



Risk Mitigation Strategies in Information Systems Continuity Plans for Public Institutions: The case of Industrial Development Zones (IDZs)

Department of Information Systems

University of Cape Town

In partial fulfilment of the requirements for INF5004W

Date: 18/12/2017

Student Number: Mbulelo Tom

Student Number: TMXMBU001

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this literature survey entitled '*Risk Mitigation Strategies in IS continuity plan for an IDZ Organisation*' from the work(s) of other people has been attributed, and has been cited and referenced.
3. This paper is my own work.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.
5. I acknowledge that copying someone else's assignment, essay or paper, or part of it, is wrong, and declare that this is my own work.

Mbulelo Tom

Signed by candidate

Date: 18 December 2017

Table of Contents

Declaration	ii
List of Tables	vi
List of Figures	vi
Abstract	vii
1. INTRODUCTION.....	1
1.1 Background	1
1.2 Problem Statement	2
1.3 Context of the Study	3
1.4 Research Goal and Objectives	4
1.5 Research Methodology	4
2. LITERATURE REVIEW	6
2.1 Introduction	6
2.2 Risk in Information Systems	6
2.3 Internal Factors Associated with Risks of Information Systems.....	7
2.3.1 Top management support.....	7
2.3.2 Communication and sharing of information	8
2.3.3 Risk awareness and know-how.....	9
2.3.4 Mitigation strategies.....	9
2.3.5 Policy implementation	10
2.3.6 Technological factors	11
2.4 Risk Mitigation Strategies.....	16
2.4.1 Information systems continuity plan (ISCP)	18
2.4.2 Disaster controls	20
2.4.3 Risk and disaster management	22
2.5 Summary	25
3. RESEARCH METHODOLOGY	27
3.1 Introduction	27
3.2 Philosophy and Approach	27

3.3 Strategy	28
3.4 Research Design	29
3.5 Data Collection	29
3.5.1 Sample.....	30
3.5.2 Data-collection techniques	32
3.5.3 The development of the questions.....	33
3.5.4 Pre-testing of research instrument.....	34
3.6 Data Analysis	34
3.6.1 Thematic analysis.....	34
4. FINDINGS AND DISCUSSION	37
4.1 Introduction	37
4.2 Demographics	37
4.3 Technological Disaster	38
4.4 Human Factor	40
4.4.1 Disaster experience.....	41
4.4.2 Disaster awareness	42
4.5 Organisational Factors	43
4.5.1 Mitigation strategy solutions.....	43
a) Mobility as a solution	43
b) Revision of security policy	45
c) On-going continuous security checks.....	47
4.5.2 Documentation.....	47
4.5.3 Information difficulties and communication.....	49
4.5.4 Mitigation strategy challenges	52
a) Top management support.....	52
b) Lack of expertise	53
4.6 Summary	55
5 Conclusion	57
5.1 Background and Summary of the Study	57
5.2 Contribution of the Study	57
5.3 Future work	58
6 References	60

Appendix A67

List of Tables

Table 2.1: ISCP Phases.....	18
Table 2.2: Six key principles of IS continuity (Järveläinen, 2013; Continuity Central, 2013)	24
Table 3.1: The advantages of using a case study	28
Table 3.2: The participants selected for this research	30
Table 3.3: Composition and roles of the sample populations.....	31
Table 3.4: Emerging key themes.....	36
Table 4.1: Respondents profile	38
Table 4.2: Summery of the results.....	55

List of Figures

Figure 2.1: Turner’s Sequence of Event Model.....	12
Figure 2.2: Incubation stage of man-made disasters	14
Figure 2.3: Conceptual model of risk management factors.....	25

Abstract

Information systems (IS) and new technologies have become an integral part of conducting business in today's world. Almost all organisational sectors have adopted the use of IT systems and applications to conduct business and stay competitive in the industry within which they operate. However, if not well managed, Information Technology (IT) usage has the potential to expose organisations to various threats and vulnerabilities, which can have disastrous consequences. A risk mitigation plan is a strategy that helps an organisation to deal with a wide range of unexpected events. It covers a long-term plan and strategy that acts as a safety net to both avert a disaster and ensure long term survival.

The purpose of this study is to examine risk factors and associated mitigation strategies in public organisation. The case study is the Industrial Development Zone (IDZ) of South Africa. The study had two objectives: (i) identify risks associated with IDZ; and (ii) examine how IDZ address risk mitigation strategies. A qualitative enquiry was used to carry out the study. Data was collected via interviews that were conducted with executive and other key managers from the IDZ. The study identified human, organisational and technological risk factors as those that impact mitigation strategies in public institutions of South Africa. Proposed contextual solutions for these challenges included: (i) the adoption of mobile solutions and on-going research of new mobility solutions so as to keep up to date with technological advancements; (ii) the regular update of security policies of the organisation so as to align with environmental challenges; and (iii) on-going continuous security checks to evaluate and test disaster preparedness. Awareness of tools and applications used to address mitigation was seen as a key technological factor.

This study contributes to a better explanation of the challenges faced by IDZs in the developing country of South Africa, and puts forward recommendations for practice

1. INTRODUCTION

1.1 Background

As organisations continue to adopt, use and rely on technological applications and processes to address their business objectives, they are also simultaneously facing new challenges, such as threats to cyber security that arise from the use of varying technologies. The “pervasive use of technology has caused a critical dependency on IT” (Nfuka & Rusu, 2010) and, as business processes become more complex, inherent risk factors are bound to occur that if not addressed could lead to a reduction in the overall performance of an organisation (Mangla, Kumar & Barua, 2014). This becomes even more of a challenge when considering interdependencies between critical infrastructures “because they may allow a failure that is seemingly isolated in one critical infrastructure to cascade to multiple critical infrastructures” (Stergiopoulos et al., 2015, p. 34). As a consequence, organisations need to be up to date with how best to address these emerging challenges and continuously engage in risk mitigation strategies. According to Heiskanen (2012), public institutions in developing countries should continuously engage their risk mitigation strategies because they are more vulnerable to threats than their developed counterparts.

This study focuses on public institutions in developing countries because the landscape of developing countries places organisations at risk of potential threats which could consequently lead to mistrust from investors, suppliers, clients and stakeholders (Hiles, 2004). Ben-David et al. (2011, p. 2) identify five forces that shape the security landscape of developing countries: (1) poor ‘security hygiene’, i.e. the degree to which up-to-date software patches and recent malware protection are run; (2) unique usage patterns not commonly seen in developed economies, such as reliance on mobile technology for conducting financial transactions, even in places where credit cards and the web have not yet penetrated; (3) novice users who join the internet without knowledge of the risks posed online (keeping in mind that disseminating security educational material and tools is extremely challenging); (4) the use of pirated software, which may not necessarily pose a security risk but it can be challenging to verify that such software is not malicious; and (5) limited understanding of adversaries’ perspectives. If not addressed, these factors, including others such as political, organisational and cultural concerns, have the potential for significant adverse impacts on organisations. But, if well managed “with proper risk management and mitigation, failure could be reduced or negative impact and cost minimized” (Nfuka & Rusu, 2010; Franch et al., 2013).

Against this background, the purpose of the study is to explore technological risk factors and associated mitigation strategies in the public institutions of South Africa. Specifically, the study uses the IDZs, are government-created entities responsible for providing state-of-the-art locations for ancillary industrial investment (Lewis & Bloch, 1998) as a case study. In the South African context, IDZs are perceived as neither having met their goals nor generated anticipated development (Nel & Rogerson, 2013). Although challenges associated with their failure have been identified, they have not been examined from the perspective of technological risks posed to the IDZ systems (Mbambo, 2015) as well as associated mitigation strategies.

1.2 Problem Statement

Organisations in the public sector are now engaging in the use of information communication and technology (ICT) in their public service delivery endeavours (Nfuka & Rusu, 2010, p. 2). ICT use has several benefits, such as the potential to lower operational costs, increase transparency and enhance efficiency and policy effectiveness (Cordella & Tempini, 2015). Despite the benefits, ICT use poses some risks – an uncertain event or condition that, if it occurs, has either positive or negative effects on the project objectives of an organisation (Cagliano, Grimaldi & Rafele, 2015, p. 3). For example, “information is increasingly under threat as vulnerabilities in information technology systems that process, store, and transmit information are constantly being exploited for economic, espionage and other gains” (Yaokumah, 2015, p. 1318). Organisations can face technological risks resulting from an interruption/failure of information systems and equipment that result in harm to business processes, their surroundings and the environment. According to Gartner (2013), 40% of private, public and variously sized organisations go out of operation within three to five years after they experience such risks. If not well managed, risks can develop into a disaster – an occurrence that has the potential to cause serious havoc to business and social structures and current business processes (Shaluf, Ahmadun & Said, 2003).

In the IT context, Karkoszka (2014) describes three types of disasters: (i) natural, which are biological, geographical, climatological and hydrological disasters; (ii) man-made (technical) disasters, which are unexpected interruption from IT infrastructure components, such as networks, hardware and software, resulting in a disturbance to daily business process operations; and (iii) hybrid, which are a combination of both technical and natural forces. To ensure organisations are

protected from risks that can lead to these types of disasters, they need to have mitigation strategies in place to address such risks. However, many organisations do not engage in these strategies (AT&T, 2008) and those that do remain unprotected from technological adversities because of poor risk/security policies; lack of awareness, information and staff involvement when developing mitigation strategies; as well as a lack of security education and training programmes (Dangare & Mangrulkar, 2015). In South Africa, for example, the lack of, or out of date hardware and software; inadequate network systems; power failure; and lack of risk mitigation strategies, such as business and disaster plans, were potential causes for technological adversity (Stride, 2007). Given that “people’s perception of risk and its influencing factors has become an important element of research in past decades” (Knuth et al., 2015, p. 581), and the fact that there remain limited studies examining public institutions’ risk mitigation strategies, this study seeks to explore how public institutions in a developing country, such as IDZs, perceive technological risk and the factors associated with both risk and mitigation strategies.

1.3 Context of the Study

This study is situated in the context of a developing country – South Africa. The government of South Africa has dedicated IDZs, created to encourage increased levels of foreign direct investment in the economy. The strategic intent of most IDZs is, amongst others, to:

- Develop and establish a purpose-built world-class industrial park incorporating a delimited customs controlled area and linked to ports;
- Provide quality infrastructure, including information technology centres (ITCs) and transport infrastructure, business and utility services; and
- Attract foreign and local investment projects that will create jobs and which are export-led and sustainable, and to make arrangements for and mobilise financial, human and other resources for the development of IDZs to promote, foster and mentor Black Economic Empowerment (BEE) and small-, medium- and micro-enterprise (SMME) business opportunities in and around the zone (Karkoszka, 2014)

An IDZ is therefore an “industrial estate linked to an international air or sea port, which might contain one or multiple customs controlled areas (CCA) tailored for manufacturing and storage of goods to boost beneficiation, investment, economic growth and, most importantly, the development of skills and employment in these regions” (<http://www.sars.gov.za/>). Although IDZs do attract and focus investment, some IDZ projects have faced “considerable national criticism from business, other provinces, and civil society” (Haines & Hosking, 2012). This is because most African countries that have introduced initiatives such as IDZs have not been successful in reaping the acclaimed benefits. The challenges that South African IDZs face include, but are not limited to, poor governance and quality of infrastructure within the zones. According to Mbambo (2015), power and electricity remain major concerns for most IDZs. His findings show that some zones cannot accommodate electricity intensive operations and have resorted to focusing on enterprises that consume less electricity. IDZs also have challenges related to communication infrastructure, such as cellular phone signals and internet connectivity; and some do not have a deep-water port to handle bulk cargo ships or even an efficient transportation network linking them to the rest of the economy. IDZs also face structural disadvantages of operating in remote, under-resourced, low skilled and isolated locations (Nel & Rogerson, 2014). These challenges pose risks that could potentially lead IDZs to fail to generate anticipated development.

1.4 Research Goal and Objectives

The purpose of this study is to examine technological risk factors and associated mitigation strategies in Industrial Development Zones (IDZs) of South Africa. The study has the following objectives:

- 1) Identify risks associated with IDZ.
- 2) Examine how IDZ address risk mitigation strategies.

1.5 Research Methodology

The study followed a qualitative approach in order to understand the risks from the perspective of IDZ stakeholders and to engage with them on the employed mitigation strategies. A qualitative approach allows the researcher to become immersed in the contextual setting and it must therefore be

acknowledged that the stakeholder's reality is socially constructed by the researcher, who is an active participant in the research environment and is laden with preconceptions, assumptions and beliefs from their cultural settings. The researcher also creates and shapes their own understanding of risk and mitigation strategies based on their social context. The study adopts qualitative interviews as a source of data collection and uses thematic analysis to make sense of the data.

2. LITERATURE REVIEW

2.1 Introduction

The purpose of this chapter is to give a conceptual background to the study. The chapter commences with a brief definition of risk in information systems. The next section presents the factors associated with risk mitigation, as well as an overview of a technological disaster with a theoretical model on disasters and how various disasters can be formed. Thereafter, the chapter reviews risk mitigation strategies to elucidate the core role of disaster management in an organisation. The chapter closes with a summary.

2.2 Risk in Information Systems

Every organisation faces risks in its operations. These risks are dependent on the contextual challenges the organisation faces. Organisations that rely on ICTs to meet their objectives face technological risks, such as the possibility of destruction to a business process and to related information, resulting in an accidental event that adversely impacts the availability of the information system (Vernim & Reinhart, 2016). Understanding the cause of these risks has been of great concern for researchers and practitioners alike because after one understands the cause, one can provide mitigation strategies to address risk factors. Risks can emanate from both within and outside of the organisation (Aghili, 2010).

External forces, such as market pressure, institutional regulation and sociocultural factors can pose potential risks to an organisation. For example, organisations situated in contexts with a weak institutional framework for the adoption and use of mature ICT related innovations pose security and privacy concerns for both consumers and the organisation (Molla-Adankew, Molla & Licker, 2005). The general infrastructure, such as transportation and ICT, has been reported as potentially detrimental to the smooth running of ICT related systems. For example, in Ethiopia and Nigeria, the lack of reliable power supply is noted as a key challenge for the adoption of sophisticated solutions and the smooth running of online services, such as e-banking (Apulu & Latham, 2011, p. 72). The more sophisticated and unpredictable the external environment becomes, specifically with reference to technological innovation, the more at risk an organisation becomes because “today’s strongly

connected, global networks have produced highly interdependent systems that we do not understand and cannot control well. These systems are vulnerable to failure at all scales, posing serious threats to society; even when external shocks are absent. As the complexity and interaction strengths in our networked world increase, human-made systems can become unstable, creating uncontrollable situations even when decision-makers are well-skilled, have all data and technology at their disposal, and do their best” (Helbing 2013, p. 51).

Most studies have shown that external pressures have great influence on how organisations embark on ICT and related innovation and can subsequently influence how the organisation responds to risks. This study focuses on internal factors that pose a risk to an organisation as it is well established that at least half of the breaches to information systems emanate from the organisation itself (Spears & Barki, 2010), and due to the fact that information technology related projects have a long history of failing (Bakker & Leiter, 2010). To this end, risk management has become a key area through which organisations try to provide mitigating solutions to potential risk factors before a disaster occurs (Shaluf, Ahmadun & Said, 2003).

2.3 Internal Factors Associated with Risks of Information Systems

Internal factors are commonly associated with top management support, communication and sharing, risk awareness and know-how, mitigation strategies, policy implementation and technological factors. These are discussed in the following sub sections.

2.3.1 Top management support

A successful project in IS has the backing of management who provide financial resources and other related resources, such as human resources, for its execution. Top management support has been reported as an advantage to prevent critical risk issues and provides structure to policies and tools (Werlinger, Hawkey & Beznosov, 2009). Hausmann and Williams (2015) suggest that these policy structures and tools allow top management to focus on critical issues within the organisation and enable them to prioritise their limited time and give support to IS projects. With a structured communication mechanism, this further allows management to collaborate with employees on

identifying specific risk issues that the company may experience, without risk of confusion and loss of productivity (Hausmann et al., 2015).

Top management support defines the collaboration mechanism between them and employees as essential for the success of any project initiative of the organisation (Helbing, 2013). Therefore, applying a balanced management approach, such as a top-down and a bottom-up approach concurrently, rather than using the one-sided approach of top-down, will enhance collaboration between management and employees (Hausmann et al., 2015).

The consequence of not having management support for a mitigation strategy is the risk of no budget being allocated to initiate the strategy (Helbing, 2013). This will minimise the chances of project success and prevent its implementation (Vernim & Reinhart, 2016). In addition, if there is no management support of a strategy, when a crisis does occur management will be less likely to interfere, the strategy will not receive cooperation; people will obstruct its implementation and will not use the new system or continuity plan (Vernim et al., 2016).

2.3.2 Communication and sharing of information

Whilst management support is critical for project success, it is important that communication processes within the organisation are well defined for information flow between organisational members. Lack of information sharing and communication has been associated with the development of risk factors. Järveläinen (2013), for example, reports that although some organisations do have risk mitigation strategies, they fail to adequately communicate these to the rest of the organisational members. This lack of communication can lead the organisation to become vulnerable to potential threats. Recurring organisational weaknesses due to human factors, together with the inflexibility of an organisational hierarchy that results in a failure to reveal important information, or where information is made available to those who do not understand its significance, with issues between experts in cross departmental units, can result in comprehensive disaster for an organisation (Järveläinen 2013).

2.3.3 Risk awareness and know-how

According to Dangare and Mangrulkar (2015), disasters can be influenced by employees' lack of awareness, skill, familiarity and exposure. Organisations need to engage in constant communication, and regular awareness and training programs to highlight policies. This can be achieved, for example, through a persistent awareness drive. According to Continuity Central (2013), employees are eager to learn more about policies on disaster awareness and preparedness and are seeking to increase their knowledge in this domain and enhance their skills on preparedness. Such awareness and training programs have the potential to reduce perceived risks and increase these levels of preparedness, subsequently having an effect on behaviour associated with how risk is managed (Paton, 2003; Dangare et al., 2015). In addition, these programs can act as a catalyst to improve employee morale because low morale can reduce effectiveness, safety or system performance (Jones et al., 2015). A lack of morale can stem from the negative feelings of an employee, such as dissatisfaction and job role dislike. Dangare et al. (2014) indicates other factors that could lead to lack of morale and later cause technological disaster, such as an unsafe work environment, lack of communication and lack of involvement. The growing size of technical systems errors and rapid changes in job roles affect the ability of the operative staff to cope with unforeseen disturbances. These factors are worsened by human tendencies to blame individuals for bad outcomes (Jones et al., 2015, p. 55). Having considered the role of management approaches, communication and risk awareness, and this literature review will now discuss mitigation strategies.

2.3.4 Mitigation strategies

Some organisations do not invest in risk mitigation strategies, such as a continuity plan. A continuity plan shows how the organisation can continue operating after a disaster (Jones et al., 2015). Risk mitigation employs unique strategies for assessing and measuring the level of risk. Such strategies involve careful strategic alignment of protection to information systems and in particular business continuity (Järveläinen, 2013). In an organisational context, risk mitigation provides a benchmark to better manage an organisational programme by balancing opportunities and risk improvement (Continuity Central, 2013). According to Järveläinen (2013), failure to adopt a risk mitigation strategy points to a lack of awareness, inadequate documentation and underestimation of serious threats. An example could be the 9/11 terrorist attack in 2001 at New York's World Trade Centre, where most

organisations with mitigation strategies in place were able to continue with operations after the disaster (Continuity Central, 2013).

According to Continuity Central (2013), 58% of all system downtime, data loss and malfunctioning of financial services and telecommunications is caused by the lack of a continuity plan. Continuity Central (2013) found that almost all complex systems are a form of production (daily business activities) and listed five basic elements – and agents – for a successful productive system:

- Functional and line managers, i.e. those who implement the operational strategies.
- Decision makers, i.e. solution and business architects.
- Pre-conditions, i.e. a skilled and knowledgeable workforce.
- Productive activities, i.e. human activities required to deliver the right product at the right time.
- Defences, i.e. where the productive activities encompass exposure to threats, both the human and mechanical elements of the system must be made available with adequate safeguards to prevent injury, damage or costly outages.

2.3.5 Policy implementation

Weak policies associated with IS use can have negative consequences for the organisations. For example, policy failure is defined as an inappropriate organisational behaviour that reduces safety and effectiveness of the system. It consists of managers' lack of experience, employee morale and strategic business pressure leading employees to neglect safety issues (Jones et al., 2015). According to Werlinger et al. (2009), revising security policies provides a framework that can be followed by all staff and to which they can also contribute using their own experience. This helps organisations to minimise risks and allows them to respond quickly. These risks are usually issues such as insecure use of the internet, revealing information to unauthorised sources, sharing company information with unknown people, failure to revise server passwords, policy not being followed and systems being left unlocked (Werlinger et al., 2009).

2.3.6 Technological factors

Technological factors relate to Perrow's (1967) theory, which states that no matter how safe a device, there is an inevitable possibility of fault and, therefore, there is no such thing as a risk-free area, machine-driven agent or perfect individual (Sagan, 2004, p. 17). Organisations are complex, and their IT systems increase this complexity because IT systems are complex due to their interdependence. System interdependency can lead to a major system failure. Technical integrity is a process, procedural, assurance and verification function that ensures that a process and systems meet their requirements under stated conditions (Continuity Central, 2013). Organisations often use backup procedures as the technical integrity to shield themselves against unforeseen disasters. As a result, organisations are able to predict measure and eliminate any malfunctioning practises that may take place in the system and processes (Werlinger et al., 2009). Because IT systems have inherent control mechanisms that can potentially detect and predict threats, the very complexity of a system can result in the organisation being over confident, complacent and in denial in the face of imminent disaster, and thus being prone to ignoring the warning signs. Due to this, organisations are cautioned against having full confidence in IT systems without having mitigation strategies in place (Werlinger et al., 2009; Hiles, 2004). For example, according to Continuity Central (2013), 58% of organisations without technical integrity could not survive or retrieve lost information after a disaster. This later causes distrust and a bad reputation with stakeholders, suppliers and business partners. It is therefore advised that organisations have risk mitigation strategies in place to address system failures or potential threats.

Turner (1976) developed a model (Figure 1) to describe the sequence of events associated with the development of technological (man-made) disasters (Shaluf, 2008). The latest literature of Hollnagel (2014) describes Turner's sequence of event stages, as they are still applicable as organisations continuously experience recurring man-made disasters. According to Hollnagel (2014), these stages not only describe the sequence of events but also serve as a guideline as to how a man-made disaster can be formed and how they can have negative impact on the organisation. Stage 1 of the model is the notional normal starting points where the organisation and employees adhere to norms and standards, and operations function as normal (Hollnagel, 2014, p. 3). Therefore, employees are still adjusting to standards, procedures and policies of the organisation and they adhere to it. According to Lewis and Liu (2017), one unique common habit of employees is that when they become too

comfortable in their environment they become reluctant, i.e. they neglect organisational standards, do not adhere to norms and operational functions and ignore policies.



Figure 2.1: Turner’s Sequence of Event Model

Stage 2 relates to the incubation period wherein errors occur and accumulate. Hollnagel (2014) postulates that man-made disasters frequently start small and go unnoticed. This stage relates to poor operational and managerial decisions which amount to an incubation period. Over a long period, problems accumulate until these explode into the form of an accident. This stage has the potential to hide warning signs. These can be difficult to notice and failure can exist unnoticed in systems for a long period of time, which may lessen the opportunity to introduce interventions and a risk mitigation strategy (Hollnagel, 2014). Therefore, the organisation subsequently finds itself in the disaster stage. Stage 3 is characterised by repetitive patterns that serve as a warning and which, if ignored, align to create a disaster (Hollnagel, 2014). It is at this stage where ignored warnings accumulate to trigger disaster. This is a stage where warning signs can be misread, evidence can be misinterpreted and where organisations fall into an incompetent trap (Hollnagel, 2014, p. 4). During this period, minor events can interact and accumulate to produce major system failure.

Stage 4 describes the actual occurrence of a disaster. A disaster is generally described as an interruption of normal business processes resulting from the interruption of the IT infrastructure components used to support them. This may be caused by minor events that were ignored until they

became a disaster. This includes hardwires, software, networks and information systems, as well as data itself (Hollnagel, 2014). Typically the nature of this event is that it disrupts business from operating as normal to the extent that monetary losses are incurred (Hollnagel, 2014). From this perspective, a disaster is defined as an event resulting from the inability of an organisation to provide critical business functions for a period of time, and which causes them to move from normal operating procedures to employ a mitigation strategy procedure (Shaluf, 2008).

Stage 5 is associated with activities that bring an organisation to the point where it may resume basic operational functioning. At this stage the organisation employs recovery mitigation strategies as far as man-made disasters are concerned. Mitigation strategy resides in resilience engineering. Resilience is a recovery system's ability to effectively adjust to hazardous events rather than disruption and surprises (Hollnagel, 2014). According to Hollnagel (2014), the following important functions of mitigation strategy management are required to be effective:

- Perform risk analysis and assessment for IT services in order to identify the threats, vulnerabilities and assets;
- Planning mitigation strategies and assessing cost; and
- Certifying solutions that are not based on compliance but rather on demonstrating recovery readiness and accountability.

Once these mitigation management processes are in place, the organisation is expected to design a solution, certify it, and implement it in accordance with the information yielded by the abovementioned processes.

Finally, Stage 6 describes the process of adjustment, in which activities are focused on attaining full operational business functioning. According to Hollnagel (2014), this stage suggests that the designed mitigation strategy can be effective only when the organisation is business-driven. Recovery times and recovery points must be driven by organisational recovery culture, not only by IT capability (Hollnagel, 2014). IT capabilities should evolve to achieve business recovery requirements. Therefore, cultural adjustment of mitigation strategy is a continuous process that needs to be maintained and entrenched in the organisation (Hollnagel, 2014).

Wright (2010) and Hiles (2004), building on Turner’s 1976 sequence of events model, see a failure of foresight and absence of knowledge and information amongst the groups and/or individuals as causes of a disaster. Turner (1976), in his work on various disasters, notes a number of features and similarities common to organisations that form and contribute to man-made disasters. Jones et al. (2015) develop this idea in their argument that in any organisation learning from accidents or mistakes reinforces the desire to improve management practices and rectify mistakes. Common features and similarities of man-made disasters (Figure 2) include: (a) rigidities in institutional beliefs, which create and atrophy a particular culture; (b) distracting decoy phenomena; (c) neglect of outside complaints; (d) multiple information-handling difficulties; (e) exacerbation of hazards by strangers; (f) failure to comply with regulations; and (g) a tendency to minimise emergent danger (Turner, 1976; Shaluf, 2008). In Figure 2.2, Heiskanen (2012) elaborates on the incubation stage in Turner’s model of five stages that leads to a man-made disaster.

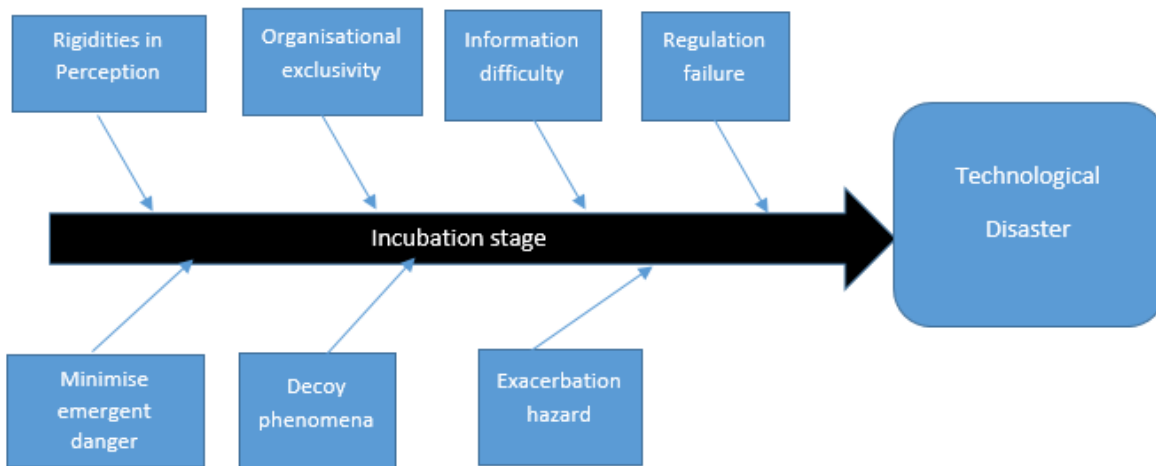


Figure 2.2: Incubation stage of man-made disasters

Turner’s model (1976) and Heiskanen’s incubation model (2012) comprise seven stages in the process of generating a technological disaster:

1) Rigidities in perception

The organisational cultural setting and intuitional factors inhibit the perception of a disaster. In particular, failure of perception may be created and reinforced by a set of organisational cultural and subcultural beliefs. Turner (1976) suggests that all organisations cultivate within the constituent of constant culture, which is related to their environment and tasks. Although part of organisational effectiveness stems from their development of such a culture, this can also lead to collective blindness

to important issues, which might drive them to a disaster. Moreover, if these beliefs and culture are long established within the organisation, they will inevitably influence the perceptions and attitudes of staff (Turner, 1976).

2) Organisational exclusivity

Turner (1976) suggests that defiance of an organisation by choosing to ignore outside warnings can result in disaster. In his study, Turner (1976) gives an example of the concern of an outsider individual who foresees a hazard that ultimately leads to disaster. Because the organisation developed a culture of 'We know our flaws better than outsiders when it comes to the dangers of the situation with which we are dealing', the organisation was facing dismissal from the local municipality as well as a bad reputation.

3) Information difficulties

Turner's 1976 model suggests that information difficulties are sometimes caused by an ill-structured organisation, which militates against the organisation's capability to handle a problem. According to Turner (1976), to solve this the organisation needs to expand its resources in such a way that the process of identifying and tackling the problem is not ill structured. Furthermore, Turner (1976) suggests that information difficulties can occur when inaccurate, misleading or conflicting information is communicated from one person to another and important information does not reach the relevant people. Even if relevant personnel receive information, the full import is often not perceived by the relevant person because s/he fails to see its significance.

4) Failure to comply with regulations

Turner (1976) suggests that this happens when regulations, although satisfactorily implemented, are not complied with simply because they are out-dated and not easy to apply in changed social, technological and cultural settings.

5) Minimising emergent danger

In this stage, Turner (1976) sees recurring problems occurring when an organisation fails to observe the magnitude of danger, even if the danger is clearly visible. Turner (1976) notes that even if the danger is seen and acknowledged, no one seems to take responsibility for averting the danger; instead everyone in the organisation plays the blame game.

6) Decoy phenomena

In this stage, Heiskanen (2012) explains that distraction and confusion occur about roles when planning a recover approach. According to Turner (1976), this is caused by a single unit involvement when planning a recovery plan. As suggested by Heiskanen (2012), a recovery plan should be cross functional and roles must be clearly identified.

7) Exacerbation hazard

Heiskanen (2012) suggests that this happens when danger occurs and no one knows what to do due to a lack of recovery in place. Sometimes a recovery plan is present but, due to a lack of communication or information sharing, people become unaware if there is a recovery plan in place or not. Therefore, when the crisis strikes no one knows what to do.

2.4 Risk Mitigation Strategies

Risk mitigation is the action taken by an organisation to reduce adverse impact (Talluri, Kull, Yildiz & Yoon, 2013). Lewis et al. (2017) and Jones et al. (2015) see mitigation as being an essential internal risk control for any organisation to safeguard itself from the negative effects of risk. It holds a unique strategy that is closely related to and matches the business profile (Talluri et al., 2013) and allows organisation to assess risks and predict vulnerabilities and give them the ability of what to do and how should a disaster occur. Especially in the public sector, investors, suppliers and clients develop trust and confidence when a mitigation strategy is in place (Karkoszka, 2014). A study by Pepitone (2012) shows that, any organisation with a mitigation strategy has the ability to sustain any terror event, as well as gains trust and good company reputation. Ideally, a mitigation strategy is not one overwhelming activity, it can rather be seen as a phased activity, involving an information systems continuity plan, disaster recovery, incidence response planning, business continuity planning and risk management (Pepitone, 2012). Each activity is unique, requiring a different skill set, specific documentation and planning. Therefore, the end result should be a set of documentation that provides a quick reference for responding to a disaster (Talluri et al., 2013). When done properly, these mitigation strategies will prevent many common crises situations, minimise the impact of actual disasters and speed up the return to normal operations (Talluri et al., 2013, p. 258).

Risk mitigation strategies are essentially an approach to putting into practice information systems' continuity plans to protect the organisation's critical information (Bakker & Leiter, 2010). To address risk mitigation, organisations adopt a business continuity management (BCM) approach that assists them to identify and avoid potential damaging incidents that would have a severe business impact (Järveläinen, 2013). It offers a suitable tool for engaging top management in the discussion relating to the business implications of different operational incidents that are not necessarily security related (Järveläinen, 2013, p. 70). These include antedating organisational risks; ensuring the continuity of business operations; shielding critical functions at all times; ensuring effective, quick and efficient time to respond to a disaster; and ensuring a holistic on-going BCM process (Järveläinen, 2013). According to Elliott, Swartz and Herbane (2010), the primary objective of BCM is to bring confidence to an organisation and to build resilience in ensuring long-term survival in the face of rapid changes to business environments, disasters, organisational risk and crises. It further assists organisations to study clearly and in detail the worst possible future scenario in terms of how quickly the organisation can restore its normal operations, and where and how the organisation would operate following a disaster. While the scope of continuity management extends to all business operations, Järveläinen (2013) argues that its proactive application in the area of IS could foster its evolution and increase the robustness of IT services.

There are several processes executed under BCM for planning the recovery of general business operations in the event of disruption: a business continuity plan (BCP), which focuses on business processes rather than IT infrastructure to ensure that an organisation can continue; an IS continuity plan (ISCP), which encompasses activities that safeguard IT services and information systems and ensure that they carry on in the event of a disaster; a disaster recovery plan (DRP) with the purpose to ensure the accuracy and consistency of the data stored in a database in order to restore operations faster, thus ensuring the continuity of operations and shielding sensitive information; and an incidence response plan (IRP), a sub tool which is meant to protect an organisation's information assets and mitigate damage from incidents should they occur (Best Computer Practices, 2009; Continuity Central, 2013). From an IT perspective, several risk mitigation strategies are proposed: an organisation provides an ISCP and a DRP with a benchmark to better manage organisational programmes by balancing opportunities and risk improvement (Raval & Fichadia, 2007).

2.4.1 Information systems continuity plan (ISCP)

An ISCP is defined as “a complete process of developing measures and procedures to ensure an organisation’s disaster preparedness. This includes ensuring that the organisation would be able to respond effectively to a disaster and that their critical business processes can continue as usual” (Järveläinen, 2013, p. 70). It includes preparing the organisation to respond effectively to an incident at the moment it occurs for the purpose of ensuring the continuity of business operations (Järveläinen, 2013, p. 70). Heiskanen (2012) advocates that an ISCP be proactive, meaning that it initiates steps in advance to ensure that, no matter what happens, an organisation and its operations will not be disrupted. Its purpose is not only to forestall disaster but also to assist an organisation to recover from damage that has already occurred to the system and infrastructure. Pepitone (2012) concurs with Järveläinen (2013) that this plan helps an organisation to recover and resume its normal operations and critical processes. An ISCP therefore defines procedures an organisation should have in place to prevent interruption of critical services and to ensure that essential functions can continue during and after a disaster (Jones et al., 2015). Three phases have been identified that constitute an ISCP, as shown in Table 2.1.

Table 2.1: ISCP Phases

Resolve	<p>What critical business processes and supporting equipment does the organisation have? How long can each of those processes remain unavailable before the functioning of the organisation is seriously or permanently disrupted? Are there any options for outsourcing or replacing those processes during the crisis? Which partners and suppliers can respond quickly? What specific risks do the organisation face and who needs to be involved in developing the continuity plan?</p>
Response	<p>Who needs to form part of a disaster response team and who will declare a disaster? How will a recovery team communicate? How will information be circulated to all employees? In the event of any kind of disaster where will people work and with what equipment?</p>
Rebuild	<p>Who will be responsible for the damaged IT infrastructure? How will the insurance claims be handled? What will be done to maintain the IT systems, servers and productivity levels during and after the crisis?</p>

The purpose of the resolve phase is to identify and predict potential disasters, and the preventive actions that should be taken. Organisations are required to document the current state, i.e. current business process, risk status and how things are currently done in the organisation, and provide procedures for on-going pre-empting action to mitigate risks (Heiskanen, 2012). The study of Pepitone (2012) suggests that all organisation that have written procedures for routine maintenance

activities in and out of the building, with the inclusion of steps to prevent system failure and regular system and server inspections, have the ability to resolve any predicted disasters. Having written rules will help the organisation by ensuring that if by any chance one of the routine activities, such as an off-site server, fails or burns out; at least they know that there are other written rules that can be used, such as insuring IT infrastructure (Heiskanen, 2012). It will further reduce the odds of crises and this might reduce legal liability should crises occur (Heiskanen, 2012).

The resolve phase also aims to provide organisations with an integrated defensive and offensive capability to deal with their competitive environments. A highly available IT infrastructure that has both people and systems residing entirely within the potential impact zone of a single disaster will definitely not provide an organisation with the resiliency to maintain operations through a disaster (Järveläinen, 2013). Järveläinen (2013) posits that many organisations ideally maintain the geographic separation of multiple data centres at appropriate distances, and thus have the ability to survive any technological events caused by a disaster. While organisations may be able to recover applications to a replicated site, if only a limited number of skilled employees are stationed at a recovery station the organisation might not be able to recover from an operational perspective (Continuity Central, 2013). For example, a travel booking system was disrupted during recent picketing in the public sector but employees were able to continue work by going to another location and so the residual effects of the disaster were prevented. This relates to the study by Jones et al. (2015) and suggests that organisations should take advantage of strengthened physical locations and consider having an alternative work-site with strong infrastructure.

Heiskanen (2012) recommends that once these ISCP phase questions have been addressed, the organisation monitors risk, maintains the environment and documents the crises or emergency response measures as part of an on-going preventive action to mitigate risks (Pepitone, 2012). Järveläinen (2013) argues that in any organisation or business people will come and go, business processes will change, technology will improve and change, equipment will be replaced, and all these changes will cause risk to transform and migrate. Järveläinen (2013) suggests that an IT unit should have written procedures for a backup regimen, continuous security screening and regular IT system maintenance procedures.

During the response phase the organisation needs to know well in advance what to do if it wishes to avoid being failing under the weight of a crisis. According to Hiles (2004), organisations should not treat this phase as finding a one-size-fits-all solution. They should start by documenting basic

response procedures, the people to be involved and contact information for everyone that might need to be notified. This fosters a positive situation, as everyone understands what to do, which relates to using more than one communication mechanism as some communication mechanisms might not be available during major havoc (Lewis et al., 2017). The primary advantage of this is that documentation for dealing with the most common situations will be brief and targeted (Lewis et al., 2017). First responders will know what they need to do to manage these most likely emergencies, as it is significant to gain a quick control over small crises quickly so that they will not develop into major disasters (Lewis et al., 2017). Once the abrupt crisis situation is stabilised, attention turns towards rebuilding and returning to normal.

The final phase – rebuild – has the main goal of replacing or reconstructing damage that may have been caused by a disaster (Lewis et al., 2017). This includes ensuring that the full extent of the damage is assessed to avoid long lead-time items that can be ordered in advance to minimise downtime. This is where good documentation of all organisation assets is essential (Järveläinen, 2013). Ideally, the response and rebuild phases will correspond to some extent so that recovery time can be shortened (Heiskanen, 2012). Having documentation and people with skill sets for these efforts will speed up and simplify both efforts.

2.4.2 Disaster controls

According to Heiskanen (2012), risk acknowledgement of risk assessment actions should be taken to minimise the risk. Failure to do so will have a negative impact on organisation finances. An example from a study of Järveläinen (2013) was when a Parastatile building burnt down in a fire that resulted in employees evacuating the building. However, due to strong controls and competent responsible personnel they were able to survive. According to Lewis et al. (2017), the organisation survived because of the monthly practise or drill they conduct as safety awareness. Types of disaster controls are discussed below.

2.4.2.1 Ability to monitor

Monitoring refers to the ways an organisation looks at opportunities and threats that may happen in the short- or long-term both inside and outside of the organisational environment (Hollnagel, 2014,

p. 8). A necessity for monitoring is understanding what the organisation is looking for, and monitoring for signs of what may happen (Hollnagel, 2014, p. 8). One of the benefits of monitoring is that it becomes easier to respond faster or even to pre-emptively. In addition, it enables the organisation to address possible changes before they become a reality (Hollnagel, 2014).

2.4.2.2 Ability to respond

This refers to the organisation knowing what to do when confronted with disruptions and disturbances (Hollnagel, 2014, p. 6). This relates to procedures, activities and adjustment of on-going functioning to match the new condition (Hollnagel, 2014, p. 6). However, this will require resources being ready or flexible enough as it may be necessary for an organisation to change from a state of normal operations to a state of readiness (Hollnagel, 2014, p. 6). This points to other concerns, such as the availability of resources, the ability to sustain the response for a period of time and the monitoring of effect (Hollnagel, 2014). However, it is significant for an organisation to know how the set of events has been defined and if the responses are ever revised (Hollnagel, 2014). Yet another concern is how readiness to respond is maintained, i.e. how plans are kept up to date and how readiness to respond is verified (Hollnagel, 2014).

2.4.2.3 Ability to learn

Ability to learn is to make use of experiences and change behaviour as a result of this experience (Hollnagel, 2014, p. 10). It is a milestone and the core stem of response and monitor (Hollnagel, 2014). Neither responding nor monitoring can improve unless some kind of learning takes place (Hollnagel, 2014, p. 10). According to Lewis et al. (2017), it is undeniable that future performance can only be improved if organisations learn from past performance, learn the right lessons from the right experience, and learn from what went wrong as well as what went well (Hollnagel, 2014).

Consistent with that philosophy, Hollnagel (2014) asserts that more can be learned from events with serious outcomes, such as unusual crises, threats and disasters. According to the general learning theory, effective learning requires three conditions: first, that there is sufficient opportunity to learn. Second, there is some similarity between the situation and events. Lastly, it must be possible to confirm that something has been learned (Hollnagel, 2014, p. 10).

2.4.2.4 Mobility solution

The mobility solution allows employees to plan and perform day-to-day business activities away from the physical building in the event of infrastructure failure or any form of a disaster (Hollnagel, 2014). The more employees can use their mobile devices and applications as a solution to access and share corporate resources from anywhere at any time, the better they can collaborate on efficient project management in the case of access denial from a building (Ahmad, et al., 2012). These are essential tools for conducting work away from the workplace, the idea being that it is easy to respond to demand and work functions. Hollnagel (2014) advocates that thinking beyond the physical building needs to be proactive, meaning steps should be initiated in advance to ensure that no matter what happens an organisation and its operations will not be disrupted.

2.4.3 Risk and disaster management

Jones et al. (2015) define risk and disaster management as a process involving the investigation of the possibilities of losing an IT system and, from this, framing strategies to minimise the damage (Järveläinen, 2013). Järveläinen (2013, p. 70) postulates six fundamental concepts that are key to the management of risks and disasters.

- (a) Impacts: understanding the consequences of risk occurrence by assessing risk impact and benchmarking the mitigation actions. Risk cannot be easily identified and the impacts and causes of risks can be distracted by the risk itself (Järveläinen, 2013). Therefore, the attempt to mitigate risk is based on measuring risk impact and its probability to occur. According to Jones et al. (2015), in many cases less important risks can appear much more threatening and important risks can be underestimated.

- (b) Threat: upon completing a risk assessment, the next step is the identification of how risks can impact the organisation and developing a precautionary measurement for reduction of risk. The SWOT model by Mintzberg, Ahlstrand and Lampel (1998) in the study of Jones et al. (2015, p. 55) focuses on scanning the business environment in order to identify the organisational environment. Performing risk assessment using the SWOT model is likely to improve the way the organisation sees its future for the purpose of minimising risk and impact of risk (Jones et al., 2015). Similarly, an

organisation without risk assessment will likely be exposed to a higher level of risk when compared to one with a risk assessment (Ozkazanc & Yuksela, 2015, p. 752). Having a risk assessment using SWOT analysis enhances the organisational capability to resist disasters and recover.

(c) Resilience: this is the ability to absorb external pressure and become stronger. When risks are known and mitigation plans are in place, vulnerabilities are reduced and this enables the company to survive. Heiskanen (2012) argues that organisational capability of resilience can be accomplished by integrating the mitigation strategy with its components, such as DRP, IRP and BCM. In doing so, Ozkazanc & Yuksela, 2015 have seen a potential role to integrate the mitigation activities of the organisation where risk mitigation is designed to improve resilience since it puts into planning approaches, structure and skills in multi-functional. This will strengthen resilience by shoring up areas of vulnerability (Ozkazanc & Yuksela, 2015).

(d) Effectiveness: the recovery plan should be tested and communicated to everyone so that they know what to do when disaster strikes. The literature of Ozkazanc & Yuksela, 2015 indicates that the effectiveness of the mitigation approach relies on performing a number of activities and encourages people to be involved in the mitigation strategy through periodic testing, updating, training and maintenance. Everyone within the organisation must be involved in the mitigation strategy for it to be effective (Jones et al., 2015). These activities involve creating teams, assigning roles and responsibilities, developing backup and disaster recovery plans, performing risk analysis, testing plans, and training, maintaining and updating developed plans (Continuity Central, 2013).

(e) Response: examining and deciding on the how of the recovery. This should include all responsible personnel from different departments giving input as to how the organisation should recover. This phase involves coordination and collaboration between all organisation units and management levels (Continuity Central, 2013). It therefore requires a state of change and is about new way of responding and reacting to unexpected incidents. Therefore, perceiving the response tactic as being merely a planning exercise is not adequate. It has to be a forward thinking, daily activity that emphasises flexibility and technological integration that should be embedded into the culture of the organisation (Elliott, Swartz & Herbane, 2010).

(f) Interests: protection of all stakeholder interests. This relates to gaining confidence from stakeholders and clients by ensuring that the organisation takes measures of recovery against vulnerabilities (Jones et al., 2015). This builds a good organisational reputation and competency in

the industry in which the organisation operates. Therefore, investing in risk management promotes confidence not only in the organisation but to relevant stakeholders as well (Järveläinen, 2013).

There are other additional key principles that relate to the abovementioned principles. The relationship between these is that they enable organisations to ensure the continuity of data, technology and services with the management of risk and disaster. According to Continuity Central (2013), best practise is that all organisations adopt as many continuity principles as they can to ensure that they are safely covered, so that if one of the principles is not well defined they will still be protected. Table 2.2 discusses the six key principles associated with risk and disaster management cycle.

Table 2.2: Six key principles of IS continuity (Järveläinen, 2013; Continuity Central, 2013)

Principles	Definition	Example
Protect	Protecting the ISC or ITC environment is critical for maintaining the desired levels of system availability for an organisation.	Processes and plans to defend against threats, i.e. ensuring a backup so that a secondary copy of data is always available.
Detect	Detecting incidents at the earliest opportunity will minimise impact on services, reduce recovery effort and preserve quality of services.	Use of monitoring and alert tools to detect capacity deficiencies, such as running out of memory or storage.
React	Reacting to an incident in an appropriate manner will enable efficient recovery and minimise the incidence and length of down time.	The predefined procedure the operator has in place to communicate alerts to the relevant parties for them to fix a threat and, if they do not, the procedures to escalate the issues in order to forestall the threat.
Recover	Recovery of services should be performed in a controlled and predetermined fashion.	Activities that must be performed in a controlled and predetermined fashion to bring the business processes and systems back to a point of operation.
Resume	A full understanding of the recovery priorities, as well as the recovery point and recovery time objectives, assigns priority to the reinstatement of the most critical services.	Enkindling the activities, plans and documentation used to re-commence business operation.
Return	The process of returning from disaster mode to normal operations is often neglected by organisations. All IS continuity plans should have an existing strategy that allows them to vacate their ITC disaster recovery centre when the time comes.	The process of going back to normal operations and returning to the facilities that were damaged during the disaster.

In addition, having established that risk and disaster can be better managed by adopting key principles and concepts that can minimise system instability and data retention, it can be observed that BCM is part of the risk mitigation strategies that ensure the continuity of business, ensuring effectiveness and

efficient response time (Järveläinen, 2013). The next section will elaborate more on BCM and its components.

2.5 Summary

The literature review identified seven internal factors that are key to the continuous operation of IT systems after a threat or disaster has occurred. These include communication, management support, risk awareness, expertise, adequate resource allocation, policy implementation and technology. From a technical perspective, IT systems are to conform to technical integrity for them to support continuous operation of IT systems after a threat or disaster has occurred. The organisation further needs to develop and continue engagement in the implementation of as ISCP that will ensure the organisation recovers and resumes its normal operations and critical processes after a threat. Figure 3 summarises the key elements for examining internal factors associated with the process of managing risk in an organisation and will be used as a guide to examine the phenomenon of disaster management in this study.

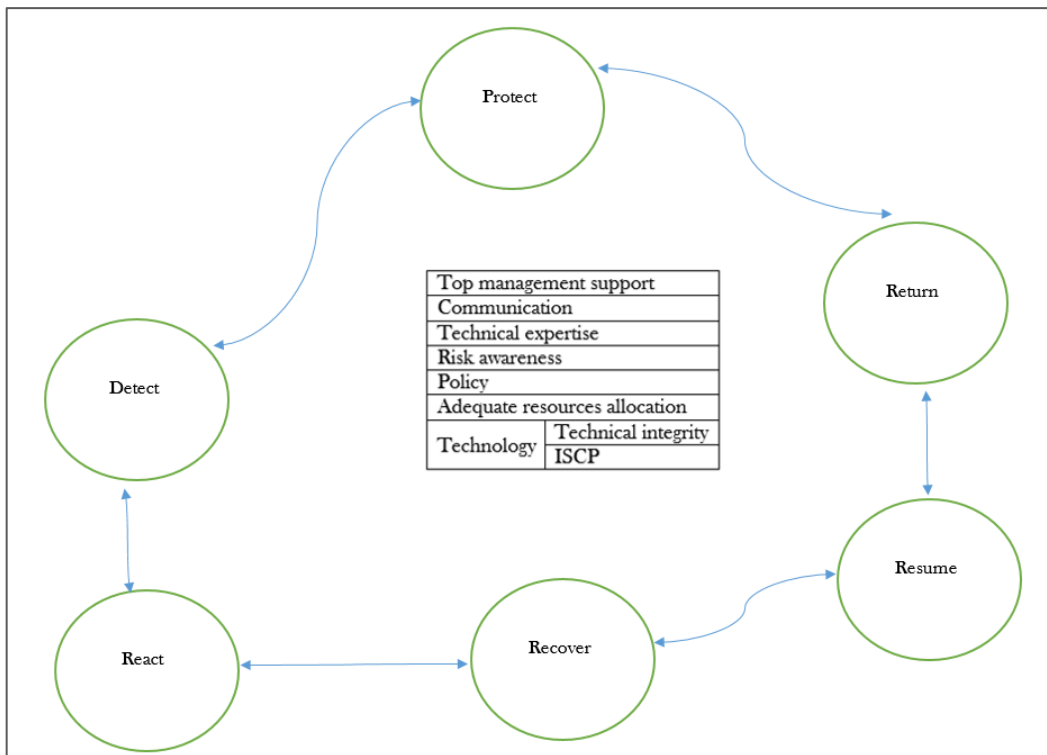


Figure 2.3: Conceptual model of risk management factors

According to the model, an organisation needs to pay attention to risk factors whilst simultaneously engaging in the cycle of risk management. Failing to engage in a risk management process is in itself a risk factor. Given that organisations are affected by contextual factors, within each phase of the risk management process the organisation should be cognisant of the need to readdress risk factors that could have changed due to a volatile environment. For example, in the protect phase the organisation does not only provide measures for protecting the IT systems from potential threats, such as providing IT security controls, but also examines other risk factors, such as resource allocation for the protection process and expertise availability for implementing and maintaining protection measures.

The above model relates to the incubation stage from Turner's model (1976) where information difficulty is a critical element. This is a stage where certain events go unnoticed and misunderstood by management and employees of an organisation because of incorrect assumptions and difficulties in handling information in a complex situation.

3. RESEARCH METHODOLOGY

3.1 Introduction

This chapter illustrates how the researcher carried out the study. It details the techniques for collecting, measuring and analysing data when conducting research (Creswell & Clark, 2007). The aim of this chapter is to discuss the methodology adopted for the study. It comprises the philosophy and approach, data collection, sample, data analysis, limitation, timeline and summary, and each will be briefly discussed.

3.2 Philosophy and Approach

This study is deductive in nature and follows an interpretive approach. An interpretive approach is based on the assumption of the state of flux of an experience and has an inherent logic that requires the social scientist to grasp the ‘subjective meaning’ of action (Partington, 2002; Bryman & Bell, 2007). With subjective meaning, it is recommended that every individual build his or her own existence. Usually, interpretivism relates to experience and focuses on the way people make sense of the world (Easterby-Smith, Thorpe & Jackson, 2008). Interpretive researchers attempt to understand phenomena through accessing the meanings that participants assign to them. According to this research philosophy, data is people’s constructions of others’ edifices regarding the ways in which their compatriots behave and the reasons for their actions (Easterby-Smith et al., 2008).

The rationale for choosing this research philosophy is that there are few studies that pay attention to industrial development organisations. The majority of studies have not set a focus on the IDZ sector; they set their focus on private companies, thus resulting in limited literature being available on mitigation strategies for IDZs. Although a number of studies have been conducted on mitigation strategies, such as the information systems continuity plan, not much attention has been given to factors that affect the continuous function of the organisation in terms of mitigation strategies. Therefore, an interpretive approach will allow the researcher to interact with experienced participants who will be able to detail their work or expertise in risk mitigation. The researcher will be able to gather rich in-depth information from various opinions through interacting, and assessing body language and observation. Information gathered will be tied back to the literature and will validate

meanings. Another reason for adopting an interpretive approach is the researcher’s assumption about reality that people’s experiences are different. The people involved in the researched phenomena can construct reality. The study takes an interpretive stance as it aims to explore the negative continuous function of IDZs in depth, which can be expressed through social constructs, such as language, consciousness and shared meaning (Creswell, 1994; Myers, 2009).

3.3 Strategy

Saunders, Lewis and Thornhill (2000) describe a research strategy as a general method that a researcher employs to answer the research question. Research strategies are classified by Easterby-Smith et al. (2008) into the following categories: case study, action research and survey research. Action research is a strategy that allows a researcher to collaborate with practitioners and therefore requires the researcher to be part of the organisation in which the research is being conducted (Easterby-Smith et al, 2008; Saunders et al., 2000). Survey research strategy is more positivistic because it helps researchers collect large volumes of data from sizable samples and to generalise the findings (Hair, Babin, Money & Samouel, 2003).

For the purpose of this research, a case study approach was selected. A case study is a method that seeks to describe a particular case in detail and develop a theory from that approach (Saunders et al., 2000). A case study strategy offers the researcher the opportunity to capture the richness of in-depth information, since it enables collecting various opinions and attitudes, which assist the researcher to achieve research objectives. It also provides an opportunity for the researcher to examine how a difficult set of situations comes together to produce a particular manifestation. Table 3 summarises the advantages of using a case study as a research strategy.

Table 3.1: The advantages of using a case study

Advantage	Reference
Ability to apply a single case or multiple cases for better generalisation of results.	Yin (1994)
The ability to learn more about poorly understood situations.	Bryman (2004)
The opportunity for extensive analysis of many specific details in comparison with other research methods.	Kumar (1996)
Supports the use of existing theories and provides opportunities for generating new theories.	Willig (2001)

Adopting a case study approach renders this research of possible benefit because it has the potential to capture in-depth richness of information and augment the present dearth and general unavailability of information about risk mitigation issues in South Africa. South African IDZ organisations rely on statistics from other countries, which reveal and record causes of disaster in these countries (Karkoszka, 2014). In developed countries, such as Europe and the USA, and developing countries, including other African countries, conditions are different from South African IDZs. South African IDZs have less stable infrastructure and fewer skills available to ensure system stability and continuity. The problem facing South African IDZ research is the relative unavailability of reliable studies and sources (Stride, 2007). This could be due to the lack of a regulatory body and a single source of reliable and unbiased information. Thus, adopting a case study has the potential to add a level of information visibility, which could prove valuable to researchers and guide future research.

3.4 Research Design

Ghuri and Gronhaug (2005) classify research designs into three categories: descriptive, exploratory and causal. Cooper and Schindler (2006) claim that exploratory research is suitable when the area of research is not clear – a new field – or if it is not clearly identified. The purpose of an exploratory research design is for the researcher(s) to learn something new about the phenomenon and this occurs when a researcher has observed something or has an idea or hypothesis/theory and seeks to understand it more. Cooper et al. (2006) argue that the purpose of an exploratory research design is to determine if what is being observed might be explained by an existing theory. Therefore, based on the aforementioned background and due to the relatively small scope of available literature on mitigation strategy, such as that dealing with ISC in IDZ organisations, the researcher is able to observe and capture data in an area where ideas are not clearly defined or identified in literature and thus make this research exploratory.

3.5 Data Collection

Data collection is a process through which a researcher collects information needed to answer the research question or problem (Saunders et al., 2000). This research employs a qualitative data collection approach because the researcher seeks direct interaction with participants on a one-to-one

basis. The benefit of the qualitative approach for the research is that the information gathered is rich and has deeper insight into the phenomenon under study (Saunders et al., 2000).

3.5.1 Sample

Easterby-Smith et al. (2008) describe how research in social sciences involves determining the research population and sample. A population is any group that shares common traits and the sample is a subset of the population from which evidence is obtained (Black, 1999). The primary targeted sample for this research is the IT department at IDZ Organisation X, since this department is the heart of innovation, strategy and an ISCP. However, the sample is expanded to cover all departments. As Järveläinen (2013), points out that the disaster recovery plan (DRP) and ISCP must be cross-functional as ideas of personnel across different departments need to be included. The researcher believes that these ideas have the potential to enhance the validation of the research. The IT department’s population comprises ten (10) participants as follows: a chief information officer (CIO), IT managers, IT project managers, a solution architect, an ICT system administrator, a business process analyst (BPA), a business analyst (BA), a developer, and two Oracle support team members. In addition to the targeted sample, the personnel from different departments consists of six participants as follows: two (2) executive managers (EMs), an account manager and two (2) programme directors (PDs), since they are also involved in drafting new organisational strategies. Because the IT department is small, consisting of ten people, the population consists of the entire IT department with the inclusion of five other departments as shown in Table 4.

Table 3.2: The participants selected for this research

Department	Goal
Shared services	Consolidated business operations that are used by multiple parts of the same organisation. They are cost-efficient because they centralise back office operations that are used by multiple divisions of the same company and eliminate redundancy.
Business development	Proposes business deals, pitches products or administrations to new customers and keeps up a decent working association with new contacts.
Finance	Focuses on allocation of resources and the accounting, reporting and control of income and expenditure.
Operations	In charge of the procedure of making products and administrations. It includes arranging, sorting out, planning and controlling all assets expected to create an organisation’s merchandise and administrations.
Corporate services	Exists to render a far-reaching, incorporated human asset and organisational capacity to improve administration conveyance and the welfare of all workers.

The reasons for choosing this population are as follows:

- The size of the IT department is small and likely to be of a manageable size for purposes of investigation, as recommended by Saunders et al. (2000).
- Top managers and senior IT personnel are aware of the entire integrity of their organisation and have the power to integrate an IS continuity plan effectively in their organisation (Karkoszka, 2014).
- An up-to-date list of all participants for the research was available, which included their contact telephone numbers and valid email addresses.
- The population as a whole has an in-depth understanding of IS/IT and the business continuity spectrum.

Table 3.3: Composition and roles of the sample populations

Department	Title	Number of years	Number of Participants	Role
ICT	CIO	12	1	Heads the IT portfolio and strategy.
	IT Manager	10	1	Ensures the business understands the IT requirements and that IT understands business needs.
	IT Project Manager	11	1	Oversees IT projects and manages them according to project management principles.
	Solution Architect	9	1	Architect for IT solutions.
	ICT System Admin	7	1	Responsible for ICT infrastructure and business support services.
	Business Analyst	8	1	Responsible for gathering information from stakeholders, developing business and data models that describe their requirements and writing specifications to provide an accurate blueprint for the designing, building and testing of proposed business solutions.
	Business Process Analyst	8	1	Has the knowledge and skills to analyse, improve, redesign and implement business processes.
	Developers	9	1	Develops the system and other related ICT and infrastructure tasks.
	Oracle Support/ Security Specialist	5 and 6	2	Serves as a support service, including helpdesk, support desk and Oracle support.
Non IT Personnel				
Corporate Services & Operations	Executive Manager	12 and 10	2	To drive the organisation through the appropriate paths.

Department	Title	Number of years	Number of Participants	Role
Business Development & Shared Services	Programme Directors	10 and 12	2	Heads of programmes around the IDZ and SEZ.
Finance	Account Manager/ CFO	12	1	In charge of project budgets and managing costing and expenses.

The selected organisation was established in 1999 as a government economic programme whose focus it is to raise the level of direct foreign investment in a country's economy and has started to employ new and more efficient management technological tools and processes, such as e-commerce and e-business. However, the growth in technology, especially a reliance on IT, has exposed them to threats. In this context, efforts to discover and improve the ways in which technological risk can be detected and mitigated became of paramount important

3.5.2 Data-collection techniques

According to Saunders, Lewis and Thornhill (2000), data can be collected from primary and secondary sources. Primary data is first-hand information obtained from questionnaires, focus groups, interviews, and direct observation. Secondary data includes data from existing sources, such as archives, documentary data, annual reports, publications, newspapers and internet surveys (Saunders et al., 2009). Saunders et al. (2009) recommend using both primary and secondary sources in the same study, arguing that this combination can enhance the validation of data and increase accuracy. On these grounds, this study adopts the use of both primary and secondary sources. The secondary data emanates from the organisational annual report obtained from the organisational communication head. Primary data was obtained from semi-structured interviews conducted with different participants across the departments: shared services, business development, finance, operations and corporate services, and from the IT unit.

Semi-structured interviews allow participants to talk about the phenomena without interruption. They allow a participant to raise issues or important points a researcher might not have considered. These points have the potential to lead to new insights and rich, detailed information, or the capturing of 'thick' data. Bearing in mind the relatively small size of the sample, time was not a constraint, which is another reason for choosing an open-ended question interview format. In addition, open-ended questions are more suitable for exploratory research where the researcher is not aware of, or able to

predict, alternative answers (Hair et al., 2003). A review of literature dealing with risk mitigation strategies and information systems continuity provided the researcher with the idea of developing alternatives to the answers that support the use of open-ended questions. Thereafter, the researcher can emphasise specific questions to clarify issues raised. The information from the interviews has been analysed, contrasted and compared with that provided in literature. Knight (2002) claims that semi-structured interviews form the halfway base between structured and more subjective unstructured interviews. This study adopts semi-structured interviews in person because respondents were easily reached, being based in the same location as the researcher and also for the purpose of observing the body language of respondents. Moreover, semi-structured interviews allow respondents to express their opinions and possibly bring up subjects and areas for exploration of which the researcher might not have been aware. The researcher set out to build rapport with each respondent and interviews were informal and conversational.

Meyer and Newman (2007) point out issues that might emerge during interviews, such as the biased nature of information from key informants, lack of trust, new entry to the organisation, time pressure on respondents and possible inconsistency of data collected due to the interviewer being inexperienced. To compensate for such issues, the following procedures are used:

- Interview guidelines to ensure that questions lead to detailed, rather than yes/no, responses.
- Proper planning, so that respondents may be willing to provide and offer thorough and detailed information.
- Communicating openly, accurately and transparently to build trust.

For confidentiality purposes, the organisation is not mentioned by name and is referred to as IDZ_X. The researcher signed a non-disclosure agreement that was approved by IDZ_X. Interviewees are identified by a code (Par) throughout the entire study in order to respect their anonymity.

3.5.3 The development of the research instrument

To understand what underlying technological risk factor and associated risk mitigation strategies were, a research instrument (Appendix A) was conducted to a portion of the sample population, as described in Table 3.3. Each of the questions in the research instrument was designed to provide

insight into the research question. The questions could also be mapped to Organization, Human and Technological factors.

3.5.4 Pre-testing of research instrument

Conducting pilots enable researchers to identify problems and refine the data collection strategies, and further assist in the development of instruments so that right questions are asked to yield relevant results from the respondents (Yin, 1994). The research instrument for this study was pre-tested during the pilot study involving seven participants to ensure that data would yield relevant results to achieve the research objectives. The results were recorded and analyzed. At the end of the pilot, necessary changes were made to the instrument.

3.6 Data Analysis

Data analysis is an approach that involves a rigorous and logical process to establish meaning from data (Gray, 2009). Myers (2009) suggests various methods of data analysis that can be applied to qualitative studies, such as discourse analysis, grounded theory, thematic analysis, narrative analysis and phenomenology. Data in qualitative analysis, according to Dey (1993), is fragmented into small units to establish the characteristics of each unit, and through this process connection are made between concepts and new meaning is generated. A total of ten IT personnel interviews were conducted with the inclusion of five top managers from shared services, business development, finance, operations and corporate services units.

3.6.1 Thematic analysis

Transcription

Interviews were recorded via audio recording and transcription followed. Transcribed recordings were stored in Microsoft Word to enable the data to be easily recalled, read and understood. After the data had been transcribed, the researcher began to familiarise himself with the content of the data through the process of reading and reading the data.

Generating initial code

According to Braun and Clarke (2006), this process is a cyclical process whereby codes emerge throughout the research process. The researcher went back and forth between data sets to identify codes that in most cases repeatedly expressed the same incident, which were then grouped as a theme. For example, when phrases like, *“there is a risk mitigation strategy in the organisation, but I am not aware of it”* and *“I have not seen it. For me as a manager, I see it as a risk and I can’t remember if there was anything circulated”* were analysed, it was noted that these statements were defining the same thing – a lack of involvement, information not being shared and lack of communication. These themes were grouped as a lack of information circulation. These themes are derived from a risk mitigation strategy pattern in the context of IDZ conversational topics from the interviews conducted. For example, the identified theme of lack of information circulation enabled the researcher to describe that IT unit staff lack the commitment to share the importance of a continuity plan. This also relates to the lack of knowledge of a continuity plan and lack of involving personnel from other departments in adopting a risk mitigation plan.

Searching for themes

According to Braun et al. (2006), this phase is significant for a researcher to begin examining how codes combine to form a theme in the data. At this stage, the researcher looked at the list of themes and began to focus on the pattern in the data. For example, themes like backup plan, security policy, revised policy, security procedures and risk awareness were on the list. The researcher considered the relationships between these themes. Themes consist of ideas within a culture that can be used to explain causal event (Braun et al., 2006). The researcher then narrowed down these themes to provide an overarching theme. Thematic analysis allows for themes to emerge from repeating ideas, metaphors, similarities and differences of participants’ linguistic expressions (Braun et al., 2006). The researcher examined repeated ideas and similarities from themes. For example, codes such as Backup plan, security policy, revise policy, security procedures and risk awareness, were examined to produce the theme ‘revise security policy’.

Reviewing themes

In this stage the researcher reworked potential themes and some were merged into each other. For example, themes like communicate the plan and share information were combined to become ‘communication’. Some of the themes like mobile solution were reworked as ‘mobility as a solution’. The researcher re-read the data set to check whether themes related to that data set. Themes were found to be coherent and related to the data set. The researcher repeated the process with each theme to check if they mapped back to the data set and all themes were found to be coherent. Table 3.4 depicts the emerging themes.

Table 3.4: Emerging key themes

Theme	Subthemes
Human	<ul style="list-style-type: none"> • Disaster experience • Awareness
Organisational	<ul style="list-style-type: none"> • Information difficulty and communication • Documentation
	<ul style="list-style-type: none"> • Mitigation strategy solution • Mobility solution • Revise security policies • On-going continuous security check
	<ul style="list-style-type: none"> • Mitigation strategy challenges • Top management support • Lack of expertise
Technological	Technological disaster

4. FINDINGS AND DISCUSSION

4.1 Introduction

The preceding chapter discussed the methodology used to execute the study. The purpose of this chapter is to present the findings. The rest of this chapter is organised as follows: the demographic findings are discussed, followed by the emergent themes from the analysis. The chapter concludes with a discussion of the findings.

4.2 Demographics

The study was conducted at one organisation and fifteen respondents participated from the organisation. The findings are tabulated in Table 4.1. According to the findings, ten participants are from the IT department, two from corporate services, one from business development, one from shared services, and one from finance. Corporate Services & Operations is a department that deals with activities that combine or consolidate enterprise support services, and provides specialised knowledge, best practises and technology to serve internal and external clients and business partners. The business development department proposes new deals. Shared services is a department that consolidates business operations that are used by multiple parts of the same organisation. Respondents who are not from the IT department are mostly in executive positions. These include the executive manager of Corporate Services & Operations, programme director of Business Development, and an account manager who is acting chief financial officer (CFO). The participants were chosen based on their depth of understanding of mitigation strategies, as well as their working experience at the organisation.

According to Table 4.1, one respondent has a working experience of between 0 and 5 years, seven have between 6 and 9, and seven have between 10 and 12 years of experience. The majority (8) of the respondents are between the ages of 46 and 55. Six (6) are between the ages of 36 and 45, and one (1) is between the ages of 25 and 35.

Table 4.1: Respondents profile

Respondent Alias	Title	Department	Age	Experience	Education	
Respondent 1	Executive manager	Corporate services & Operations	55	12	MBA, LLM	
Respondent 2	Executives manager	Corporate services & Operations	50	10	MBA, MCOM	
Respondent 3	Executive manager	Business development	47	12	MBA, MSC	
Respondent 4	Programme director/ Executive manager	Shared services	49	10	MBA, MSC	
Respondent 5	CFO/Finance Execute Manager	Finance	55	12	MCOM, MBA, CA	
Respondent 6	CIO	ICT	54	12	MPhil, MCOM, MSC	
Respondent 7	Solution Architect		46	9	MCOM, COBIT	
Respondent 8	System Admin		37	7	BSC, N+, A+, CCNA	
Respondent 9	Project Manager		47	9	BCOM	
Respondent 10	IT Manager		37	10	Project management certificate	
Respondent 11	Developer		40	9	IT diploma, IT certificate	
Respondent 12	Business Analyst		37	8	BCOM, CPAB	
Respondent 13	Business Process Analyst		38	8	BCOM	
Respondent 14	Oracle support		26	5	CCNA, A+, N+, IT certificate	
Respondent 15	Security specialist		40	6	BCOM, Diploma	

The findings on the respondents' qualifications show that three possess a certificate or certification, five possess a degree or diploma, and seven possess a master's degree or a Master of Business Administration (MBA). It is significant to note that education level is important to the study as it affects the attitudes of individuals and the way they understand a particular concept, their in-depth knowledge of a particular phenomenon under study and their provision of further relevant knowledge during the interview.

4.3 Technological Disaster

The findings show that the majority of respondents had not experienced a technological disaster at their work place. Most were aware of regular tests, although were not sure about the server and system

tests due to lack of experience. Respondent 15 from the IT department admitted to being unaware of regular testing of systems by the server:

“I can’t answer that ... I think they do test on a regular basis, but I don’t know time intervals ... No I don’t know ... I don’t know really, but I think Oracle, it’s monthly or quarterly, but am not sure. But there are policies and [a] service level agreement (SLA) with an ideal but again am not sure.”

Having an employee from the IT department being unaware of the kind of technical integrity systems are subject to is worrying and shows the culture of disaster readiness and awareness possessed by the organisation. According to some respondents, this lack of awareness was perpetuated by IT management because the lower the level of experience of an individual, the less management perceived them to be adding to the organisation’s IT system. Respondent 14 confirms:

“I have no knowledge of that, and thus experience is one of the factors that IT management seems to side line us. I believe that in order to create a culture of preparedness, everyone in the organisation must kept on the loop about system/server testing.”

This is consistent with findings by Lewis et al., (2017) that the necessary support, for example regarding to system and server testing, is not always provided by the business and some employees remain uninformed. According to a respondent from the IT unit, organisations perceive the role of server and system testing as being suited to only certain individuals with technical skills, as Respondent 12 explains:

“... The organisational perception is that the role of server and system testing is the responsibility of specific IT individuals, because they perceive everyone as not technically inclined.”

Respondent 9 made similar remarks:

“... As a result of this we can ignore warning signs and alarms because we are not involved in testing and therefore we don’t know if anything goes wrong or not. I personally would like to be involved and be groomed in order to be technically aware.”

These consistent remarks are alarming because, according to Hausmann et al., (2015), even though server/system testing is the responsibility of the IT unit, everybody in the organisation should be made aware of testing and procedure. Hausmann et al., (2015) cautions to examine the role of self-perception in technological disaster as the perception a department may have in terms of its

contribution to testing, i.e. other departments may perceive themselves not to be technically inclined; therefore they do not participate in system/server testing.

Few were aware of the testing procedures. For example, Respondent 6 indicates that in his capacity and his knowledge as a CIO the system and server test involves IT resources, the service provider and business users.

“... Testing is conducted from the Disaster Recovery server room at our head offices. It involves IT resources, such as testing staff and specialist, ten desktop PCs from which testing is conducted and those PCs are built to accommodate all user profiles within the organisation, and of course our service provider. Bear in mind that testing is conducted bi-annually and all data from the testing result are stored on tapes as a backup regiment.”

Respondent 8 shared a similar remark to Respondent 6 by expressing his knowledge as testing staff:

“... As part of the testing team, we conduct all tests at our dedicated sever room at the head office. The testing runs for a full week, twice a year from Friday afternoon at 17:00 till the next Friday morning at 05:00. Backup of all data is done on tapes after the test and they are kept in the server room.”

The detect principle was seen as a significant strategy to be used as a monitoring and alert tool in order to detect capacity deficiencies, such as running out of memory or storage, as Respondent 6 indicates:

“We have a monitoring and alert strategy to detect all our system, server and backup storage. For example, every month we do a system/server check-up to minimise the impact of disruption due to limited storage. By so doing we are able to detect the capacity our server/systems have to store a backup of all our data.”

4.4 Human Factor

Two factors were identified as important for addressing disaster and mitigation planning in the organisation: disaster experience and awareness.

4.4.1 Disaster experience

The findings show that the majority of the respondents had not experienced a significant disaster in their working environment. However, most were very vocal about the recent shut down of the server in the organisation. For example Respondent 1 indicated that recently:

“I did experience a disaster, and it did affect my job where I had lost everything on my laptop including my work. I have also experienced a cyber-crime in the past and all the company information that was on my PC was lost. I was frustrated because I was fearful of investors and clients that they might find out that information were lost because the information that was lost contained a year-end financials, product pricing and financial monthly report.”

Respondent 5 reiterates:

“I personally cannot state I have experienced a disaster at work but the Monday disaster was a problem ... the server had to shut down and systems went down for the whole week and we couldn't work. Our suppliers were frustrated with the situation because they were not able to do invoicing, and on their side as well it causes a delay.”

There was a consistent understanding that a disaster was not a common incident at the organisation and therefore most had not experienced it. This is perceived as a problem because, according to Respondent 12, this could lead to employees not being ready when a disaster happens and “most like me have a low level of fear for a disaster”. The findings were consistent with Jones et al. (2015) who notes that it is not until a disaster or a terrible loss occurs that people realise the need for disaster preparedness. The absence of the experience of a disaster results in a low level of fear of a disaster and adversely impacts the practices of effective continuity efforts. Consistent remarks of self-awareness reflected a relationship between experiencing a disaster and developing an understanding of vulnerabilities. As Respondent 3 shares:

“Establishing a relationship between experience of a disaster and attitude will provide staff with a disposal towards a disaster and self-awareness. This implies that should there be a disaster, we will know what to do. We will be fully prepared and this will create a culture of preparedness.”

The proposed recommendations were not currently practised at the organisation and none of the respondents could categorically describe how they would address a disaster and what mitigation plans

they have in place. The lack of employee's preparedness, familiarity and exposure is what Jones (2015) and Lewis et al. (2017) attribute to the causation of a disaster.

4.4.2 Disaster awareness

The need for regular awareness was perceived to be important for an environment characterised as not being fearful of a disaster. According to most respondents, regular risk awareness raised possible disaster awareness, which can then lead to a continuous risk mitigation strategy. According to Respondent 13, this needs to be explicitly communicated, because:

“Some of us still have that comfort that it's [a disaster's] not going to happen to us. Based on our experience, we think we safe until something happens. Therefore risk awareness is significant to create preparedness.”

Respondent 3 supports the need for regular organisational awareness at all levels and suggests “every two weeks or a month there should be awareness programs and put them [the programs] on the intranet, to increase level of preparedness”. In this way, according to Respondent 15, the organisation will be “raising awareness of the risk of a potential occurrence and the way it should be managed, and in so doing improves the organisation's preparedness to disasters”. These findings show that employees are willing to learn, become aware of disaster situations and be prepared when an incident occurs. According to Ozkazanc & Yuksela, 2015, employees are eager to learn more about policies on disaster awareness and preparedness and are seeking to increase their knowledge in this domain and enhance their skills on preparedness. These programs can act as a catalyst to improve (i) employee morale because low morale can reduce effectiveness, safety, or system performance (Hollnagel, 2014); (ii) and simultaneously change behaviour as a result of experience (Hollnagel, 2014).

Respondent 1, from corporate services, postulates that strong awareness can be achieved by training all employees on strategy mitigation and suggests that “training programs target at improving awareness and motivate us employees by providing us an opportunity to work in groups through scenarios in order to face future challenges”. There was a common understanding from other respondents that awareness should not only be about disaster preparedness in the organisation, but, according to Respondent 4, it should be an on-going “education and training program that intends to cultivate awareness of mitigation procedures to all employees in the organisation”. Although most respondents admitted not being aware of training programs in the organisation, they regarded such

programs as enablers for employees to be disaster conscious and to be risk aware and prepared. Training programs help to reduce resistance by providing all employees with an opportunity to think critically of future challenges. These findings are consistent with Kumar et al. (2017) who believe that if considerable effort and expenditure on education, training programs and level of preparedness remains high, it will encourage awareness in an organisation because these programs provide all employees with an opportunity to think in-depth about future disasters.

4.5 Organisational Factors

4.5.1 Mitigation strategy solutions

Three mitigation strategies were proposed: the need for mobility, the revision of security policies and on-going continuous security checks.

a) Mobility as a solution

Several respondents highlighted the need to be mobile as a means of addressing a disaster scenario and as one potential mitigation plan. Respondent 1 explains:

“Technology nowadays progresses so fast we become more mobile, and we require a mobile solution, so if the power fails, or we denied access from the building, as we have experienced that incident, at least we have laptops, iPads and smartphones built with organisational app, so we have this mobility as a solution.”

Such a solution that allowed mobility was seen as important for the continuity of work, as Respondent 3 clarifies:

“Relating from my previous experience, we used mobility as a solution in ensuring that in a case of a disaster there is a solution in place which will allow us to continue our work in an absence of an office space. People will manage their own time, while technological developments are enabling new forms of productivity independent of office-based work.”

The solution was also vocalised by the systems specialist, as he perceived mobility as an adaptable method for conducting and planning work away from the physical building. Respondent 8 explains:

“The mobile solution will provide us with the flexibility to plan, conduct work and share important files while we [are] away from the physical building. This increase flexibility and agility. Technology is creating an opportunity for a new form of collaboration, changing not only where we work from, but how we work.”

This was reiterated by Respondent 9:

“Accessing your work while you at home or any space office, serves us as a solution since picketing is something we experiencing every now and then. The mobile solution platform offers the advanced knowledge sharing capabilities that transcend business activities. This is a flexible method to be reflected in the physical infrastructure of work, where it is no longer necessary for a dynamic teams to be co-located.”

Continuous research on new mobility solutions was also pointed out as significant for organisations as, despite the fact that a solution might currently exist, it is critical to continue researching new advancements so the organisation can remain ahead of technological changes and abreast of innovations. As Respondent 11 states:

“Once we adopt mobility as a solution, we need to continue with the research on new mobility so as to keep up to date to merge with the new technology changes and threats. New technology platforms support a broader challenge to traditional organisational structure and enable a network-oriented approach.”

Consistent with Respondent 11, another respondent from IT (Respondent 2) recalls his experience that:

“We operate in an unstable technological environment, in this way to proceed with investigating new application that are good with the versatility will give us the capacity to remain ahead to threats.”

Respondent 15, using his knowledge as a specialist and as a disaster recovery member, explains that there are recovery activities that are performed in a controlled manner to bring the business processes and systems back to a point of operation after a disaster:

“We have recovery activities, such as a temporal housing of data, reconstruction and repair of any damaged to our infrastructure, review [of] a document of lessons learned and operational life support

system. This continues until all systems return to normal. We measure both long and short term strategy.”

Consistent with Respondent 15, another respondent from IT (Respondent 6) recalls that:

“Our risk mitigation strategy is a tested plan and is designed in such a way that it caters [to] a wide range of disaster activities. For example, if any crisis occurs our recovery team consults the documented recovery plan, which consists of lessons learn, mitigated disasters and risks encountered from past experience.”

Respondents were able to recognise the significance of mobility as a solution, as it will allow them to plan and conduct work away from the physical environment. They also recognise the need to continue with research on new technologies once the mobility has been implemented. As a result, the growing pressures of working life cause more people to manage their own time, while technological developments enable new forms of productivity independent of office-based work. Similar reasoning is provided by Lewis et al. (2017) that essential tools, such as mobile devices and applications for conducting work away from the workplace, are important as they make it easy to respond to work functions and allow employees to plan and perform their day-to-day business activities away from the physical workplace, as well as in the case of infrastructure failure (Dangare et al., 2015). The findings of this study recall those of Vernim and Reinhart (2016), as they emphasise the importance of organisations providing the necessary flexible services to clients and being able to continue working in any given space.

b) Revision of security policy

There was a concern from most respondents that the security policies of the organisation were not regularly updated and could consequently not be relevant for the current technological environment. As Respondent 3 indicates:

“Yes I am aware of the security policy. For example, once or twice a year ICT needs to remind us, as they never did because a technological disaster five years ago will not be the same as this year; we are moving in terms of technology.”

Respondent 6 recalls his experience:

“... According to my personal experience from my past employment is that security policies should be revised each year, in order to align the organisation with any form of protection it may require. Remember, as technology advances it creates more opportunity for new threats. Therefore, keeping continuous security policies is vital to stay ahead from threats.”

Similar remarks are made by Respondent 8:

“From all companies I worked for, I realised that revising security policy is the key, because it provides a blueprint that can be followed by everyone. And therefore will allow organisation to minimise risk and continuously stay ahead of new threats.”

Another experienced respondent from shared services recalls his experience by indicating that even though security policy is the responsibility of the IT unit it should be organisation oriented. Respondent 4 explains:

“Judging from my experience, security policy is the IT unit’s responsibility. However, I think security policy should be placed at the centre of a company’s objectives and encourage more strategic thoughts amongst its practitioners.”

These findings highlight the importance of examining the practice of security policies in relation to the organisation as a whole so as to help organisations to minimise risks and allow them to respond quickly to a disaster (Hollnagel, 2014). There was a concern from a systems specialist respondent from the IT unit that the organisation should also focus on the development of re-insurance security policies and the collaboration between various IDZ organisations as part of their practice of revised security policies. As Respondent 13 states:

“From my knowledge, there is a risk and security policy that aims to reduce risk by transferring it to other organisations, known as re-insurance companies. This procedure is documented as part of mitigation strategy good practice including activities, such as collaborating with other IDZ companies in order to share financial burden.”

Respondents from this theme were able to reflect on their working experience. They vocalised that security policies need to be regularly revised in order to meet new technological challenges. They also recognise the need to utilise the company intranet as a form of security awareness, i.e. once or twice a year the organisation needs to remind employees about security policies because they operate in a changing technological environment. Jones (2015) suggests training and campaigns as the best

means of creating awareness and increasing understanding about security policies. This must be organisation oriented and placed at the centre of company objectives.

c) On-going continuous security checks

Most respondents identified the need to have continuous security checks. For example, Respondent 2 notes: “regular system performance checks are important to eliminate any unforeseen situation.” Another respondent indicates: “a tested plan should be actioned regularly” (Respondent 3). Furthermore, “Once a month or quarterly we need to have a drill or simulation where there would be a false alarm about the disaster. In that way we will be able to improve our disaster experience, once it happens we will be able to identify if it’s a minimum or major disaster and we will know what to do.” (Respondent 10). According to Ahlan et al. (2015), conducting drills and simulations is the most effective way to evaluate and test disaster preparedness and instil a sense of confidence.

Another experienced respondent from IT recalls his knowledge of the organisational planning for vacating the building when disaster occurs by indicating the alternative building with full of organisational equipment. Respondent 9 explains:

“We are planning on having the alternative work station about 20 km away from our head offices. It is going to be built with full working station equipment, such as PCs, printers, telephones, office tables and chairs. This plan will allow us to continue with business as usual at our alternative workstation. While on the other hand we are fixing any damages caused during the crises.”

The proposed recommendations were not currently practised at the organisation and none of the respondents could categorically describe how to address a disaster and what mitigation plans they currently have in place.

4.5.2 Documentation

All respondents reported a lack of documentation of important information and events. For example, Respondent 6 saw the lack of documentation as a continuous problem during disaster occurrence:

“Lack of documenting the type of disasters that we have experienced and their solutions seems a continuous issue. It is very significant to document what caused a previous disaster, how they were mitigated and what fixes were implemented.”

Respondent 9 restates:

“We do not learn from our previous mistakes, consistently we encounter a disaster, for example, cyber-crime and infrastructure related issues; however, no documentation is set up. It implies that issues that we have encountered have been overlooked.”

Although most respondents report the lack of documentation as a challenge, those from the IT department were more vocal. For example, Respondent 9 noted that employees perceived documentation as a trivial task and therefore it was not given importance. As Respondent 9 explains:

“People verbally legitimise why the documentation is basic, yet nothing concrete is done. For example people keep on talking about documentation but there always seem to be an excuse on why it is not happening. This seems to be an aspect of an organisation and not only a problem in disaster mitigation ... it seems like people they talk without acting on their words. This is a big organisation to have such kind of employees who do not think beyond safety.”

Respondent 10 agrees that the lack of documentation is a problem for the organisation and, after reflecting on past experience, noted that this is the only organisation they have worked for that lacks disaster and mitigation documentation. They explain:

“According to my vast experience, 35 years on the job, I understand that registry as part of documentation should exist which lists all the disaster experienced and their solutions. It should be easily accessible to everyone in the organisation and must kept updated on a regular basis, because we [are] operating in a technological environment.”

Respondent 2 shares similar remarks:

“All problems should be listed and if the problems and solutions are in the central place, it is easy for a lookup by all employees, so that when the similar crises occur I know where to look up for a solution.”

The implication is that the organisation should hold employees accountable for the documentation of their respective functionalities, and ensure organisational access to this documentation. Kumar, Zaveri and Choski (2017) note that this is crucial in any organisation because providing information on a disaster and how it can be mitigated will encourage awareness and preparedness. It will also help with retaining institutional memory because in any organisation people will come and go, business processes will change, technology will improve and change, equipment will be replaced, and all these changes will cause risk to transform and migrate (Järveläinen, 2013).

With regards to accountability, Respondent 8 called for dedicated personnel who would handle the documentation of disaster and mitigation concerns in the organisation:

“Nobody is looking at problems experienced, and nobody seems to take the accountability to document the issues and rectifications, i.e. we need an accountable person whose responsibilities are to look after all disasters experienced and make sure that they are addressed and documented.”

The findings show consistent remarks from all respondents that there is a lack of documentation of important information, such as experienced disasters and fixes. It is very important to document such information because employees come and go and, therefore, if experienced employees leave the organisation without any documentation in place, this will cause a time delay on critical business processes and fixes because the new employees may not have the capacity to solve issues on time. On the other hand, some experienced employees vocalised that this document must be saved and stored on a central repository for quick reference and accessibility by all employees and must be kept up to date at all times. These findings echo Kulba et al. (2017), who suggest that an IT unit should have written procedures for how issues are resolved and what issues are encountered and regular IT system maintenance procedures. In so doing, the IT unit sets a precedent for being accountable and addressing the documentation challenge.

4.5.3 Information difficulties and communication

This theme refers to the distribution or exchange of information across the entire organisation. The findings show that the information being communicated is not comprehensive enough and not all employees are provided with this information. For example, Respondent 10 indicates that most employees have been not given information on how to handle a disaster occurrence:

“Even though some and very few are aware on what to do, I don’t think that all of us are aware of what we need to do in the case of a disaster, and most of us will not know what to do or which step to take.”

Respondent 5, who is a CFO and an organisational risk committee member, agrees:

“Sometimes information is communicated between certain individuals and it’s a continuous problem because some of them do not understand the importance of mitigation plan. This translates the lack of awareness for specific individuals.”

The findings show that lack of communication and knowledge sharing was a common problem in the organisation. These findings are similar to those of Ahmad et al. (2012) who note that sometimes necessary information about a security procedure is circulated to irrelevant people, small numbers of individuals or discrete groups who do not utilise the information simply because they do not understand the content or fail to see its importance. Further, these findings on the lack of communication and information sharing have been established as a common organisational challenge, as noted by Hausmann et al. (2015). For example, according to Järveläinen (2013), in many public organisations the mitigation plan is present but not circulated across departments and individuals and some relevant personnel are not included during the development of the risk mitigation plan. In this study, this problem was mainly vocalised by respondents who were not from the IT department, such as Respondent 5:

“Knowledge is not shared in this organisation. You will only find out about something when it is no longer important or in use. This is really frustrating and affects my work performance.”

Respondent 3 agrees and indicates that in their capacity as a manager, having information communicated to them at all times is crucial for planning and continuity:

“I think as a manager, I should know so that within that IS continuity plan I should become a risk owner of some part of element on it, to understand so that the environment that I am managing, including the assets that are in my disposal, I am able to respond within the provision of that continuity plan.”

The above feelings expressed by Respondent 3 were consistent amongst all managers as they saw a mitigation plan as important to the organisation and requiring all stakeholders to be involved in its planning. As Respondent 12 indicates:

“Being involved in the process of the mitigation plan is important and then communicate the mitigation plan; if the plan is for the organisation, then it should be communicated throughout the organisation. Mitigation strategy is organisational and therefore everyone should be included on the communication”.

Similar remarks were made by Respondent 1:

“Mitigation plan requires effective communication across departments in order to ensure that requirements of mitigation strategy are translated to real actions and remains relevant with changing business environment and business activities.”

Continuous assessment of the mitigation plan was also highlighted as important for the continuity of the organisation, as Respondent 15 states:

“A mitigation plan should then be tested to see if it would be able to work. Furthermore, risk committee will be able to foresee disasters that might occur, then after the risk committee see if the mitigation plan is executable, then they should communicate and circulate it to the rest of the organisation.”

Reevaluation of the mitigation plan is an important aspect of safeguarding the organisation because, according to Kulba et al. (2017), the plan should be tested and translated to real world actions to ensure that it speaks to a relevant business environment and is communicated throughout the entire organisation. In this way, when danger occurs everyone will know what to do. Respondent 6 indicates in their capacity and knowledge as a CIO there is a predefined procedure in the organisation to communicate alerts to relevant parties for them to fix a threat:

“When there is an incidence in our company, our recovery team communicates the crises by alerting appropriate personnel within each unit in order for them to fix any crises or threats. These personnel are part of recovery committee and they have a know-how of a situation. By so doing we are able to minimise incidence in a controlled manner.”

Respondents indicate that minimal information being distributed and information being kept between specific individuals is a challenge to employees, specifically those who are not in the ICT. They felt that information should be shared across the entire organisation because each employee becomes a

risk owner of some element. Therefore, in any occurrence they are able to respond within the provision of continuity plan. Mitigation strategy requires effective communication, therefore it needs to be tested and circulated to the rest of the organisation.

4.5.4 Mitigation strategy challenges

The findings show that there are two challenges faced namely top management support and lack of lack of expertise as discussed below.

a) Top management support

A successful project requires the backing of management who provides financial and other related resources for its execution. The findings of this study show that there was minimal support from top management. One consistent grievance from respondents was the lack of financial resources from top management to address the disaster and mitigation strategy. The respondents perceived financial resources as a key asset because it is associated with the need for up-to-date IT infrastructure, as Respondent 14 illustrates:

“Money is a factor because we need the financial resources to keep us up with the new technologies to protect organisational information assets. This can never be successful without the top management support. Without finance we will never keep up an innovative approach to mitigation strategy”.

Respondent 11 from the IT department reiterates this:

“We need to go to internet base, not a server base environment. Moreover, we need more human resources and physical resources, which entail us to seek more financial backup. Remember, as technology progresses, new technological challenges also progresses, therefore server base environment has more challenges than internet base environment.”

Respondent 10 associates top management’s lack of commitment to the provision of financial resources with their management style, which did not favour on-going communication and collaboration with employees. As a consequence, management and employees do not share the same vision and urgency for addressing disaster management. The findings echo those in literature that most organisations allocate relatively small portions of their budgets to mitigation strategy plans (Ahlan et al., 2015) because of the lack of top management support for a mitigation strategy and their

deliberate ignorance of the importance of IT systems and very real threats to those systems (Ahlan et al., 2015). According to Respondent 10:

“The most important step that our managers can pursue is for them to channel their effort in to understanding the need of each department, in this requires them listening to us ... a consistent collaboration between us employees and the management is important, so that we can all offer a comprehensive knowledge on mitigation strategy. We all have something to contribute to mitigation strategies because we are custodians of risk”.

The continuous lack of collaboration and support from top management was seen as problematic to the realisation of mitigation implementation strategies, as Respondent 4 warns:

“If employees and top management are cross divided, there will not be a shared vision for mitigation strategy and risk management; and the consequence will be catastrophic as you know ... I mean we could be prone to all sorts of cybercrime and stuff like that ... that is not something we want to experience in our organisation.”

This comment was consistent across the data corpus, as Respondent 5 shows:

“Senior manager support is very important to determine the success of the risk mitigation project and therefore I feel it is significant for them to give us the support by allocating enough time for trainings, finance the project and availability of human skill”.

b) Lack of expertise

There is a concern from the executive managers that the organisation lacks IT expertise, specifically when it comes to disaster recovery and mitigation strategy implementation. Although the respondents see existing IT skills as important, they believe they are insufficient to address the turbulent technological environment within which the organisation finds itself. For example, Respondent 7 shows how difficult it is to obtain employees who have know-how in the organisation:

“... Most people do not understand what to do in the case of a technological disaster ... this is a problem because we need people at all times who understand the organisation and its risks, process and technology. In this way we can say we are prepared for disaster should it occur.”

Business development executive manager that managers who are responsible with organisational resources such as human skill and finance that contributes towards mitigation strategy that they are not informing the recovery team for preparedness, as Respondent 4 states:

“When I called the employees they were astonished that they were required for [a] mitigation strategy session as no one from top managers had informed them. Some participants came with no document prepared of any kind and some had no clue about what they ought to be doing.”

Moreover, creating teams and assigning roles and responsibilities was seen as appropriate, as Respondent 10 states:

“... Top management should assign a person with the appropriate seniority and authority to be responsible for risk mitigation strategy. This person will assign individuals within each department based on their experience and the knowledge of organisational disaster to develop and maintain risk mitigation strategy.”

Similar remarks were made by Respondent 7:

“... Selected people from various business areas who understand the organisation and its risks, process and technology are required to create mitigation strategy. Mitigation strategy should be cross functional and include personnel from each department.”

This consent was also vocalised by Respondent 2, who is at the executive level:

“... Recovery teams from all departments need to be involved in providing knowledge and the understanding to guide mitigation strategy and develop the continuous improvement to keep it current.”

Having a recovery team constituted of members from each department is perceived as important. As documented by Hyväri (2016), this means having recovery coordinators within each business area who are responsible for creating and documenting risks and rectifications for their own departments and who drive risk mitigation strategy at departmental level. Järveläinen (2013) postulates that the selected recovery teams should not only be from the IT unit, but should involve people from other departments in order to ensure wide participation since overall process is risk mitigation strategy and recovery solution for business functions. Ahlan et al. (2015) argues that having small teams from

various departments with clear responsibilities , which understand their area of expertise and proper structure, is better than having a single large recovery team that holds the entire obligation.

4.6 Summary

The purpose of this chapter was to provide the qualitative findings from the study. The results show that most respondents at the organisation have not experienced a technological disaster and as a consequence few are aware of what to do in the occurrence of one. Most respondents felt the lack of awareness was due to a lack of collaboration and information sharing within the organisation, specifically amongst various departments. The IT department was perceived to have the know-how to address technological disaster but there was minimal involvement of employees from other departments in the development of a mitigation strategy and even in the distribution of information of what to do during a disaster. Collaboration and information sharing was seen as key to addressing the lack of awareness of the mitigation strategies the organisation has in place.

Respondents also noted that although mitigation strategies might be in place there is a need to include mobile solution related strategies that would allow continuous operation of the organisation and a revisit of the security policies to see if they address the current technological landscape. A continuous observation by the respondents was the lack of top management support for the implementation of these strategies because such solutions need financial support and expertise to implement them. As such, solutions were proposed and minimal management support provided. The lack of such support also negatively affects the distribution of important information to members of the organisation, making the information reach few of those requiring the information.

Table 4.2: Summary of the results

Some of the results	Comments
Documentation	There is no central registry to store documents of how problems were solved
	Lack of documentation on how problem were solved
	Don't learn from past mistakes
	All problems should be listed and documented

	There should be a lesson learned document
Awareness	No awareness on system testing
	Risk awareness is significant to create preparedness
	Strong awareness can be achieved by training all employees on strategy mitigation
	training programs target at improving awareness and motivate employees by providing them with an opportunity to work in groups through scenarios in order to face future challenges
	It should be an on-going education and training program
Responsibility	For server testing everyone perceive it as a role of IT
Monitor and alert strategy	There is a server and backup storage to detect the capacity of a server/system that have to store a backup of all data
Mobility solution	There must be a mobility as a solution so that worker can still continue working
	It allows to work in an absence of working environment
	Plan and share work in a flexible time
Security policy	Security policy must be revised once or twice a year
Alternative work station	having the alternative work station about 20 km away from our head offices
Information circulation	Information must be circulated to everyone
Shared knowledge	Knowledge must be shared throughout the organisation
Involvement	Involve everyone in the mitigation plan, then communicate it across department
Test the mitigation plan	mitigation plan should then be tested to see if it would be able to work

5 Conclusion

5.1 Background and Summary of the Study

The purpose of this study was to examine risk factors and associated mitigation strategies in public institutions of South Africa. An Industrial Development Zone (IDZ) was used as a case study within the South African context. The study had two objectives of (i) identifying risks associated with public institutions; and (ii) examining how public institutions address risk mitigation strategies. Following a qualitative enquiry approach, the study identified human, organisational and technological risk factors as those that impact mitigation strategies in public institutions of South Africa. Human factors perceived as significant to how mitigation strategies are implemented were the levels of experience, exposure and awareness that organisational members have with regards to disasters. The lack of documentation of important information, such as experienced disasters and fixes, lack of communication and knowledge sharing, lack of top management and lack of available expertise were recorded as organisational risk factors that consequently impacted mitigation strategies.

Proposed contextual solutions for these challenges included: (i) the adoption of mobile solutions and on-going research of new mobility solutions so as to keep up to date with technological advancements; (ii) the regular update of security policies of the organisation so as to align with environmental challenges; and (iii) on-going continuous security checks to evaluate and test disaster preparedness. Awareness of tools and applications used to address mitigation was seen as a key technological factor. Findings show that most organisational members, including those in the IT unit, were unaware of the security systems in place.

5.2 Contribution of the Study

Whilst most IT systems are faced with technological challenges, few studies have examined this problem in the context of an Industrial Development Zone (IDZ). This study contributes to a better explanation of the challenges faced by IDZs in the developing country of South Africa and, in so doing, puts forward the following practical recommendations:

- Establish awareness and training programs to ensure all employees are cognisant of mitigation plans.

- Encourage information and knowledge sharing by including key members of each department in mitigation plans.
- Ensure top management's involvement in mitigation planning and their need to provide financial support and expertise.
- Adopt mobile viable solutions as potential mitigation strategies.
- Establish on-going security checks and revise existing security policies.

5.3 Limitation and Future work

The conceptual model in Figure 2.3 clearly demonstrates how failing to engage in a risk management process can adversely impact on critical business process. Given that organisations are affected by contextual factors, with each phase of the risk management process, the organisation should be cognisant of the need to readdress risk factors which could have changed due to the volatile environment. Although this research has contributed to the understanding of mitigation strategies, it has prompted the need for future research. Future research should focus on following issues:

- The research focused on a number of aspects of technological risk factor and mitigation strategies such as; risk in information systems, internal factors, mitigation strategies, the effective of mitigation strategies, disaster factors and the effectiveness of the mitigation strategies approach in the IDZ i.e. public organisation. Although this research helped to explore these factors and to achieve the objectives of the research, it did not provide the opportunity to explore in more depth some of the areas related to risk mitigation in other public sector organisations. This is one of the limitation of the study. Further research can focus on the practice of risk mitigation strategies within other type of public organisations, such as Local Municipal, Regional Municipal and Government sectors
- The study has not set a thorough focus on technological factors to assess a high availability of systems and server testing due to participants' lack of knowledge and experience on testing. This was another limitation. As the findings from the experience and respondent with specialities indicated, high availability systems and efficient server testing would have the potential of detecting significant problems which result in time wasted in troubleshooting

problems that were not documented in previous testing. This indicates that the respondents felt that documenting testing result was an integral part of their organisational approach. Therefore further research is required in order to provide a deeper insight on how sever and system testing is conducted and collaborates with risk approach. It can be conducted using different methodologies that employ in depth type of research and which focus on a larger number of experienced respondents

6 References

- Ahlan, A.R., Lubis, M. & Lubis, A.R. Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science*, 72 (2015):361-373.
- Aghili, S. (2010). Organizational Risk Management. *The Internal Auditor*, 67(3):21-23.
- Ahmad, A., Hadgkiss, J. & Ruighaver, A.B. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security*, 31(5):643–652.
- Altınay, F., Dagli, G. & Altınay, Z. *The role of information technology in becoming learning organization*. 12th International Conference on Application of Fuzzy Systems and Soft Computing, ICAFS 2016. 29-30 August 2016. Vienna, Austria.
- Apulu, I. & Latham, A. (2011). Drivers for Information and communication technology adoption: a case study of Nigerian small and medium sized enterprises. *International Journal of Business and Management*, 6:51-60.
- Apulu, I., Latham, A. & Moreton, R. (2011). Factors affecting the effective utilisation and adoption of sophisticated ICT solutions: Case studies of SMEs in Lagos, Nigeria. *Journal of Systems and Information Technology*, 13(2):125-143.
- AT&T. (2008, June). *AT&T Business Continuity Study Results*. Retrieved June 23, 2012, from https://www.att.com/Common/merger/files/pdf/business_continuity_08/business_Continuity_Study_Results.pdf
- Bakker, A.B. & Leiter, M.P. (Eds.). (2010). *Work Engagement: A Handbook of Essential Theory and Research*. New York, NY: Psychology Press.
- Ben-David, Y., Hasan, S., Pal, J., Vallentin, M., Panjwani, S., Gutheim, P. & Brewer, E.A. (2011). *Computing security in the developing world: A case for multidisciplinary research*. In Proceedings of the 5th ACM workshop on Networked systems for developing regions.
- Best Computer Practices. (2009). *DR Glossary of Terms*. Available from http://www.best-computer-practices.com/best-computer-practices/index.php?option=com_content&view=article&id=57&Itemid=64. [Accessed: 06 February 2009].

- Black, T. (1999). *Doing Quantitative Research in the Social Sciences*. London: Sage Publications.
- Braun, V. & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3:77-101.
- Bryman, A. & Bell, E. (2007). *Business Research Methods*. (2nd edition). New York: Oxford University Press.
- Cagliano, A.C., Grimaldi, S. & Rafele, C. (2015). Choosing project risk management techniques. A theoretical framework. *Journal of Risk Research*, 18(2):232-248.
- Collis, J. & Hussey, R. (2003). *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*. (2nd edition). New York: Palgrave Macmillan.
- Continuity Central. (2013). *2011 SMB Disaster Preparedness Survey*. Available from <http://www.continuitycentral.com/news05548.html>. [Accessed: 17 January 2013].
- Cooper, D. & Schindler, P. (2006). *Business Research Methods*. (9th edition). New York: McGraw Hill.
- Cordella, A. & Tempini, N. "E-government and organizational change: Reappraising the role of ICT and bureaucracy in public service delivery". *Government Information Quarterly*, 32.3(2015):279-286.
- Creswell, J.W. (1994). *Research Design: Qualitative and Quantitative Approaches*. Thousand Oaks, CA: Sage.
- Creswell, J. & Clark, P.V. (2007). *Designing and Conducting Mixed Methods Research*. Thousand Oaks, CA: Sage.
- Dangare, N.N. & Mangrulkar, R.S. (2015). *Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad Hoc Network*. International Conference of Information Security & Pravity (ICISP2015). 11-12 December 2015. Nagpur, India.
- Dey, I. (1993). *Qualitative Data Analysis*. Routledge: London.
- Easterby-Smith, M., Thorpe, R. & Jackson, P. (2008). *Management Research*. (3rd edition). London: Sage.

- Elliott, D., Swartz, E. & Herbane, B. (2010). *Business Continuity Management: A Crisis Management Approach*. (2nd edition). London: Routledge.
- Fischer, J.E., Reeves, S., Rodden, T., Reece, S., Ramchurn, S.D. & Jones, D. (2015). *Building a Birds Eye View: Collaborative Work in Disaster Response*. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '15). ACM Press.
- Franch, X., Susi, A., Annosi, M.C., Ayala, C.P., Glott, R., Gross, D., Kenett, R., Mancinelli, F., Ramsany, P., Thomas, C., Ameller, D., Bannier, S., Bergida, N., Blumenfeld, Y., Bouzereau, O., Costal, D., Dominguez, M., Haaland, K., López, L., Mourandini, M. & Sienna, A. (2013). *Managing risk in open source software adoption*. ICSOFT 2013: Proceedings of the 8th International Joint Conference on Software Technologies.
- Gartner. (2009). *Gartner for IT Leaders Toolkit: Presentation for the 2009 BCM Program Overview*. Stamford, USA: Gartner Inc.
- Geertz, C. (1973). *The Interpretation of Cultures*. New York: Basic Books.
- Ghuri, P. & Gronhaug, K. (2005). *Research Methods in Business Studies: A Practical Guide*. (3rd Edition). London: Prentice Hall.
- Gray, D. (2009). *Doing research in the real world*. Sage Publications: London.
- Haines, R. & Hosking, S. (2012). A bridge too far? The arms deal, the Coega IDZ, and economic development in the Eastern Cape. *Society in Transition*, 36(1):1-23.
- Hair, J., Babin, B., Money, A. & Samouel, P. (2003). *Essentials of Business Research Methods*. New York: John Wiley and Sons.
- Hausmann, V. & Williams, S.P. (2015). Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies. CENTERIS / ProjMAN / HCist 2015. October 7-9, 2015.
- Heiskanen, E. (2012). The ethical culture of organisations and organisational innovativeness. *European Journal of Innovation Management*, 15(3):310-331.
- Helbing D. (2013). Globally networked risks and how to respond. *Nature*, 497:51-59.

Hiles, A. (2004). *Business Continuity: Best Practice*. (2nd edition). Brookfield, CT: Rothstein Associates.

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Farnham, UK: Ashgate.

Hyväri, I. *Roles of top management and organizational project management in the effective company strategy implementation*. (2016). 29th World Congress International Project Management Association (IPMA), WC 2015, 28-30 September to 1 October 2015. *Procedia - Social and Behavioral Sciences*, 226(2016):108-115.

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, 33(2013):583-590.

Karkoszka, T. (2014). Processes Risk Management and Continuity Assurance. *KEM*, 615:133-138.

Knight, P. (2002). *Small-Scale Research*. (1st edition). London: Sage.

Knuth, D., Kehl, D., Hulse, L., Spangenberg, L., Brähler, E. & Schmidt, S. (2015). Risk perception and emergency experience: comparing a representative German sample with German emergency survivors. *Journal of Risk Research*, 18(5):581-601.

Kulbaa, V., Bakhtadzea, N., Zaikinb, O., Shelkova, A. & Chernova, I. (2017). *Scenario analysis of management processes in the prevention and the elimination of consequences of man-made disasters*. International Conference on Knowledge Based and Intelligent Information and Engineering Systems, KES2017. 6-8 September 2017. Marseille, France.

Kumar, R. (1996). *Research methodology: a step by step guide to beginners*. Sage Publications: London.

Kumar1, J.S., Zaveri, M.A. & Choksi, M. (2017). *Task Based Resource Scheduling in IoT Environment for Disaster Management*. 7th International Conference on Advances in Computing & Communications, ICACC-2017. 22-24 August 2017, Cochin, India.

Lewis, D. & Bloch, R. (1998). SDIs: Infrastructure, agglomeration and the region in industrial policy. *Development Southern Africa*. 15(5):727-755.

- Lewis, K.K. & Liu, E.X. (2017). Disaster risk and asset returns: An international perspective. *Journal of International Economics*, 108:S42-S58.
- Mangla, S.K., Kumar, P. & Barua, M.K. (2014). A flexible decision framework for building risk mitigation strategies in green supply chain using SAP-LAP and IRP approaches. *Global Journal of Flexible Systems Management*, 15(3):203-218.
- Mbambo, D.M. (2015). *An examination of the quality of infrastructure provided in South Africa's industrial development zone*. [Doctoral dissertation]. Cape Town: University of Cape Town.
- Mintzberg, H., Ahlstrand, B. & Lampel, J. (1998). *Strategy Safari; the Complete Guide Through the Wilds of Strategic Management*. London: Prentice Hall.
- Molla-Adankew, A., Molla, A. & Licker, P.S. (2005). ECommerce adoption in developing countries: A model and instrument. *Information and Management*, 42(6):877-899.
- Myers, M. & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, 17(1):2-26.
- Myers, M.D. (2009). *Qualitative Research in Business & Management*. London: Sage.
- Nel, E.L. & Rogerson, C.M. (2013). Special economic zones in South Africa: Reflections from international debates. *Urban Forum*, 24(2):205-217.
- Nel, E.L. & Rogerson, C.M. (2014). Re-spatializing development: Reflections from South Africa's recent re-engagement with planning for Special Economic Zones. *Urbani Izziv*, 25:S24.
- Nfuka, E.N. & Rusu, L. (2010). *Critical Success Factors for Effective IT Governance in the Public Sector Organizations in a Developing Country: The Case of Tanzania*. 18th European Conference on Information Systems.
- Ozkazanc, S. & Yuksela, U.D. (2015). *Evaluation of disaster awareness and sensitivity level of higher education students*. 7th World Conference on Educational Sciences, (WCES-2015). 05-07 February 2015. Novotel Athens Convention Center. Athens, Greece.
- Partington, D. (2002). *Essential Skills for Management Research*. (1st edition). London: Sage.

- Paton, D. (2003). Disaster Preparedness: a social-cognitive perspective. *Disaster and Prevention Management*, 12(3):210-216.
- Pepitone, J. (2012). Facebook: IPO debacle was Nasdaq's fault. *CNNMoney*. Available from <http://money.cnn.com/2012/06/15/technology/facebook-ipolawsuit/index.htm>.
- Perrow, C. (1967). A framework for the comparative analysis of organizations. *American Sociological Review*, 32(2):194-208.
- Raval, V. & Fichadia, A. (2007). *Risk, Controls, and Security: Concepts and Applications*. New Jersey: John Wiley & Sons.
- Sagan, S.D. (2004). Learning from Normal Accidents. *Organization & Environment*, 17(1):15-19.
- Saunders, M., Lewis, P. & Thornhill, A. (2000). *Research Methods for Business Students*. (2nd edition). Essex: Prentice Hall.
- Shaluf, I., Ahmadun, F. & Said, A. (2003). A Review of Disaster and Crisis. *Disaster Prevention and Management*, 12(1):24-32.
- Shaluf, I.M. (2008). Technological disaster stages and management. *Disaster Prevention and Management*, 17(1):114-126.
- Spears, J.L. & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*, 34(3):503-522.
- Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M. & Gritzalis, D. (2015). Risk mitigation strategies for critical infrastructures based on graph centrality analysis. *International Journal of Critical Infrastructure Protection*, 10:34-44.
- Stride, R. (2007). *Disaster invocations in South Africa - what are the causes?* Retrieved July 01, 2011, from <http://cbr.co.za/article.aspx?pkarticleid=4234>
- Talluri, S., Kull, T.J., Yildiz, H. & Yoon, J. (2013). Assessing the efficiency of risk mitigation strategies in supply chains. *Journal of Business Logistics*, 34(4):253-269.
- Turner, B. A. (1976). The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly*, 21(3):378-397.

Vernim, S. & Reinhart, G. (2016). *Usage Frequency and User-Friendliness of Mobile Devices in Assembly*. 49th CIRP Conference on Manufacturing Systems (CIRP-CMS 2016).

Werlinger, R., Hawkey, K. & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1):4-19.

Willig, C. (2001). *Introducing qualitative research in psychology: Adventures in theory and methods*. Open University Press: Buckingham.

Wright, R. (2010, March). *Toyotas Are Safe (Enough)*. Available from <http://opinionator.blogs.nytimes.com/2010/03/09/toyotas-are-safe-enough/>. [Accessed: June 2012].

Yaokumah, W. (2015). Evaluating the effectiveness of information security governance practices in developing nations: A case of Ghana. *Standards and Standardization: Concepts, Methodologies, Tools, and Applications* IGI Global.

Yin, R. (1994). *Case study research: Design and methods*. Sage Publications: Beverly Hills, CA.

Appendix A: Research Instrument

1. Demographic details

The study was conducted at one organisation and fifteen respondents participated from the organisation

a. Department

Ten participants are from the IT department, two from corporate services, one from business development, one from shared services, and one from finance.

b. Title

These include the executive manager of Corporate Services & Operations, programme director of Business Development, and an account manager who is acting chief financial officer (CFO), business analyst, business process analyst, project manager, solution architect, developer, oracle support, security specialist, CIO. The participants were chosen based on their depth of understanding of mitigation strategies, as well as their working experience at the organisation.

c. Role in the organisation

The participant role in the organisation is as follows:

- CIO – is in charge of information technology strategy, establishing IT framework, IT security policies and computer programmes required to support the organisation's goals and objectives
- Solution Architect – designs, describe and managing the solution engineering in relation to specific business problems. They find the best solution amongst all possible to solve the existing business problem. They ensure that the solution meets the company standards that are relevant to technology, human and financial resources

- System admin – is responsible for the upkeep, configuration, and reliable operation of computer systems, especially multi-user computers such as servers.
- Project manager – is in charge of the overall responsibility for the successful initiation, planning, design, execution, monitoring, controlling and closure of the project. Key among project manager’s duties is the recognition that risk directly impacts the likelihood of success and that this risk must be both formally and informally measured and determine the most effective mitigations.
- IT manager – in charge of business continuity and advising organisation on IT solutions that will be best help them grow and perform more efficiently. IT manager is also responsible and accountable for the smooth running of computer systems, servers and the maintenance of the organisation’s computing needs.
- Developer – plays a key role in the design, installation, testing and developing of a software systems. The software the developer create are likely to help business be more efficient and provide better service.
- Business analyst – help organisation to implement technology solution in a cost effective way by determining the requirements of a project or program and communicating them clearly to relevant stakeholders. Business analyst further define needs and recommending solutions that deliver value to the organisation.
- Business process analyst – draw interferences from process details and link these inferences to the big picture by considering business objectives in identifying process improvements. Business process analyst usually meet with users, collecting data, researching process, analysing information and observe process in action to identify process improvement.
- Oracle support – act as a single point of contact for the hosted Oracle systems and also responsible for the Oracle applications systems maintenance support, monitoring, application of all patches, upgrade and technical code release management.

- Security specialist – safeguards information system assets by identifying and solving potential and actual security problems. Protects system and servers by defining access privileges, control structure and implement security improvements.
- Executive manager – defines the vision and goals of the entire department. He does this by implementing policies and procedures, and by establishing budgets. Executive manager also oversee personnel decisions, and managing contracts and negotiations as well as analysing data to make the best business decisions.
- Program director – maintain full responsibility over a respective department. Program director manages their department ensuring that tasks and objectives are being met.
- CFO – makes a new investment in an organisation by improving the organisation's operations and profitability. CFO controls the organisational budget, costs and provide a solid direction to organisation assets and investments.

d. Experience: Number of years in position

- Executive Managers – 10 and 12 years
- CIO- 12 years
- Program director – 10 years
- CFO – 12 years
- Solution architect – 9 years
- System admin – 7 years
- Project manager – 9 years
- IT manager – 10 years
- Developer – 9 years
- Business analyst – 8 years

- Business process analyst – 8 years
- Oracle support – 5 years
- Security specialist – 6 years

2. What factors affect how you manage risk

The factors that affects how organisation manage its risk are Human, Organisation and Technological factors.

Human factor

- Cyber-crime - the majority of cyber-attacks take the form of phishing, where cyber target individuals rather than the systems.
- Excessive system user privileges- when employees are granted default system privileges that exceed requirements of their job functions, these privileges are abused. For example, some employee whose job requires the ability to change only user account such as username and password, they take advantage of excessive system privileges and grant their colleagues to have access on systems administration.

Organisational factor

- Leadership style and management practice- for managers' leadership style is even more influential as an individual gains rank, incompetence becomes a very real risk. Some managers with a hands-off management style they place an organisation at risk by failing to identify incompetence until is too late to correct
- Failure to communicate – failure to communicate between departments to share their knowledge on risk and what risk are they currently facing.

Technological factor

- Layers of redundancy – the organisation had a single layer of redundancy which had exposed them to system malfunctioning. That is, the servers and the infrastructure

had a single component in which there was no independent backup component to ensure system functionality continues in the event of failure.

3. How does the organisation mitigate these risks?

Human factor

- Cyber-crime – To this end, the organisation trains employees in basic security practices such as how to recognise potential threats and what precautions to take. Also to stay ahead to thread landscape, the organisation leveraging both the in-house expertise of cyber security team in addition to the know-how of the cyber security vendor.
- Excessive system user privileges – the organisation have implemented a user rights management as a security feature controlling which rights a user can access and what actions a user can perform. Therefore a system admin is granted a privilege to access specific function and perform a particular action, and that is being monitored regularly.

Organisational factor

- Leadership style and management practice – the organisation perform and interpret employee background checks persuade to the law. They conduct a human development skills for senior managers to ensure that leaders are competent and well qualified for their role.
- Failure to communicate – project managers leads the development, documentation and implementation of a communication plan that identifies appropriate audience, establishes the communication schedule and manages the flow of information around the organisation. Communication plan makes it easier to say the right things in the right way to the relevant people using the best tools. This plan includes what needs to be communicated, how often, channel of communication and individual responsibilities.

Technological factor

- Layers of redundancy – one way to reduce the organisation’s technological risk, the organisations has added a layers of redundancy throughout the infrastructure. Their cloud infrastructure, on premises environment and server has a lines of N+1 availability, a configuration in which multiple components have at least one independent backup component to ensure system functionality continues in the event of a failure.