most number of respondents seem to agree (46%) that information system risks have financial implications. This is followed by respondents that strongly agree (42%). 4% of respondents were neutral, disagreed and strongly disagreed. The results suggest that the majority of respondents seem to agree and strongly agree that there are financial risks that are related to information risks.

There are also risks relating to poor system performance. The respondents understood how risks affect the organisation. The effects, such as the financial risks, are the results.

RQ3 included analysis on how risks cause poor system performance.

Table 5.22: Information system risks cause poor system performance

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	25%	54%	17%	4%		100%
No. of Respondents	6	13	4	1		24

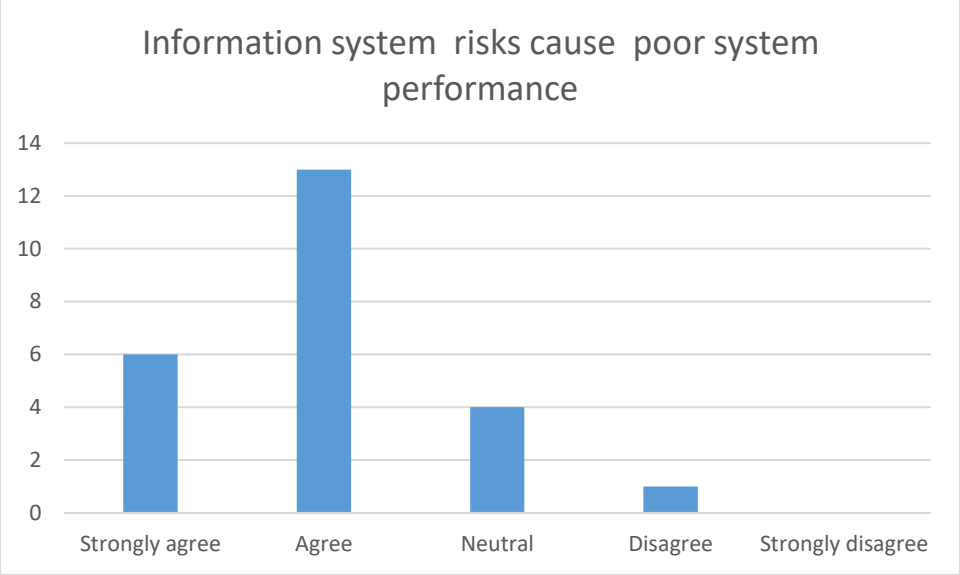


Figure 5.22: Information system risks cause poor system performance

The results on how risks cause poor system performance are shown in Figure 5.22 and Table 5.22. The most number of respondents seem to agree (54%) that information system risks cause poor system performance. This majority is followed by the number of respondents that strongly agree (25%). Respondents that are neutral were 17% and those that disagree were 4%.

The majority strongly agreed (25%) and agreed (54%) that Information System (IS) risk causes poor system performance. The 21% that are neutral and disagreeing show that a small number were not aware and along those who disagreed (4%).
This is the last statement relating to the RQ3 analysis.

The above responses provide convincing evidence that there is an understanding of risks relating to the organisation's business. This could relate to operational activities that are guided by management procedures and governance policies that define the defence mechanisms against threat. Their intention is to increase the level of defence on attacks or threats to IT resources.

RQ4: What is the importance of risk assessment?

The fourth research question probed the importance of risk assessments on Port MIS.

The questionnaire statements that addressed this research question were:

- "I am personally aware of threats that exist by being connected to the Internet".

- “Employees have adequate risk awareness of the use of information systems”.
- “The Company has regular risk assessments being conducted”.

The next section focuses on the importance of risk assessment and, like the previous research question, the analysis is based on a number of statements relating to the research question.

Table 5.23: I am personally aware of threats that exist by being connected to the Internet

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	25%	42%	17%	4%	12%	100%
No. of Respondents	6	10	4	1	3	24

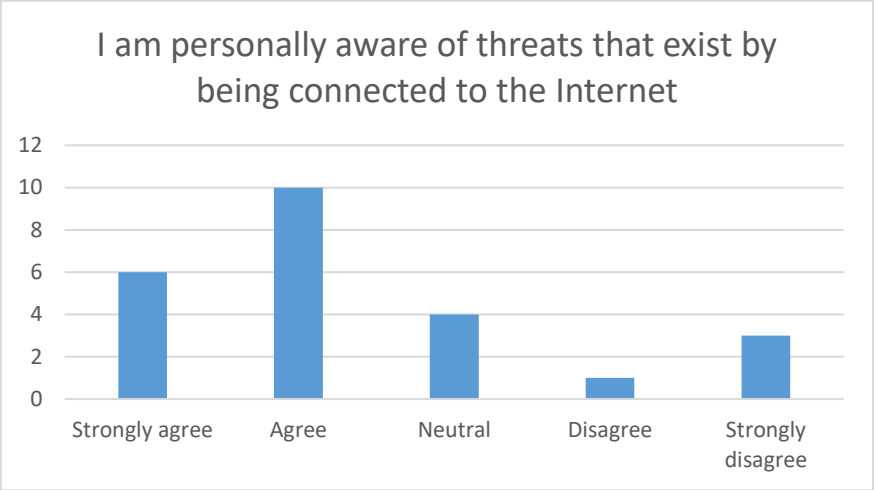


Figure 5.23: I am personally aware of threats that exist by being connected to the Internet

The first statement relating to RQ4 is on whether people are aware of threats relating to being connected to the internet. The results show that respondents in Figure 5.24 and Table 5.24 agreed (42%) that they are aware of threats that exist by being connected to the internet. Respondents that strongly agree (25%) with the statement followed. Respondents that were neutral (17%) were followed by respondents that strongly disagreed (12%), with the least disagreeing (4%).

These attacks are focused on the user’s computer or internet connections, not on the person using the computer. The focus is on pharming and the intent is to attack the

system reconfiguration. Telecommunication systems face such risks and the ideal would be to change the system's configuration.

Table 5.24: Employees have adequate risk awareness of the use of information systems

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	12%	46%	42%			100%
No. of Respondents	3	11	10			24

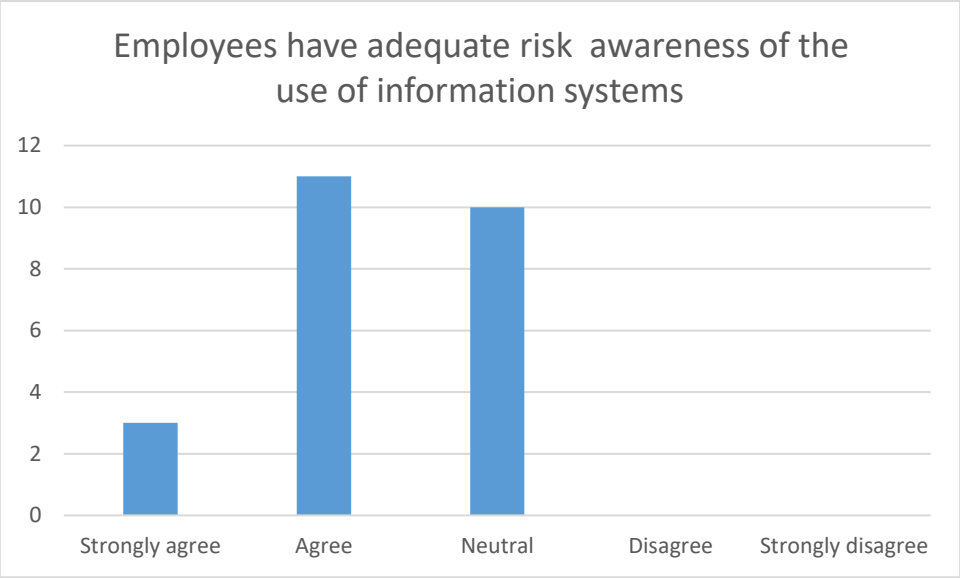


Figure 5.24: Employees have adequate risk awareness of the use of information systems

The next statement assesses the awareness of employees to information system risks. The results are captured in Figure 5.24 and Table 5.24. The results of the previous statement and current statement are conflicting somehow. The analysis shows that most of the respondents agree (46%) that employees have adequate risk awareness of the use of information systems. It is significant that the second most respondents are now neutral. Previously the group that was neutral was the group that strongly agreed.

The number of respondents that are neutral seem to have increased to 42%, as it was previously 17%. This has lowered from those who strongly agree with the statement that employees have adequate risk awareness of the use of information systems. None disagreed or strongly disagreed. The majority of those who agreed and strongly agreed has significantly gone down (13%). However, the neutrals went up (35%). It should cause alarm that awareness on the use of information system, when compared to the awareness on being on the internet, are not correlating.

This shows that a number of respondents are not aware of risk awareness strategies on the use of information systems. Clearly, risk awareness campaigns are not in place. This would also lead to query if the organisation does conduct regular risk assessments.

Table 5.25: The company has regular risk assessments being conducted

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	25%	54%	13%	4%	4%	100%
No. of Respondents	6	13	3	1	1	24

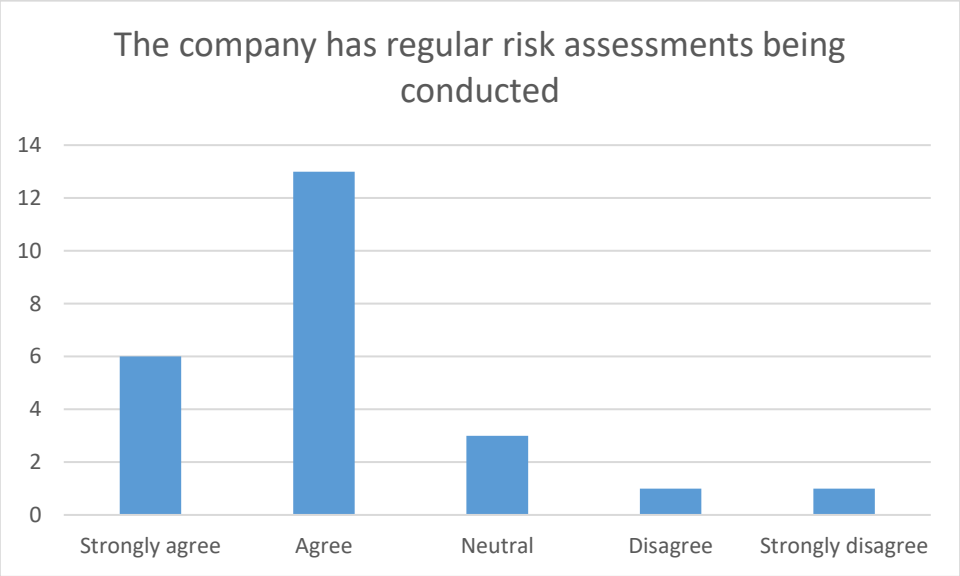


Figure 5.25: The company has regular risk assessments being conducted

The results on whether the company has regular risk assessments being conducted are on Figure 5.25 and Table 5.25. The results indicate that most respondents agree that the company has regular risk assessment being conducted. However, this result is quite alarming based on the inconsistency with the previous statement (Refer Table 5.24).

With a port being a high-risk organisation, it must not be assumed that users understand the purpose of IS assessments. Transnet is a high-risk organisation that conducts risk assessment on its operations. With caution exercised, the second most group was those that strongly agreed (25%) and the neutrals were lower (12%). The

two groups with similar results strongly disagree (4%) and disagree (4%). The two groups did not feature on the previous statement (Employees have adequate risk awareness of the use of information systems). This should cause alarm because users need to know more about risk assessments.

The combination of those who strongly agree and agree (79%) with the statement seem to be higher than the previous statement (58%). The individuals who are neutral have dropped. The neutral respondents have dropped significantly (38%). This huge change should be not be taken at face value as an improvement. However, it could be an understanding that regular risks assessments are done because of the nature of the environment where the system is used. Assessments are done on the ports, but not on the system itself.

Both need assessments to be done regularly. This is to mean that within the organisation, initiatives for setting the security strategy is lacking.

RQ5: What is the importance of risk management?

The fifth research question focused on the importance of risk management on Port MIS.
The questionnaire statements that addressed this research question were:

- Third parties handle risks to information systems at the same level as our organisation.
- The organisation's information system is protected from criminal elements by controlled access to them.
- Risk awareness campaigns that help to minimise risk should be conducted.
- Procedures help to minimise risk.
- The system can easily recover from technical disasters e.g. internet downtime.

Table 5.26: Third parties handle risks to information systems at the same level as our organisation.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	4%	38%	42	16%		100%
No. of Respondents	1	9	10	4		24

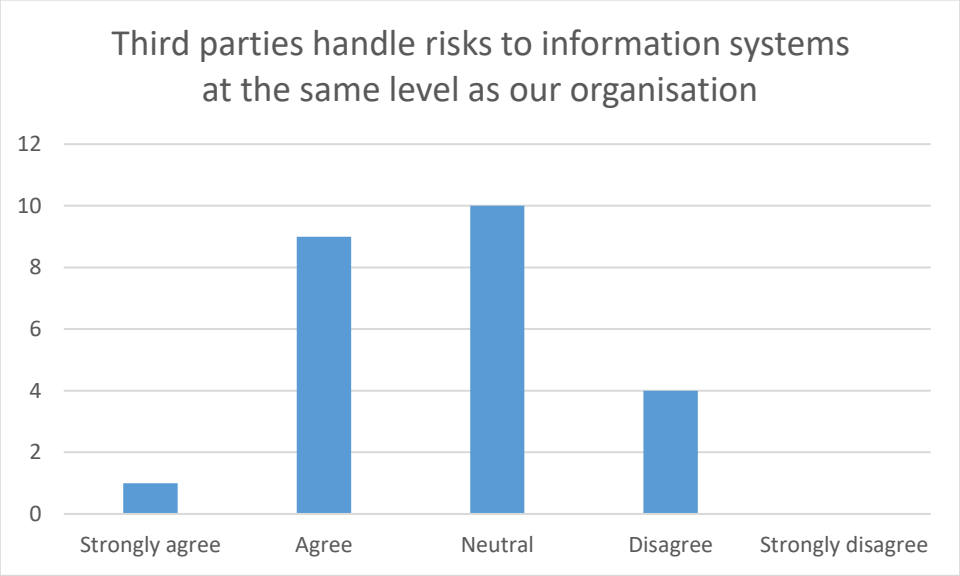


Figure 5.26:

Third parties handle risks to information systems at the same level as our organisation.

Figure 5.26 and Table 5.26 show the importance of risk assessment and enquiring how the third parties handle risk to information systems. Do they take precautions at the same level as the organisation? It was found that the most number of respondents were neutral (42%) to the statement. The second highest group of respondents agreed (38 %). The third highest group disagreed (17%) with the least group of respondent agree (4%). There is no respondent that disagree.

It is important to know that both internal and external parties handle risks at the same level in the organisation where they work. It is a known fact that in outsourcing, organisations collaborate with companies that can provide them with IT systems to help their own business. In return, companies offer them incentives for taking the risks. These strategic partners are remunerated well and they need to match the organisation's standards, if not better them. A company will need to collaborate with organisations that meet or exceeds their expected standards in handling threats.

Table 5.27: The organisations' information system is protected from criminal elements by controlled access to them.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	33%	42%	25%			100%
No. of Respondents	8	10	6			24

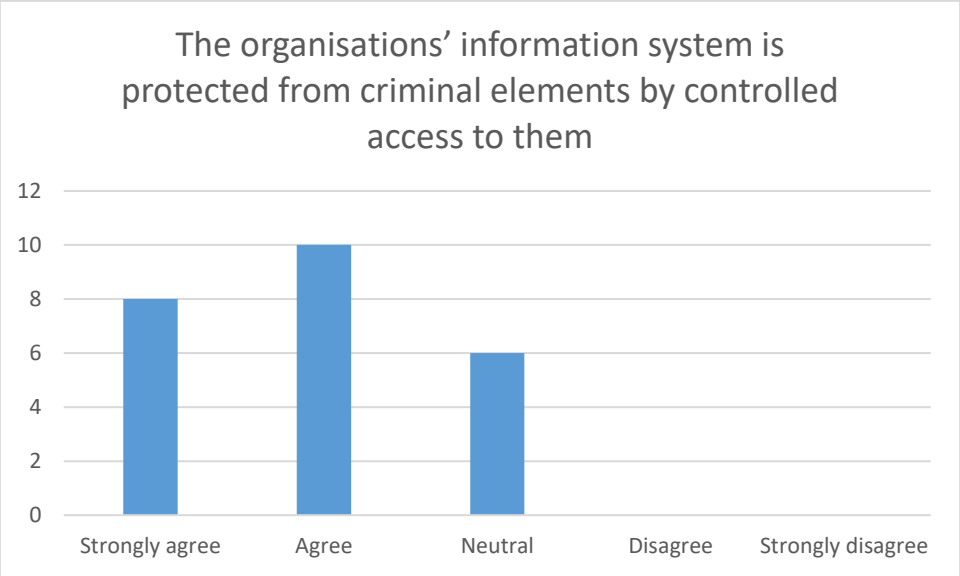


Figure 5.27: The organisations' information system is protected from criminal elements by controlled access to them

The impact of criminal elements has been captured in Table 5.27 and Figure 5.27.The analysis shows that the most number (42%) of respondents agree with the statement. The next group (33%) strongly agrees and the last set of respondents (25%) were neutral. There were no respondents that disagreed and strongly disagreed. It is known that a significant number of organisations assign enormous funds for IT security, thus the employees feel that the systems are doing their best to filter criminal elements.

Table 5.28: Testing recovery plans should be done routinely.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	50%	50%				100%
No. of Respondents	12	12				24

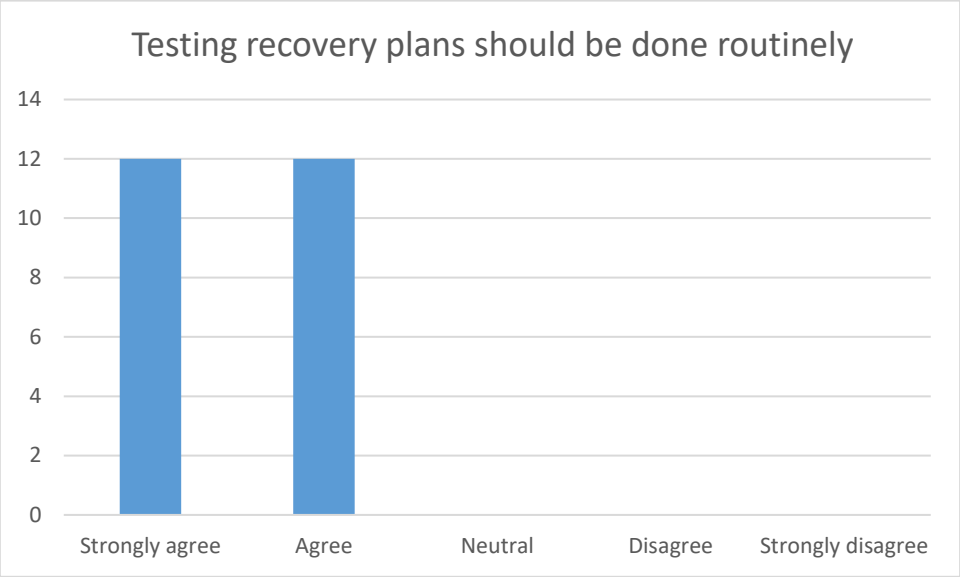


Figure 5.28: Testing recovery plans should be done routinely

The results of the statement that testing recovery plans should be done routinely are captured in Figure 5.28 and Table 5.28. The analysis shows that half agree (50%) and strongly agree (50%).

The analysis of the above shows that it is a one-sided choice – the respondents all agreed that testing the recovery plan should be done routinely. The above could be cause for alarm as it reveals that there is a need for testing of recovery plans to be done routinely. On system recovery, the myth is that any plan that has never been fully tested is useless – emphasising that the Port MIS recovery plan does need to be regularly tested. The respondents agree with this.

Table 5.29: Risk awareness campaigns to help minimise risks should be conducted

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	42%	58%				100%
No. of Respondents	10	14				24

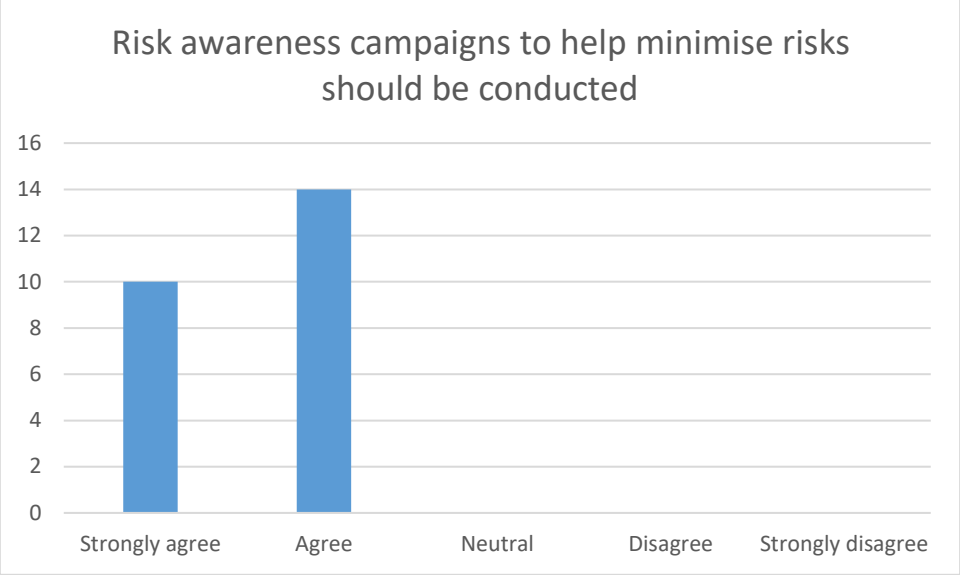


Figure 5.29 : Risk awareness campaign to help minimise risks should be conducted

The results of the statement that risk awareness campaigns help to minimise risk are captured in Figure 5.29 and Table 5.29. Most of the respondents agreed with the statement that risk awareness campaigns help to minimise risks when conducted. There were no neutral, disagreeing and strongly disagreeing respondents.

The combination of those who agree and strongly agree confirms that the respondents feel that risk awareness campaigns do help to minimise risks and should be conducted. However, the issue is that there is no strong conviction by a majority on the statement. This should be a concern as it confirms that there is a need to have risk awareness campaigns to help minimise risks. The same point was recognised on testing recovery plans. Risk awareness should entail knowing the disaster recovery sites as employees should not be found wanting during disasters.

Table 5.30: Procedures help to minimise risks

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	46%	46%	8%			100%
No. of Respondents	11	11	2			24

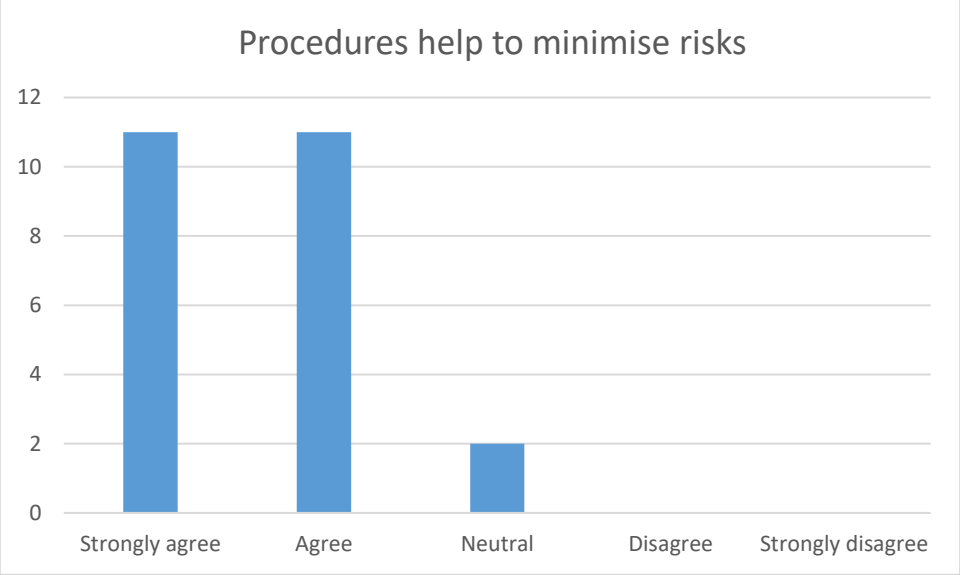


Figure 5.30: Procedures help to minimise risks

The results of the statement that Procedures help to minimise risks were captured in Figure 5.30 and Table 5.30. The analysis shows that the same number of respondents chose strongly agree and agree (46%) that procedures help to minimise risks. The neutral group represented (8%). No respondents disagreed.

The combination of respondents that were in favour of procedures to minimise risks was 92%. This is a combination of those who agree (46%) and strongly agree (46%). This shows that respondents understand that procedures really help to limit risks to information systems. Spremu (2012) in Chapter 2 mentioned that procedures for managing IT risks at business unit level or functional level should follow set standards and norms set by international regulatory bodies. The organisation would have to follow such standards to help to minimise risks.

Table 5.31: The system can easily recover from man-made disasters such as fires.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	17%	58%	21%	4%		100%
No. of Respondents	4	14	5	1		24

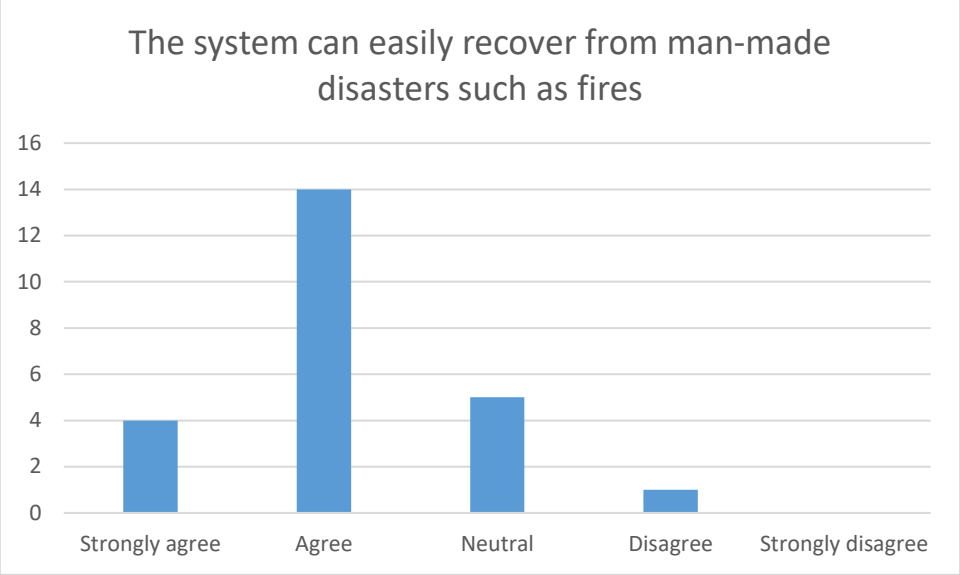


Figure 5.31: The system can easily recover from man-made disasters such as fires

With the procedures in place, another aspect to consider is unforeseen circumstances. The results for the statement that the system can easily recover from disasters are in Figure 5.31 and Table 5.31. The highest number of respondents agree (58%) that the system can easily recover from man-made disasters such as fires. The second most number (21%) of respondents seem to be neutral. The third most number (17%) of respondents strongly agree, with the last (4%) respondents disagreeing with the statement. There is no respondent that has strongly disagreed.

There is a significant number of respondents that strongly agreed and agreed (75%) that the system can easily recover from man-made disasters, such as fires. The analysis showed that the majority of respondents agreed and strongly agreed that the system can recover from disasters.

Table 5.32: The system can easily recover from man-made disasters such as vandalism.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	17%	54%	17%	8%	4%	100%
No. of Respondents	4	13	4	2	1	24

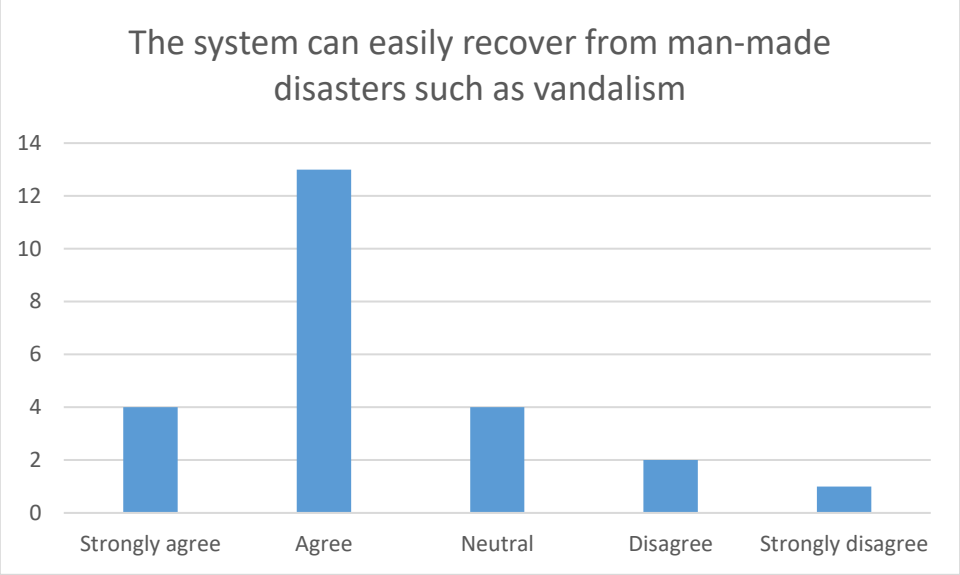


Figure 5.32: The system can easily recover from man-made disasters such as vandalism

The results of the statement that the system can easily recover from man-made disasters such as vandalism was captured in Figure 5.32 and Table 5.32. Most respondents agree that the system can recover from vandalism. There is however, a difference between vandalism and fire recovery. The results are inconsistent although they are both man-made disasters. There is a drop in those who agreed from recovery of fires (63%) to those in vandalism (54%).

The number of respondents that agreed and strongly agreed have declined (71%). The increase was noted on the combination of those who are neutral, disagree and with those who strongly disagree (29%).

The results on the statement that the system can easily recover from technical disasters such as internet downtime was captured in Figure 5.33 and Table 5.33.The analysis shows that most of the respondents agree (63%) that the systems can easily recover from technical disasters. This is followed by the second most number of neutral respondents (25%).

Table 5.33: The system can easily recover from technical disasters such as internet downtime

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	12%	63	25%			100%
No. of Respondents	3	15	6			24

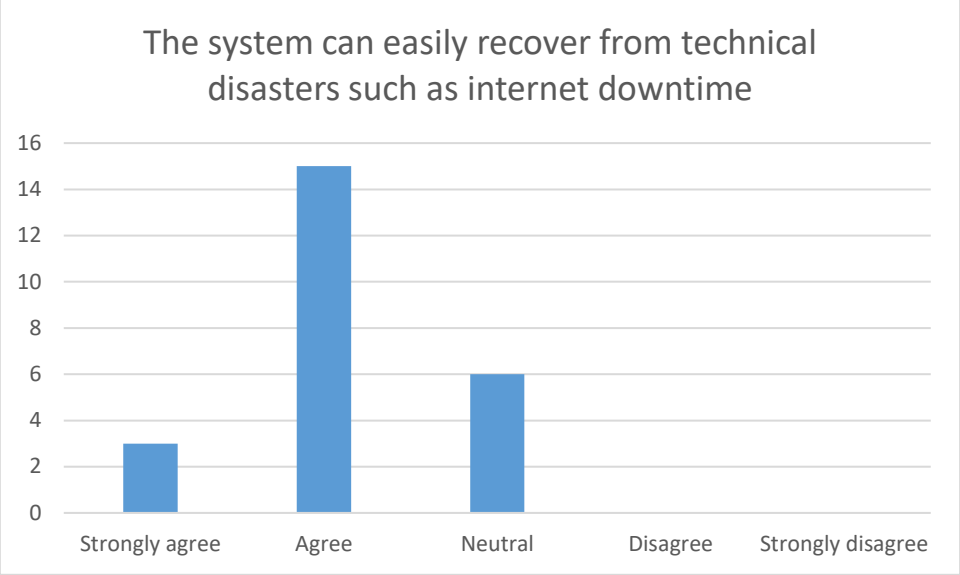


Figure 5.33: The system can easily recover from technical disasters such as internet downtime

The number of respondents that agree (63%) and strongly agree (12%) made up the most number of respondents. This result shows that the system can recover with ease from technical disasters. The concern is the number of those that are neutral (25%), meaning that they are not aware of what would happen in the case of technical disasters. Awareness of what to do when disaster strikes take into consideration that users need to be informed of what to do when risk awareness campaigns are conducted.

Table 5.34: The system can easily recover from natural disasters such as floods and storms

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	12%	59%	17%	8%	4%	100%
No. of Respondents	3	14	4	2	1	24

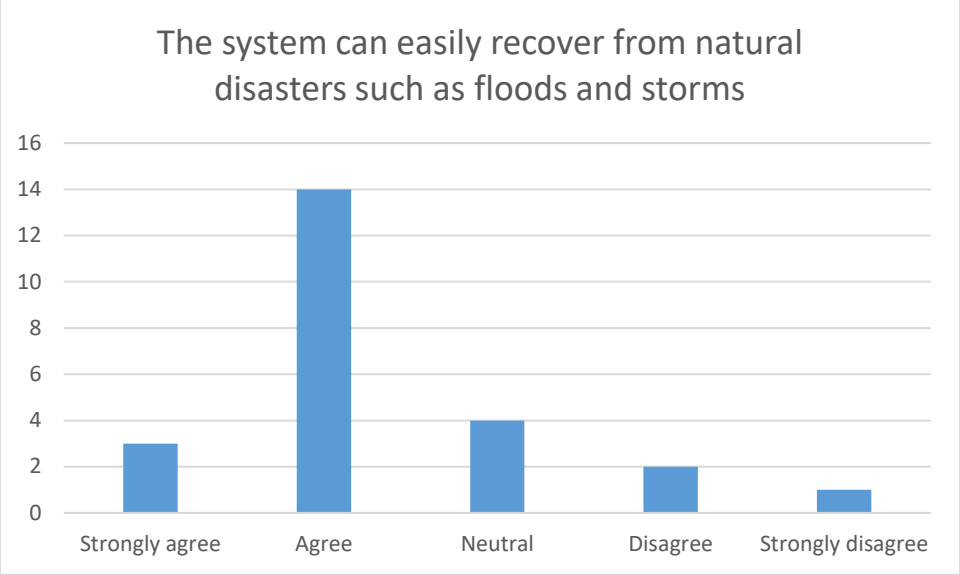


Figure 5.34: The system can easily recover from natural disasters such as floods and storms

The results of the statement that the system can easily recover from natural disasters such floods and storms are shown in Figure 5.34 and Table 5.34. The results seem to have risen. The number of respondents that agree are 59%. The second most respondents (17%) are neutral. Responses proved to be different to the previous statement. More respondents were neutral or disagreed.

The analysis from technical disasters shows a decline in the number of those who both agree and strongly agree – when compared to the responses to technical disasters. The results might indicate that there is a concern worth noting relating to recovering from disaster.

Management must note that recovery is a critical aspect to consider. On the system, recovery plans have been mentioned - that centrally coordinated planning for disaster recovery (DR) is a must. In addition, it was pointed out that the greater and more compound the business, the more empirical it becomes. There has to be a centralised process for all DR plans, so that each separate division or other entities are not duplicating the practice. Although these are independent disasters, they should be centrally coordinated.

The disaster recovery planning has to cater for all kind of disasters. The management should also inform users that both natural and unnatural disasters carry the same risks for the business.

RQ 6: Do all eight ports in South Africa attach the same level of importance to risk assessment for their Port MIS?

The sixth research question asked about the level of importance of risk management on Port MIS at each port.

The questionnaire statements that addressed this research question were:

- Risk assessment is continuously conducted on my department.
- There are risk assessment standards on my department.
- The organisation has the same risk assessment standards across all ports.

Table 5.35: Risk assessment is continuously conducted on my department.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	29%	38%	21%	12%		100%
No. of Respondents	7	9	5	3		24

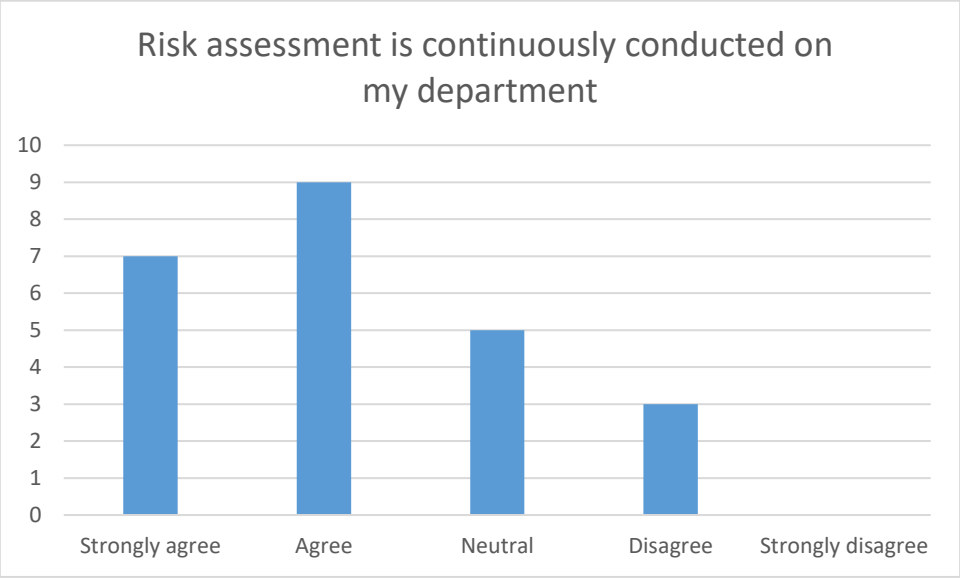


Figure 5.35: Risk assessment is continuously conducted on my department

This section is a discussion of the statements relating to understanding if all eight ports in SA attach the same level of importance to risk assessment for their Port MIS. The respondents' responses were captured in Figure 5.35 and Table 5.35.

38% of the respondents agree that risk assessment is continuously conducted in their departments. The second most number (29%) of respondents strongly agreed with the

statement. The third most number (21%) of respondents were neutral, with the least (12%) group disagreeing with the statement. There is no strong conviction on the agreement that departments have risk assessments done continuously. This could be alarming and needs managerial action. Risk assessments should be guidelines or standards that need to be in place.

67% of respondents agreed and strongly agreed that risk assessments were done in their departments. Those that disagreed and were neutral showed that there is a possibility that IS Risk assessment is not continuously conducted in their departments. There should be a mandate ensuring that IS risk assessment is continuously conducted in all departments.

Table 5.36: There are risk assessment standards in my department.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	25%	67%		8%		100%
No. of Respondents	6	16		2		24

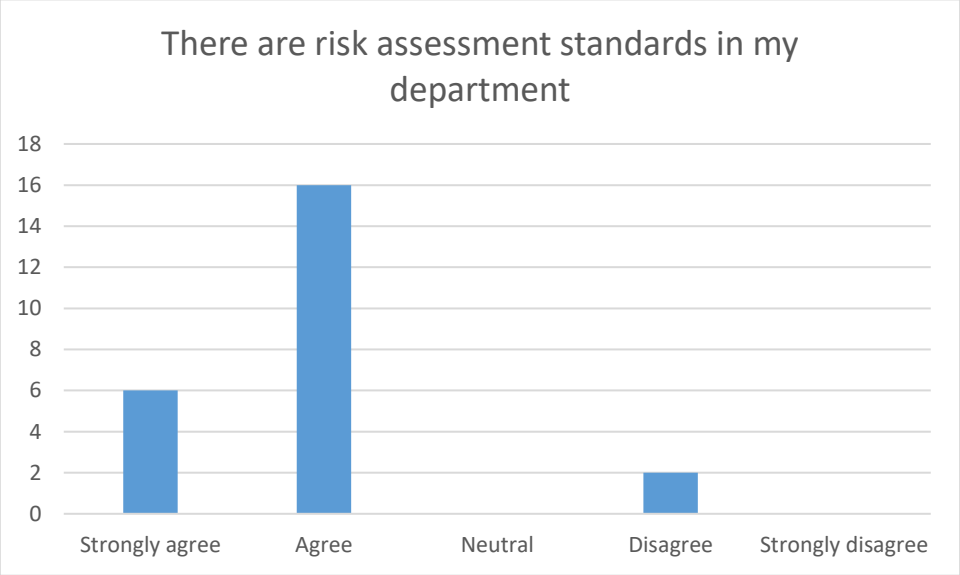


Figure 5.36: There are risk assessment standards in my department

This statement probed if there were risk assessment standards in relation to departments that claim to have assessments conducted. The results of the statement are shown in Figure 5.36 and Table 5.36.

The most number of respondents (67%) agreed that there are risk assessment standards in their departments. There are, however, inconsistencies with the previous results that probed if risk assessments are continuously conducted in departments. The respondents agreed (67%) compare to the previous (38%).

This reveals that there are risk assessment standards. However, they are not properly implemented. The second most respondents were those who strongly agreed (25%). There were 8% of respondents that disagreed, with none on neutral and strongly disagree. The respondents who agreed and strongly agreed made up over 50% of the results. However, they were not strong on conviction. They should apply OCTAVE, which is a methodology known to be better for self-directed teams as in departments. This would help to maintain standards that are internationally recognised, such as NRTSAPD, which is used to assess real time threats.

The number of respondents that agreed and strongly agreed have gone up when compared to the previous statement: 67% from 29% of respondents. This highlights that there are standards, but they are not used in assessing the system risks or they could relate to other matters within the Transnet group. The respondents who were neutral have also diminished (to 0%), lower than the individuals that disagree. This is a contrast worth noting for remedial action and recommendations. This led to the last analysis statement for RQ6.

The next statement encompassed all the ports.

Table 5.37: The organisation has the same risk assessment standards across all ports

	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	33%	46%	21%			100%
No. of Respondents	8	11	5			24

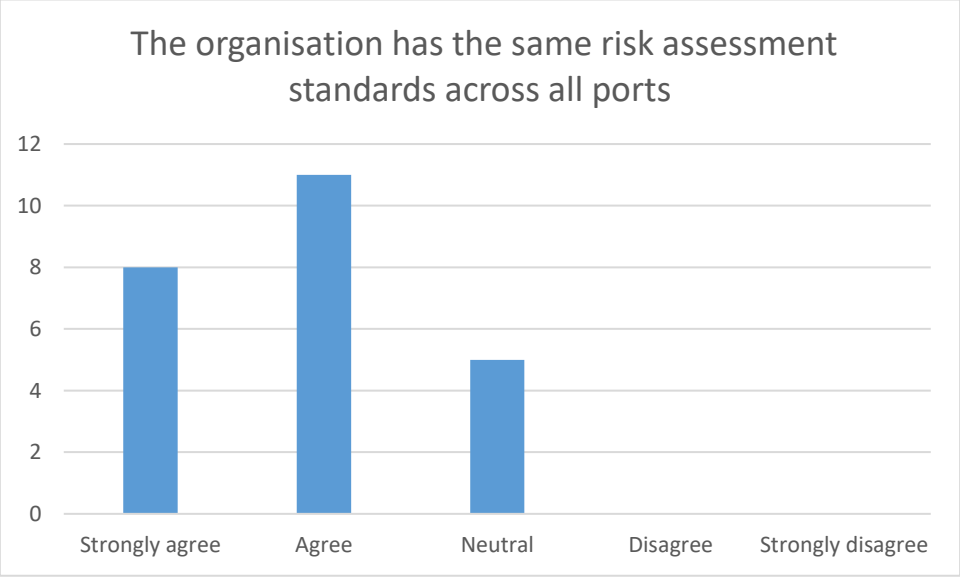


Figure 5.37: The organisation has the same risk assessment standards across all ports

The purpose of this next statement was to find out if there were consistencies in the way risk was managed in all ports. The results of the statement that the organisation had the same risk assessment standards across all ports is shown in Figure 5.37 and Table 5.37.

The most number of respondents agreed (46%) that the organisation had the same risk assessment standards. The second most respondents also strongly agreed (33%) and the last group was neutral (21%). There were none that disagreed and strongly disagreed. There was inconsistency in the numbers of those that agreed and strongly agreed, with the new total being 79%, a slight decline from the 83% of the respondents. There is also growth of the neutrals, who moved up to 21% from none. This could imply that other respondents were not aware if the same standards were applied across all ports.

RQ6 exposed huge discrepancies in how risk assessments are done, although standards were available and being applied across all ports. All ports did not have the same standards applied. The statements revealed that there are risk assessment done, but the use of the same standards is not a certainty. This means that standardisation is needed.

RQ 7: How can a risk management strategy be standardised for all eight ports?
The seventh research question asked how risk management strategies could be standardised for all eight Ports.

The questionnaire statements that addressed this research question were:

- It is ideal to have policy guidelines for Transnet employees for the use of information systems.
- Disaster recovery plans are a “must-have" for Transnet operations.
- Employees on the internet should be protected from online threats.
- There should be an overall organisational strategy on Risk Management for Port MIS.

Table 5.38: It is ideal to have policy guidelines for Transnet employees for the use of information systems

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	67%	33%				100%
No. of Respondents	16	8				24

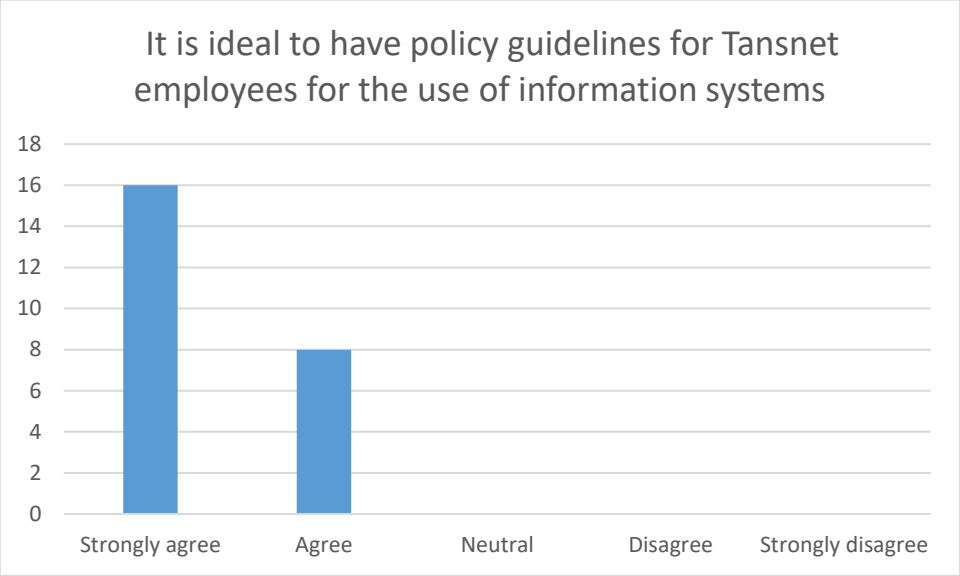


Figure 5.38: It is ideal to have policy guidelines for Transnet employees for the use of information systems

The results of the statement that it was ideal to have policy guidelines for Transnet employees for the use of information systems is shown in Figure 5.38 and Table 5.38.The results show that most respondents strongly agreed (67%) that it is ideal to have policy guidelines, with the second most group agreeing (33%) with the statement. There were no other responses on the statement. The finding was that respondents mostly strongly agreed that it was ideal to have policy guidelines for Transnet employees for the use of information systems. This aligns with the fact that the respondents had only chosen the option to agree and strongly agree. This reveals that there is a need for policy guidelines on the use of information systems.

Organisations have numerous information security policies and procedures to protect themselves against risks. These policies are to decrease and prevent the planned or unintentional actions of staff that could deteriorate the efficiency of the hardware and/ or software protection systems. This would reduce their usefulness. Respondents clearly have a good understanding of what policies could do to help to manage risks relating to Port MIS.

Table 5.39: Recovery plans after disasters is a “must-have" for Transnet Operations

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	63%	33%	4%			100%
No. of Respondents	15	8	1			24

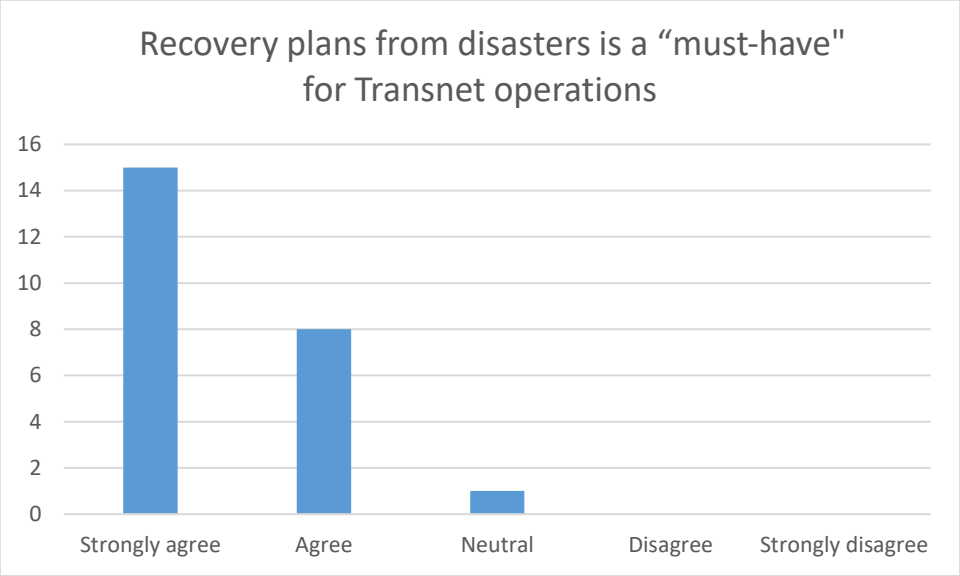


Figure 5.39: Recovery plans from disasters is a “must-have" for Transnet operations

The results for the statement that recovery plans after disasters was a “must-have" for Transnet operations is shown in Figure 5.39 and Table 5.39.The most number of respondents strongly agree (63%) that disaster recovery plans is a ‘must have’ for the organisation. The second most group also agrees (33%), but only to have one (4%) at neutral. This analysis shows that disaster recovery plans are necessary.

Close to 100% of respondents agree and strongly agree that disaster recovery plans are necessary. DR site planning and building should never be left for later as the system production time has the capability to draw on all the resources towards it. Delaying DR planning might end up with it failing to materialise.

Table 5.40: Employees on the internet should be protected from online threats

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	75.%	25%				100%
No. of Respondents	18	6				24

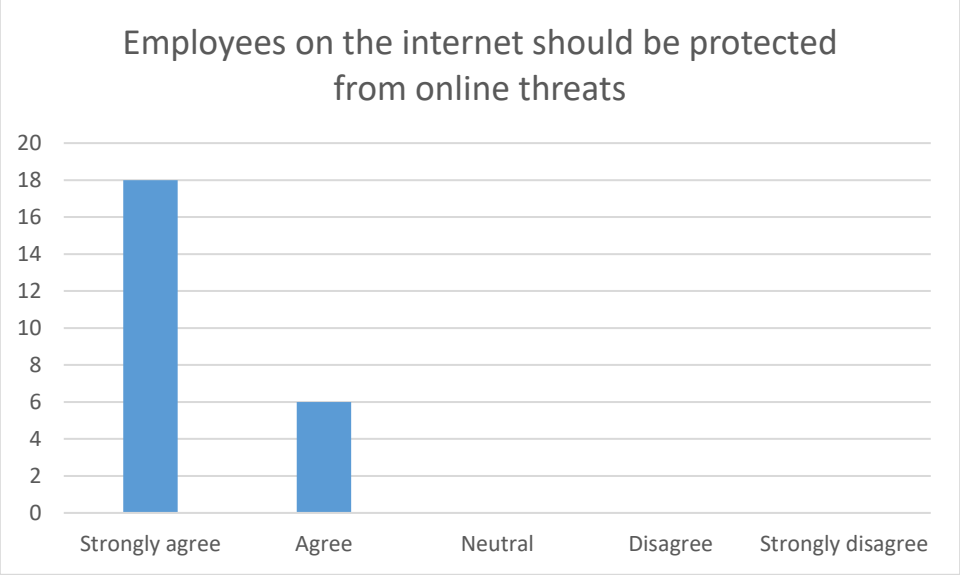


Figure 5.40: Employees on the internet should be protected from online threats

The next statement analysed related to the management of risks exposure online. This is to understand if respondents were protected online.

The responses to the statement that employees on the internet should be protected from online threats are shown in Figure 5.40 and Table 5.40. The results show that most respondents strongly agree (75%) that employees on the internet should be protected from online threats. The second most group of respondents agree (25%) with the statement.

The results lean towards the suggestion that there is a need for employees on the internet be protected from online threats, as this is supported by all respondents. Companies tend to put in more money on sophisticated software to protect their employees online. It would be unwise to choose less expensive but weaker software to protect employees while they are online.

Table 5.41: There should be an overall organisational strategy on Risk Management for Port MIS

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
% Respondents	46%	54%				100%
No. of Respondents	11	13				24

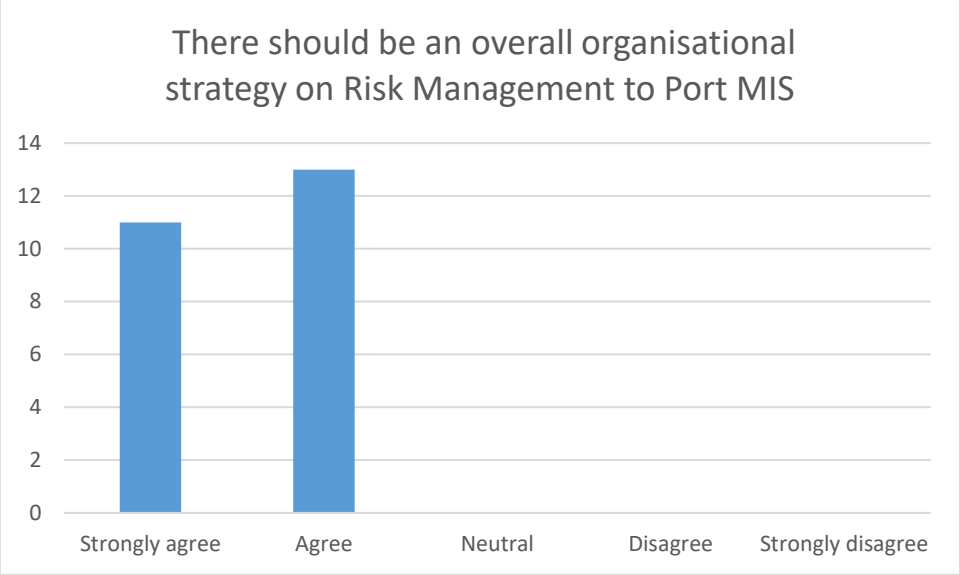


Figure 5.41:There should be an overall organisational strategy on Risk Management to Port MIS

The results of the statement that there should be an overall organisational strategy on Risk Management for Port MIS are shown in Figure 5.41 and Table 5.41. The most number of respondents (54%) agree that there should be an overall organisational strategy on Risk Management for Port MIS. The second most respondents agree strongly (46%).

Hundred percent (100%) of respondents agree and strongly agree. This shows a strong conviction that respondents agree with the statement. This emphasises the importance of having an overall organisational strategy on Risk Management for Port MIS.

The review on risk management of Port MIS showed that respondents agreed with strong conviction that policies on the use of the systems, protection on the internet and disaster recovery plans were all vitally needed. The real focus has been on the overall organisation strategy that encompasses all the ports. The respondents agreed, however, though not with strong conviction, that they do have an understanding of Risk Management on Port MIS. It can be concluded that the respondents feel that there is a need for an overall Risk Management on Port MIS strategy.

The strategy should encompass most of the statements where the respondents are not strong on agreeing with the statements pertaining to the research objectives. Research objectives related to Risk Management of Port MIS. Thus, it had to have

respondents strongly agreeing with statements relating to them to show a level of understanding on how to manage risks.

5.3 SUMMARY

Chapter 5 discussed the findings based on the feedback from respondents. The respondents were from management and encompassed senior and mid-management personnel who are assumed to be working on the Port MIS system. These results confirmed the need for the Port MIS to be protected from risk.

CHAPTER 6

CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

Chapter 6 presents the recommendations on the data analysed in Chapter 5.The data was based on the survey conducted. This chapter summarises the quantitative study for each of the research questions (Refer Section 6.2) and draws up managerial recommendations based on the qualitative study. Limitations of the study and future implications are outlined. The conclusion looks at the major recommendations that emerged from this study.

6.2 Recommendations Based on the Research Questions.

The primary objective of this study was to explore the effect of managing risk within Port Management Information Systems.

Each research question is presented and recommendations made based on the findings of this study.

The Research Questions are listed below:

RQ 1: What are the risks that apply to information systems such as the Port MIS?

RQ2: What are prevalent risk assessment methods?

RQ 3: What are the effects of risk on Port MIS and subsystems?

RQ 4: What is the importance of risk assessment?

RQ5: What is the importance of risk management?

RQ 6: Do all eight ports in South Africa attach the same level of importance to risk assessment for their Port MIS?

RQ 7: How can a risk management strategy be standardised for all eight ports?

RQ 1:What are the risks that apply to information systems such as the Port MIS?

Port MIS is at risk of theft by employees.

The recommendation is that the system gets protection from theft by putting more security around the computer equipment. This would also prevent theft by outsiders, as the respondents were not strong on conviction that the system was safe from outside threats. The outsider threats included intruders. Internal protection is also

needed in the form of who gets to use computer equipment. Policy must be followed on who signs the agreements for this.

Port MIS is at risk of attacks on its telecommunication systems eg. terror, cyber and on telephone lines.
The recommendation is that protection is needed against physical threat and damage to telephone lines. Sophisticated software is needed to defend against cyber-attacks. A disaster recovery plan on how to recover from any form of attack should be in place.

RQ2: What are prevalent risk assessment methods?

Port MIS is at risk if it does not update its prevalent risk assessment methods.
The recommendation is that the system needs software to be protected from insider and outsider threats. The respondents felt that it would be beneficial to have such software. Risk assessment methods such as OCTAVE are recommended. An OCTAVE is a self-directed method that helps in risk management. Another method that helps in real time is the NRTSAP, which calculates the probability of attacks. The respondents showed a level of understanding of who hackers are, and the prevalent system seems to be protected against them. The system has software updates done automatically, which will help to withstand new challenges.

Port MIS is at risk if users do not abide by their job description.
The officially connected users of the system are genuine, but they seem to have access to areas beyond their job description.
The recommendation is that management needs to put guidelines in place as to who gets to access what in relation to their work and job description.

RQ 3: What are the effects of risk on Port MIS and sub-systems?

Port MIS is at risk of losing data through system shutdown.
The respondents showed understanding that any system shutdown does affect their department and the business as a whole. Data loss is known to have a huge impact on the business. Information risks such as data loss can cause financial risks that lead to loss of income. The respondents agreed, but not all were strongly convicted on this point.
The recommendation is that management must emphasise the importance of information system risks more.

RQ 4: What is the importance of risk assessment?

Port MIS is at risk if users are not fully aware of the need for risk assessment.

The respondents are aware of threats of being on the internet, and of the need for assessments. The respondents feel that they have adequate awareness of the risks when using information systems. The respondents showed a need for more awareness as they were not convinced that this was of any real urgency. This was despite the fact that risk assessments were done regularly.

The recommendation is that management needs to conduct more risk awareness campaigns. There has to be a review of risk assessments relating to IS systems. The respondents agreed that risk awareness campaigns help to minimise risks and should be conducted. The procedure will have to be on set standards and norms set by international regulatory bodies.

Port MIS is at risk if disaster recovery plans are not in place.

The analysis on recovery of the system from disasters that are natural, man-made, technical and others show that the system can recover. However, there were discrepancies when it came to understanding that such disasters do impact on the business, no matter what form they take.

The recommendation is that disaster recovery (DR) has to be a centralised process for all DR plans. The disaster recovery planning has to cater for all kind of disasters. This has to be an important part of risk management.

RQ 4: What is the importance of risk assessment?

Port MIS is at risk if third parties they outsource do not handle risk as expected.

The survey revealed that outsourced third parties did not handle risks in the same way as the company contract stated.

The recommendation is that management has to collaborate more with organisations that meet or exceeds their expected standards when addressing risk. The outsourced company should handle threats in the same way as their organisation.

RQ5: What is the importance of risk management?

Port MIS is at risk if more is not done about threats from criminal elements.

The organisation's information system is protected from criminal elements through controlled access, as confirmed by the respondents. Despite this, employees still feel vulnerable.

The recommendation is that a review is necessary on efficiency of the controlled access despite the security measures already in place.

RQ 6: Do all eight ports in South Africa attach the same level of importance to risk assessment for their Port MIS?

Port MIS is at risk if all ports do not have the same standards of risk assessment.

The respondents agreed that regular risk assessments are conducted, but they differed at each level and port. Risk assessment standards within their respective departments differed. The same standards were not maintained across the eight ports.

The recommendation is that there should be guidelines or standards that need to be in place and performed consistently at all ports and in all relevant departments.

RQ 7: How can a risk management strategy be standardised for all eight ports?

Port MIS is at risk if no standardised strategy is applied at all eight ports.

The respondents agreed that it is ideal to have policy guidelines for all Transnet employees on the use of information systems. This will regulate the use of information systems and counter threats that would put Port MIS at risk.

Respondents felt that having DR plans should be urgent. DR sites, planning and building should not be left for later, as the system production time has the capability to draw all the resources towards it. Besides, the DR planning might fail to materialise.

The respondents felt that they should get protection from internet risk as part of risk management strategy. The majority had strong convictions on this need. However, they agreed on, but did not feel that it was urgent to have an overall standardised strategy for Port MIS.

The recommendation is that management must clarify Risk Management so that all have a better understanding of it. Risk management should be an organised method of handling insecurity through risk assessment, as well as devising plans to manage and mitigate risk using managerial resources. Strategies should include giving the risk

to a third party. All port employees should be made aware that risk includes security threats, threats to property value and threats that influence probability. They should note also the exposure of property to threats, threat influence on organisations and on prevailing security.

It is recommended that all these factors should be part of a document that is given to employees to make them aware of Risk Management. They need to take responsibility for all Risk Management as well.

6.3 Limitations of the Study

The study has had its own limitations that need to be mentioned in order for the reader to understand the impediments on the journey towards completion.
The following are the limitations of the study.

- Literature on previous studies relating to Port MIS and its sub-systems is limited. Most are written in Asian languages.
- The library resources at Nelson Mandela University and the search engines do not extensively cover studies relating to Port Management Information Systems.
- There is no set standard questionnaire relating to RISK Management of Port MIS.
- The questionnaire distribution was administered by Transnet, thus the sample selection population could not be controlled.
- The approval for the questionnaire distribution took very long. Thus the first draft of the questionnaire had to be accepted without being tested.
- The response turnaround time took long for questionnaires.

However, despite the above limitations, the study was conducted. The questionnaire responses were accepted based on the respondents' job title or department in which they worked. The questionnaire covered most of what the literature review covered. The responses received showed a fair level of understanding relating to the subject of the study.

6.4 Future Implications

Transnet will need to measure how effective their Risk Management is in relation to Port MIS and related sub-systems. The recommendations made should be heeded.

There will also be a need to assess how the awareness of risk is conducted, based on the study results. The other aspect that needs assessment is the understanding of the need for an Overall Risk Management Strategy. This will have to be aligned with international standards, procedures and policies.

6.5 Research Gaps

The identified gaps in the literature review included the fact that the sub-systems making up the Port MIS are not standardised. Sub-systems that make up the Port MIS are different and they are not integrated for universal use. The Port MIS system is popular, but has only one vendor, KLNET. The system has not been tested for risks, thus the study exposed some of its major characteristics. The sub-systems have also not been assessed for risks relating to them.

6.6 Conclusion

Port MIS would be an effective administrative and management tool for port managers. It is recommended that this study be a starting point for management changes at South African ports, and that risk should in future be addressed with the urgency that it warrants.

BIBLIOGRAPHY

Abbes, S. (2015). Seaport Competitiveness : A comparative empirical analysis between North and West African countries using principal component analysis. *International Journal of Transport Economics*, (January).

Agubor, C. K., & Chukwudebe, G. A. (2015). Security Challenges to Telecommunication Networks : An Overview of Threats and Preventive Strategies, 124–129.

Al-mamary, Y. H., Shamsuddin, A., & Aziati, N. (2014). The Role of Different Types of Information Systems In Business Organizations : A Review. *International Journal of Research(IJS)*, *1*(7), 1279–1286.

Al Mazari, A., Anjariny, A. H., Habib, S. A., & Nyakwende, E. (2016). Cyber Terrorism Taxonomies. *International Journal of Cyber Warfare and Terrorism*, *6*(1), 1–12. https://doi.org/10.4018/IJCWT.2016010101

Alberts, C., & Stevens, J. (2003). Introduction to the OCTAVE ® Approach, (August).

Alfayyadh, S. A. J. (2017). *Development of the framework for a lean , energy efficient , and environmentally friendly port : Umm Qasr Port as a Case Study*. World Maritime University.

Aron, R., Clemons, E. K., & Reddi, S. (2005). Just Right Outsourcing : Understanding and Managing Risk Introduction : Objectives of this paper. *International Conference on System Sciences*, *22*(2), 1–10. https://doi.org/10.1109/HICSS.2005.368

ASH Centre for Democratic Governance and Innovation. (2011). *The Sum is Greater than the Parts : Doubling Shared Prosperity in Indonesia Through Local and Global Integration*.

Baird, A. J. (2002). Privatization trends at the world's top-100 container ports. *Maritime Policy and Management*, *29*(3), 271–284. https://doi.org/10.1080/03088830210132579

Bernard. (2000). Handbook of Methods in Cultural Anthropology. *Sociological Research Online*, *5*(1), 183–186. https://doi.org/10.1525/aa.2000.102.1.183

Bertino, E. (2012). *Data Protection from Insider Threats*. (M. T. Özsu, Ed.). Morgan & Claypool Publishers. https://doi.org/10.2200/S00431ED1V01Y201207DTM028

Borrego, M., & Tech, V. (2009). Quantitative , Qualitative , and Mixed Research Methods in Engineering Education. *Journal of Engineering Education*, (August 2016). https://doi.org/10.1002/j.2168-9830.2009.tb01005.x

Cabezas, P. R., & Kasoulides, G. (2004). International Maritime Organization. *The*

International Journal of Marine and Coastal Law, *3*(3), 235–245. https://doi.org/10.1163/187529988X00184

Case, J. M., & Light, G. (2011). Emerging Methodologies in Engineering Education Research. *Journal of Engineering Education*, *100*(1), 186–210. Retrieved from http://www.jee.org

Cepolina, S., & Ghiara, H. (2013). New trends in port strategies. Emerging role for ICT infrastructures. *Research in Transportation Business and Management*, *8*, 195–205. https://doi.org/10.1016/j.rtbm.2013.07.001

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defences. *International Journal of Security and Its Applications*, *10*(1), 247–256. https://doi.org/10.14257/ijsia.2016.10.1.23

Chong, J., Techatassanasoontorn, A., & Doolin, B. (2013). Exploring qualitative comparative analysis in IS Research. In *The Pacific Asia Conference on Information Systems (PACIS)*. Retrieved from http://aut.researchgateway.ac.nz/handle/10292/5560

Chou, D. C., & Chou, A. Y. (2009). Computer Standards & Interfaces Information systems outsourcing life cycle and risks analysis. *Computer Standards & Interfaces*, *31*(5), 1036–1043. https://doi.org/10.1016/j.csi.2008.09.032

Čišić, D., & Tijan, E. (2011). Information management in seaport clusters, *2*, 371–386.

Cullinane, K., Song, D.-W., & Wang, T. F. (2003). Private Sector Participation in Asian Ports. *Turkish Chamber of Shipping in Instanbul*, *615*(5), 177–194.

Dellios, K., & Polemi, D. (2012). Maritime clouds for the European ports. In *Proceedings of the 2012 16th Panhellenic Conference on Informatics, PCI 2012* (pp. 422–426). https://doi.org/10.1109/PCi.2012.39

Department of Transport. (2009). *Arrival of Ships to a Port - Port Regulations Guide to Ports Entry*.

Ekelhart, A., Fenz, S., & Neubauer, T. (2009). AURUM : A Framework for Information Security Risk Management, (September 2008), 1–10.

Fernández, P., Santana, J. M., Ortega, S., Trujillo, A., Suárez, J. P., Domínguez, C., … Sánchez, A. (2016). Smartport: A platform for sensor data monitoring in a seaport based on FIWARE. *Sensors (Switzerland)*, *16*(3), 1–24. https://doi.org/10.3390/s16030417

Gidado, U. (2015). Consequences of Port Congestion on Logistics and Supply Chain in African Ports. *Developing Country Studies*, *5*(6), 160–168. Retrieved from

http://iiste.org/Journals/index.php/DCS/article/download/20933/21177

Gleim, S. W. (2009). *CANADA'S GRAIN HANDLING AND TRANSPORTATION SYSTEM: A GIS-BASED EVALUATION OF POLICY CHANGES*. University of Saskatchewan Saskatoon.

Goldberg, H. G., Young, W. T., Reardon, M. G., Phillips, B. J., & Senator, T. E. (2017). Insider Threat Detection in PRODIGAL. *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2648–2657. https://doi.org/http://hdl.handle.net/10125/41476

Gonzalez, R., Gasco, J., & Llopis, J. (2006). Information systems outsourcing : A literature analysis, *43*, 821–834. https://doi.org/10.1016/j.im.2006.07.002

Goodhope, O., & Polytechnic, R. S. (2014). The Role of Effective Ports Management in Facilitating International Trade in Nigeria, *6*(13), 204–215.

Govender, N., & Mbhele, T. P. (2014). Dynamics of intermodal logistical systems on containerisation and road transportation in Durban, South Africa. *Journal of Transport and Supply Chain Management*, *8*(1), 1–10. https://doi.org/10.4102/jtscm.v8i1.150

Hagan, T. L. (2014). Measurements in quantitative research: How to select and report on research instruments. *Oncology Nursing Forum*, *41*(4), 431–433. https://doi.org/10.1188/14.ONF.431-433

Han, C.-R., & McGauran, R. (2014). Tracing trails: implications of tax information exchange programs for customs administrations. *World Customs Journal*, *8*(2), 3–14. https://doi.org/10.1093/annonc/mdm364

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, *100*(4), 817–885. https://doi.org/10.15779/Z38CR6N

Herdzik, J. (2012). Possibilities of improving safety and reliability of ship propulsion system during DP operations, *19*(2).

Höst, M., & Lindholm, C. (2007). Different Conceptions in Software Project Risk Assessment, 1422–1426.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies : The Critical Role of Top Management and Organizational Culture, *43*(4), 615–659.

Ibrahimi, K. (2009). Performance Indicators and Port Authority Management. *5th International Conference of ASECU "Market Functionality and Institutional Reforms,"* (May). https://doi.org/10.13140/RG.2.1.2806.9840

Ignify. (2016). Software Solutions for Sea Ports, Ocean Shippers & Marine Terminals. Retrieved from http://www.ignify.com/port_billing_vessel_movement_management_software_solutions.asp

Irvine, A., Drew, P., & Sainsbury, R. (2013). *' Am I not answering your questions properly ?' Clarification , adequacy and responsiveness in semi-structured telephone and face-to-face interviews*. Retrieved from http://qrj.sagepub.com/content/13/1/87.refs

Jackson, L. A. (2008). Economic Acceptable Risk Assessment Model, 36–39.

Karabacak, B., & Sogukpinar, I. (2005). ISRAM : Information security risk analysis method ISRAM : information security risk analysis method, (May 2016). https://doi.org/10.1016/j.cose.2004.07.004

Karahalios, H. (2014). The contribution of risk management in ship management : The case of ship collision. *Safety Science*, *63*, 104–114. https://doi.org/10.1016/j.ssci.2013.11.004

Keceli, Y., Choi, H., Cha, Y., Aydogdu, Y. V., & Kim, H. (2008). PORT-MIS. *Entruy Journal of Information Technology*, *7*(2), 165–175.

Kim, S. Y. (2013). Korea Logistics Information systems applied Neal-Net Cooperation Mechanism.

Kimberlin, C. L., & Winterstein, A. G. (2008). Validity and reliability of measurement instruments used in research. *American Journal of Health-System Pharmacy*, *65*(23), 2276–2284. https://doi.org/10.2146/ajhp070364

Kitagaki, I., & Hikita, A. (2007). Development of an algorithm for groupware modeling for collaborative learning. *International Journal of Computers, Communications & Control*, *1*. Retrieved from http://www.journal.univagora.ro/download/pdf/72.pdf

Kleinport. (2016). KleinPort PMIS Maximizing operational efficiency. Burnaby: SAAB. Retrieved from www.kleinsystems.com

Klopott, M. (2013). Restructuring of environmental management in Baltic ports: case of Poland. *Maritime Policy & Management*, *40*(5), 439–450. https://doi.org/10.1080/03088839.2013.798440

KOSDAQ (Korea Securities Dealers Automated Quotation). (2015). Terminal & Port Solution. *Korea Logistic Network CORP*.

Kumar, R., & Singh, H. (2015). A Proactive Procedure to Mitigate the BYOD Risks on the Security of an Information System. *ACM SIGSOFT Software Engineering*

Notes, *40*(1). https://doi.org/10.1145/2693208.2693231

Landry, B. J. L., & Koger, M. S. (2006). Dispelling 10 common disaster recovery myths. *Journal on Educational Resources in Computing*, *6*(4), 6–es. https://doi.org/10.1145/1248453.1248459

Laudon, K. C., & Laudon, J. P. (2010). *Management In formation Systems : Managing the digital firm* (11th ed.). London: Pearson.

Lisle, J. De. (2011). The Benefits and Challenges of Mixing Methods and Methodologies: Lessons Learnt From Implementing Qualitatively Led Mixed Methods Research Designs in Trinidad and Tobago The Emergence of Mixed Methods Research. *Caribean Curriculum*, *18*, 87–120.

Lo, C., & Chen, W. (2012). Expert Systems with Applications A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems With Applications*, *39*(1), 247–257. https://doi.org/10.1016/j.eswa.2011.07.015

Majchrzak, A., & Markus, M. . (n.d.). Technology affordances and constraints. *Encyclopedia of Management Theory*.

Marsh. (2014). Risk Challenges and Solutions Ports and Terminals.

Mitra, C. C., & Borza, A. (2015). Research methodology – a quality assurance instrument . Analysis of internationalized masters of Babeș-Bolyai University. *Review of Economic Studies and Research Virgil Madgearu*, *1*, 37–50.

Montefiore, A. (2012). Ethics and Educational Policy. *Review of Education, Pedagogy, and Cultural Studies*, *6*, 167–185. https://doi.org/10.1080/0098559800060206

Moore, A. P., Cappelli, D. M., Caron, T. C., Shaw, E., Spooner, D., & Trzeciak, R. F. (2011). A preliminary model of insider theft of intellectual property. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *2*(1), 28–49. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84855181760&partnerID=tZOtx3y1

Muijs, D. (2005). *Doing quantitative research in education with SPSS*. *Measurement* (Vol. 27). https://doi.org/10.7748/ns2013.06.27.43.59.s52

Nehari Talet, A., Mat-Zin, R., & Houari, M. (2014). Risk Management and Information Technology Projects. *International Journal of Digital Information and Wireless Communications*, *4*(1), 1–9. https://doi.org/10.17781/P001078

Notteboom, T. E., & Rodrigue, J.-P. (2005). Port regionalization: towards a new

phase in port development. *Maritime Policy & Management*, *32*(3), 297–313. https://doi.org/10.1080/03088830500139885

Ntouskas, T., & Polemi, N. (2010). S-PORT : " A secure , collaborative environment for the security management of Port Information Systems ." https://doi.org/10.1109/ICIW.2010.62

O'Reilly, M., & Parker, N. (2012). "Unsatisfactory Saturation": a critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, *13*, 190–197. https://doi.org/10.1177/1468794112446106

Ojadi, F., & Walters, J. (2015). Critical factors that impact on the efficiency of the Lagos seaports. *Journal of Transport and Supply Chain Management*, *9*(1), 1–13. https://doi.org/10.4102/jtscm.v9i1.180

Oregon State University. (1981). *Ocean Transportation Serving Pacific Northwest Agriculture*.

Osei-Bryson, K. M., & Ngwenyama, O. K. (2006). Managing risks in information systems outsourcing: An approach to analyzing outsourcing risks and structuring incentive contracts. *European Journal of Operational Research*, *174*(1), 245–264. https://doi.org/10.1016/j.ejor.2005.01.060

Oxford University. (2016a). Management. Retrieved May 5, 2015, from http://www.oxforddictionaries.com/definition/english/management

Oxford University. (2016b). Title Risk. Retrieved May 5, 2015, from http://www.oxforddictionaries.com/definition/english/risk?q=risk

Oz, E. (2009). *Management Information Systems*. (K. Hennessy, D. Kaufmann, & A. Poirier, Eds.) (6th ed.). Cengage course Technology.

Pak, C. (2008). The Near Real Time Statistical Asset Priority Driven (NRTSAPD) Risk Assessment Methodology, (443), 105–112.

Park, N. K., Choi, H. R., Lee, C. S., Kang, M. H., Yang, J. W., Management, D., … E-mail, K. (2005). Port Management Information Systems towards privatazation, 1–13.

Pudhota, L. (2012). Collaborative Workflow Modelling Based on Activity Diagrams , Coloured Petri-nets and System Dynamics Table of Contents, (January).

Rajnoha, R., Kádárová, J., Sujová, A., & Kádár, G. (2014). Business Information Systems: Research Study and Methodological Proposals for ERP Implementation Process Improvement. *Procedia - Social and Behavioral Sciences*, *109*, 165–170. https://doi.org/10.1016/j.sbspro.2013.12.438

Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor

networks: Attacks and defenses. *IEEE Pervasive Computing*, *7*(1), 74–81. https://doi.org/10.1109/MPRV.2008.6

Ritchie, J., & Lewis, J. (2014). *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. *Qualitative Research*. London: Sage publications. https://doi.org/10.4135/9781452230108

Rødseth, Ø. J., Marinteknisk, N., & As, F. (2013). Secure Communication for E-Navigation and Remote Control of Unmanned Ships.

Rolland, E., Ulmer, J. R., & Patterson, R. A. (2014). Risk Mitigation Decisions for IT Security, *5*(1).

Romers, I. I. . (2013). *Port Call Optimization in three oil shipping markets*. Erasmus Universiteit Rotterdam.

Rowbotham, J. M. (2014). *Introduction To Marine Cargo Management*. (P. J. McArthur, Ed.) (second edi). New York: Informa Law from Routledge.

Samson, G. L. (2015). Securing an Information Systems from Threats : A Critical Review, *4*(6), 425–434.

Scupola, A. (2012). ICT Adoption in Facilities Management Supply Chain: The Case of Denmark. *Journal of Global Information Technology Management*, *15*(1), 53–78. https://doi.org/10.1080/1097198X.2012.10845612

Seidtnan, I. (2006). *Interviewing as Q.ualitative Research* (3rd ed.). New York and London: Teacher College Press.

Senator, T. E., Henry, G., Bader, D. A., Chow, E., Dietterich, T. G., Memory, A., … Koutra, D. (2013). Detecting Insider Threats in a Real Corporate Database of Computer Usage Activity. *KDD'13*.

Serpella, A. F., Ferrada, X., Howard, R., & Rubio, L. (2014). Risk Management in Construction Projects: A Knowledge-based Approach. *Procedia - Social and Behavioral Sciences*, *119*, 653–662. https://doi.org/10.1016/j.sbspro.2014.03.073

Shang, K.-C., Chao, C.-C., & Lirn, T.-C. (2016). The application of personality traits model on the freight forwarding service industry. *Maritime Business Review*, *1*(3), 231–252. https://doi.org/10.1108/MABR-09-2016-0021

Sherer, S. A. (2004). Managing Risk beyond the Control of IS Managers : The Role of Business Management, *00*(C), 1–10.

Spremiü, M. (2012). Corporate IT Risk Management Model : a Holistic view at Managing Information System Security Risks, 299–304. https://doi.org/10.2498/iti.2012.0461

Strandenes, S. P., & Marlow, P. B. (2000). PORT PRICING AND COMPETITIVENESS IN SHORT SEA SHIPPING. *International Journal of Transport Economics*, *27*(3), 315–334. Retrieved from http://www.jstor.org/stable/42747574

Tohidi, H. (2011). The role of risk management in IT systems of organizations. In *Procedia Computer Science* (Vol. 3, pp. 881–887). Elsevier. https://doi.org/10.1016/j.procs.2010.12.144

UNCTAD. (2014). *Review of maritime transport 2013*. *United Nations Conference on Trade and Development*. https://doi.org/10.18356/d6798fb6-en

Veith, H. M. (2015). *Teaching resources , autonomy , and novel skills for independence and transitions (T . R . A . N . S . I . T .) life skills program : a program development plan*. Retrieved from http://utdr.utoledo.edu/graduate-projects

Venkatesh, V., & Brown, S. A. (2013). Research article bridging the qualitative-quantitative divide : Guidelines for conducting mix methos. *MIS Quarterly*, *37*(1), 21–54.

Vukić, L., Peronja, I., & Slišković, M. (2018). Port pricing in the north port of split: A comparative analysis. *Transactions on Maritime Science*, *7*(1), 59–70. https://doi.org/10.7225/toms.v07.n01.006

Vuong, J. (2015). Disaster recovery planning, (October), 1–3. https://doi.org/10.1109/MP.2004.1301248

Wegner, T. (2007). *Applied Business Statistics : Methods and Excel based applications* (2nd Editio). Juta.

Wiesche, M., Keskinov, H., Scherman, M., & Kremar, H. (2013). Classifying Information Systems Risks : What Have We Learned So Far ? Chair for Information Systems. *46th Hawaii International Conference on System Sciences*, 5013–5022. https://doi.org/10.1109/HICSS.2013.130

Wu, H., Chen, X., Hu, Q., Shi, C., & Mo, J. (2012). Novel Design of Inland Shipping Management Information System Based on WSN and Internet-of-things, *6*(3), 307–313.

Xu, D., Li, C., & Leung, J. Y. (2012). Berth allocation with time-dependent physical limitations on vessels. *European Journal of Operational Research*, *216*(1), 47–56. https://doi.org/10.1016/j.ejor.2011.07.012

Yilmaz, K. (2013). Comparison of Quantitative and Qualitative Research Traditions : epistemological , theoretical ,. *European Journal of Education*, *48*(2).

Zeadally, S., Yu, B., Jeong, D. H., & Liang, L. (2012). Detecting insider threats solutions and trends. *Information Security Journal*, *21*(4), 183–192. https://doi.org/10.1080/19393555.2011.654318

Zhang, Z., & Xu, X. (2017). Principal agent model based design and outsourcing of information value. *Cluster Computing*, *20*(1), 67–79. https://doi.org/10.1007/s10586-016-0724-0

Zohrabi, M. (2013). Mixed Method Research: Instruments, Validity, Reliability and Reporting Findings. *Theory and Practice in Language Studies*, *3*(2), 254–262. https://doi.org/10.4304/tpls.3.2.254-262

Appendix A
Ethics clearance

FORM E

NELSON MANDELA UNIVERSITY

ETHICS CLEARANCE FOR TREATISES/DISSERTATIONS/THESES

Please type or complete in black ink

FACULTY: Economic Sciences

SCHOOUDEPARTMENT: Business School

I, (surname and initials of supervisor)
FRASER, J. F. E

the supervisor for (surname and initials of candidate)Jafta N

(student number) 205045928

a candidate for the degree of Masters Business Administration

with a treatise/dissertation/thesis entitled (full title of treatise/dissertation/thesis):

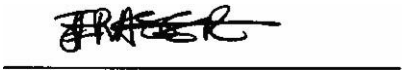
Risk Management of Port Management Information Systems considered the following ethics criteria (please tick the appropriate block):

	YES	NO
1. Is there any risk of harm, embarrassment of offence, however slight or temporary, to the participant, third parties or to the communities at lar e?		X

2. Is the study based on a research population defined as 'vulnerable' in terms of age, physical characteristics and/or disease status?		X
2.1 Are subjects/participants/respondents of your study: (a) Children under the age of 18?		X
(b) NMMU staff?		X
(c) NMMU students?		X
(d) The elderly/persons over the age of 60?		X
(e) A sample from an institution (e.g. hospital/school)?		X
		X
Handica ed e. . mentall or h icall ?		X
3. Does the data that will be collected require consent of an institutional authority for this study? (An institutional authority refers to an organisation that is established by government to protect vulnerable eo le		X
3.1 Are you intending to access participant data from an existing, stored re ositor e. . school, institutional or universi records ?		X
4. Will the participant's privacy, anonymity or confidentiality be com romised?		X
4.1 Are you administering a questionnaire/survey that: (a) Collects sensitive/identifiable data from participants?		X
(b) Does not guarantee the anonymity of the participant?		X
(c) Does not guarantee the confidentiality of the participant and the data?		X
(d) Will offer an incentive to respondents to participate, i.e. a lucky draw or any other prize?		X
(e) Will create doubt whether sample control measures are in place?		X
(f) Will be distributed electronically via email (and requesting an email response)?		X
Note: • If your questionnaire DOES NOT request respondents' identification, is distributed electronically and you request respondents to return it manually (print out and deliver/mail); AND respondent anonymity can be guaranteed, your answer will be NO. • If your questionnaire DOES NOT request respondents' identification, is distributed via an email link and works through a web response system (e.g. the university survey system); AND respondent anonymity can be guaranteed, your answer will be NO.		X

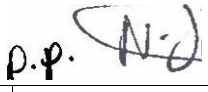
Please note that if ANY of the questions above have been answered in the affirmative (YES) the student will need to complete the full ethics clearance form (REC-H application) and submit it with the relevant documentation to the Faculty RECH (Ethics) representative.

and hereby certify that the student has given his/her research ethical consideration and full ethics approval is not required.



26/4/201

SUPERVISOR(S) DATE



HE OF DEPARTMENT **DATE**

26/04/2018

STUDENT(S) DATE

Student(s) contact details (e.g. telephone number and email address):
0815615997 and s205045928@mandela.ac.za

Please ensure that the research methodology section from the proposal is attached to this form.

Appendix B

Questionnaire

Risk Management of Port MIS

* Required

1. **To what extent do you agree with the following statement pertaining to Risk Management of Port Management Information Systems? ***

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
There should be an overall organisational strategy on Risk Management to Port MIS.					
Data loss affects my department and the organisation as whole					
Third parties handle risks to information systems the same level as our organisation					
Employees on the internet should be protected from online threats					
There are risk assessment standards on my department					
The company has regular risk assessments being conducted					
Testing recovery plan should be done routinely					
Information on systems are at risk of theft by outsiders					
Risk assessment methods are beneficial					
The organisation has the same risk assessment standards across all ports					
Risk awareness campaign help minimise risks should be conducted					
The system has protection against hackers					
There are easily accessible procedures on how to use the company's information system					
Managing risks will help not to lose future or current business					
The system can easily be destroyed by intruders					
I am personally aware of threats that exist by being connected to the Internet					
Risk assessment is continuously conducted on my department					
Connected to the system are only authorised users					
The organisations' information system is protected to criminal elements by controlled access					

to them					
Employees of the organisation can damage the company's information system internally by themselves.					
Risk assessment methods help minimise risks					
The systems is only used by authorised personnel					
Employees have adequate risk awareness of the use of information systems					
External Customers' business with the organisation can be affected by the shutdown of the system					
There is a need for software that can automatically detect threats to the information system					
It is ideal to have policy guidelines for Tansnet employees for the use of information systems.					
There is a real time protection on the systems against threat					
Disaster recovery plans from disasters is a "must-have" for Transnet operations					
Software updates are done automatically to reduce the risks of threats					
Information on systems are at risk of theft by employees					
The computer equipment can be manually stolen from its physical location.					
Users are only limited to work on systems that affect their work					
Procedures help minimise risks					

2. **Please indicate which of the following system(s) you work on ?** * *Check all that apply.*

- [ ] Facilities Management
- [ ] Billing Management
- [ ] Report/Statistics
- [ ] Vessel Management
- [ ] Cargo Management System
- [ ] Other: _____

3. **Please indicate the level of management within the organization** *Mark only one oval.*

- ◯ Non-supervisory staff
- ◯ Junior Management
- ◯ Middle management
- ◯ Senior Management
- ◯ Other: _____

4. **Please indicate the port you are based at** *Mark only one oval.*

- ◯ Ngqura
- ◯ Port Elizabeth
- ◯ Richards Bay
- ◯ Saldanha Bay
- ◯ Durban
- ◯ Cape Town
- ◯ Mossel Bay
- ◯ East London
- ◯ Other: _____

To what extent do you agree with the following statement pertaining to Risk Management of Port Management Information Systems?

5. **Information system risks cause**
   ***** *Mark only one oval per row.*

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
financial risks e.g. such as loss of income etc.	◯	◯	◯	◯	◯
poor system performance	◯	◯	◯	◯	◯

6. **The system can easily recover from disaster such as: *** *Mark only one oval per row.*

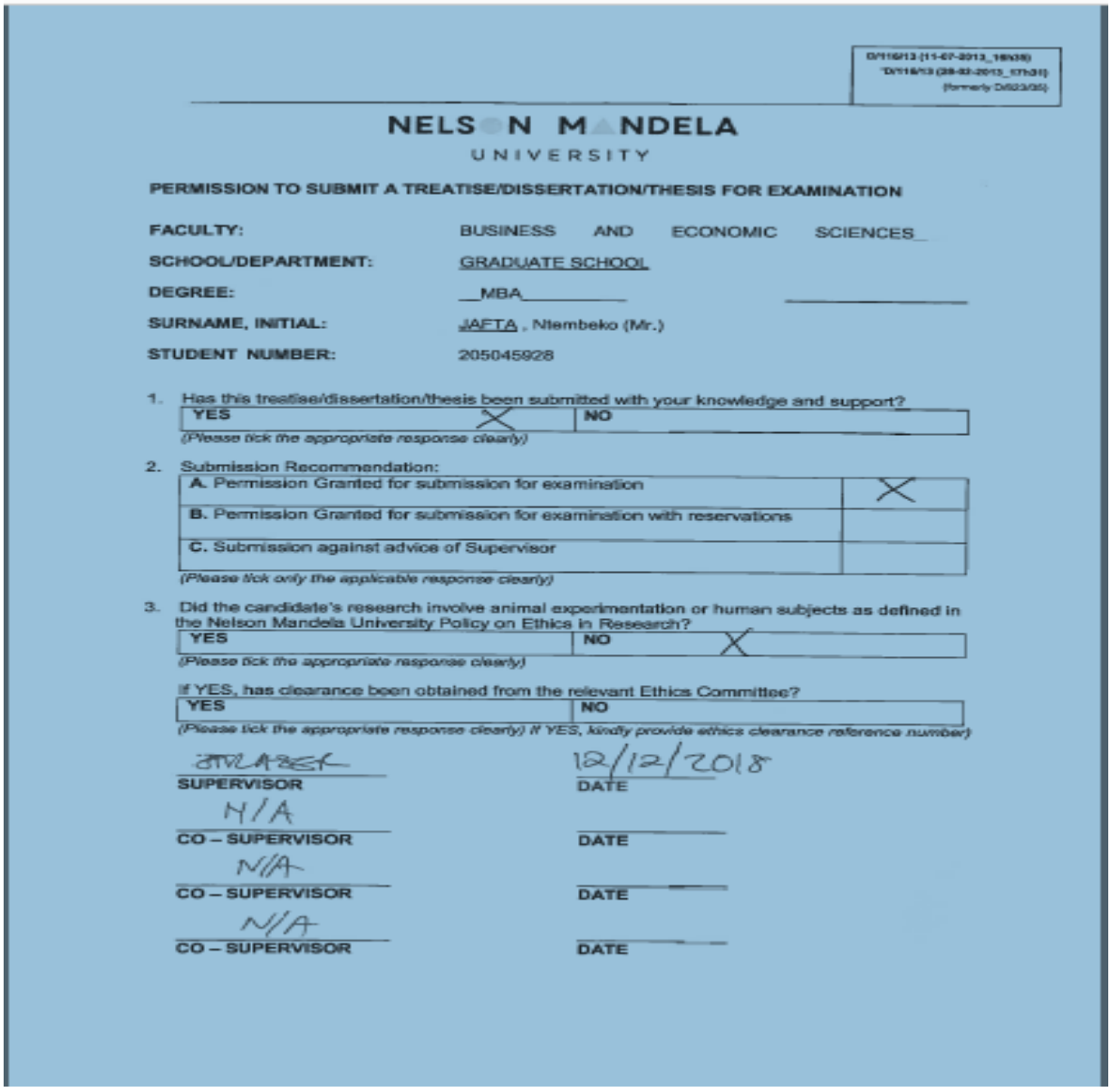
	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
Man-made disasters such as fires	◯	◯	◯	◯	◯
Man-made disasters such as vandalism	◯	◯	◯	◯	◯
Technical disasters e.g. internet downtime	◯	◯	◯	◯	◯
Natural disasters e.g. floods, storms	◯	◯	◯	◯	◯

7. **The telecommunication and IT system are at risk of the following attacks: *** *Mark only one oval per row.*

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
Terror attacks e.g. such as inter-country warfare	◯	◯	◯	◯	◯
Technological threats e.g. cyber attacks	◯	◯	◯	◯	◯
Criminal attacks such as phone lines being damaged	◯	◯	◯	◯	◯
Criminal attacks such as cables being stolen	◯	◯	◯	◯	◯

Appendix C

Permission to Submit



NELSON MANDELA
UNIVERSITY

PERMISSION TO SUBMIT A TREATISE/DISSERTATION/THESIS FOR EXAMINATION

FACULTY: BUSINESS AND ECONOMIC SCIENCES

SCHOOL/DEPARTMENT: GRADUATE SCHOOL

DEGREE: MBA

SURNAME, INITIAL: JAFTA , Ntembeko (Mr.)

STUDENT NUMBER: 205045928

1. Has this treatise/dissertation/thesis been submitted with your knowledge and support?

YES	NO
X	

(Please tick the appropriate response clearly)

2. Submission Recommendation:

A. Permission Granted for submission for examination	X
B. Permission Granted for submission for examination with reservations	
C. Submission against advice of Supervisor	

(Please tick only the applicable response clearly)

3. Did the candidate's research involve animal experimentation or human subjects as defined in the Nelson Mandela University Policy on Ethics in Research?

YES	NO
	X

(Please tick the appropriate response clearly)

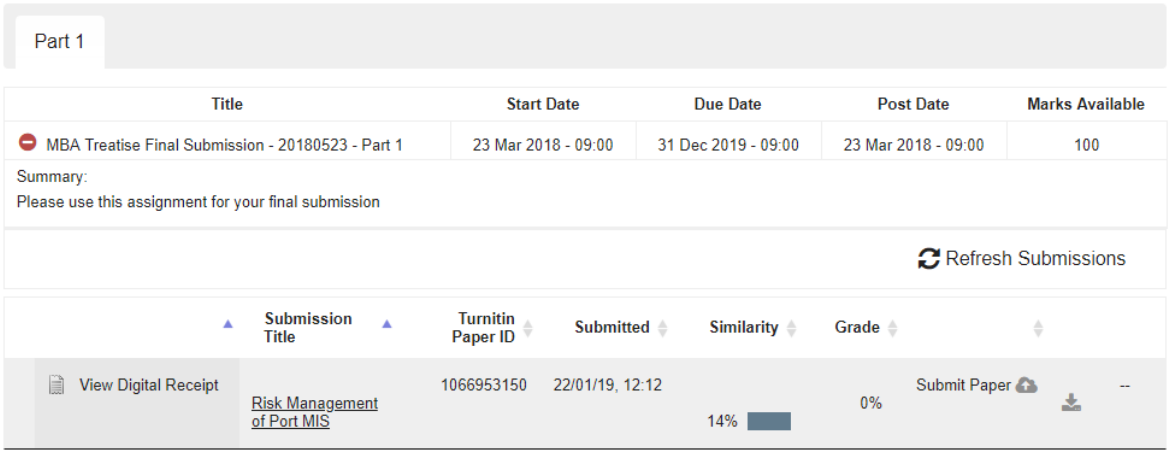
If YES, has clearance been obtained from the relevant Ethics Committee?

YES	NO

(Please tick the appropriate response clearly) If YES, kindly provide ethics clearance reference number)

SUPERVISOR	DATE 12/12/2018
CO – SUPERVISOR N/A	DATE
CO – SUPERVISOR N/A	DATE
CO – SUPERVISOR N/A	DATE

Appendix D
Turnitin Report



Part 1

Title	Start Date	Due Date	Post Date	Marks Available
MBA Treatise Final Submission - 20180523 - Part 1	23 Mar 2018 - 09:00	31 Dec 2019 - 09:00	23 Mar 2018 - 09:00	100

Summary:
Please use this assignment for your final submission

Refresh Submissions

	Submission Title	Turnitin Paper ID	Submitted	Similarity	Grade		
View Digital Receipt	Risk Management of Port MIS	1066953150	22/01/19, 12:12	14%	0%	Submit Paper	--