Investigating Recurring Impediments to Effective IT Continuity Management in a South African Insurance Firm

Dissertation presented to the Department of Information Systems
University of Cape Town

Ilse van Beulen

Dissertation - in partial fulfilment of the writing requirements for the
Coursework and Dissertation Masters Programme in Information Systems 2010
(INF5005W)

Plagiarism 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 dissertation "Investigating Recurring Impediments to Effective IT Continuity Management in a South Africa Insurance Firm" from the work(s) of other people has been attributed, and has been cited and referenced.
3. This dissertation "Investigating Recurring Impediments to Effective IT Continuity Management in a South Africa Insurance Firm" 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 / her own work.
5. I acknowledge that copying someone else's assignment or literature review, or part thereof, is wrong, and declare that this is my own work.

Date **:** 13th May 2013

Signature :

Full name of Student : Ilse van Beulen

Abstract

Information Technology (IT) has come to be an essential part of carrying out business in our technologically advanced world. Unquestionably, a business can practically not survive without IT for protracted periods of time. IT failures could present challenges to organisations which, if not managed efficiently, could lead to technological disasters from which companies would be hard pressed to recover.

Often companies are complacent about continuity plans, either because their managements have a false sense of their ability to recover from a disaster or they believe that the company is immune to disasters. Companies further believe that there is no need to take out Disaster Recovery contracts, as they are confident their insurance and maintenance contracts should cover them in case of hardware or software failure. What companies often fail to take into account is that an IT failure could extend for long periods unless they have the appropriate mechanisms in place to mitigate such failures. This lack of the awareness of the concept and importance of IT Continuity Management encompasses not only monetary losses, but the ramifications could extend to the damage of their brand and reputation, resulting in the loss of clients and might have legal repercussions as well.

The research was undertaken in Company X, one of South Africa's leading financial services groups. Despite a strong Business Continuity ethos inherent in the Company, an analysis of several tests over two years highlighted the fact that they experienced recurring issues within the IT Continuity sphere. The study was borne out of the need to understand why the same issues were encountered year after year, what factors contributed to these issues, and what measures were required to mitigate these issues. The impact of these recurring issues had a negative impact on the disaster recovery tests as most of the tests were not successful, on the resources required to perform the tests, and on the general perception people had regarding disaster recovery.

The study analysed the results (reports, audit findings, etc.) of several disaster recovery tests, and produced an inventory of the recurring issues experienced during these tests. Based on these results, a questionnaire was developed and distributed to the stakeholders who had a direct relationship with IT Continuity. The findings of the study concluded that human, organisational and technological (HOT) factors produce recurring issues which can only be mitigated with strong IT Continuity Management practices and principles. The findings are discussed against a newly developed conceptual model which depicts the relationships between the HOT factors, recurring problems, and effective IT Continuity Management principles.

Contents

Table of Figures

Table of Tables

Table of Common Terms and Acronyms

Term	Definition
Application	An application is: 1. A particular customer use to which an information processing system is put - for example, a payroll or general ledger application. 2. A program, set of programs, or software package designed for a particular purpose such as payroll or general ledger. 3. Software that provides Functions that are required by an IT Service. Each Application may be part of more than one IT Service. An Application runs on one or more Servers or Clients. See also Application Management. (ITIL V3) An application may be made up of many different types of data, such as multiple database components, data feeds from other applications or other data sources, flat files and electronic transmissions.
Application Recovery	A component of Disaster Recovery that deals with the restoration of business system software and data, after the operating system environment has been restored or replaced.
Battlebox	A secure box containing a variety of documentation / equipment selected to assist with the management and control of business continuity. It is a pro-active 'tool-box' which is readily available to control and manage a disruptive event in the organisation.
BC	Business Continuity is an extension of disaster recovery, aimed at allowing an organization to continue functioning after (and ideally, during) a disaster, rather than simply being able to recover following a catastrophic event. This is accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems and data replication techniques as well as a solid backup and recovery strategy.
BCM	Business Continuity Management: An all-encompassing term covering both disaster recovery planning and business resumption planning. BCM safeguards the interests of key stakeholders, reputation, brand and value-creating activities. The BCM Process involves reducing Risks to an acceptable level and planning for the recovery of Business Processes should a disruption to the Business occur. BCM sets the Objectives, Scope and Requirements for IT Service Continuity Management.
BCP	Business Continuity Plan: A comprehensive written plan to maintain or resume business in the event of a disruption. BCP includes both the technology recovery capability (often referred to as disaster recovery) and the business unit(s) recovery capability.
DR	Disaster recovery is the process, policy and procedure related to preparing for recovery or continuation of technology infrastructure critical to an organisation after a natural or human--induced disaster. Recovery after disaster, such as fire, earthquake, etc., that destroys or otherwise disables a system. Disaster recovery techniques typically involve restoring data to a second (recovery) system, then using the recovery system in place of the destroyed or disabled application system. See also recovery, backup, and recovery system.
DCN	Data Centre North refers to the Remote Data Centre situated in Midrand, Gauteng
DC	Data Centre
DR	Disaster Recovery
HA	High Availability: Systems or applications requiring a high level of reliability and availability. High availability systems typically operate 24/7 and usually require built-in redundancy to minimise the risk of downtime due to hardware and/or telecommunication failures.
ITC	Information Technology Continuity
ITSCM	IT Service Continuity Management: The process responsible for managing risks that could seriously affect IT services. ITSCM ensures that the IT service provider can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT services. ITSCM should be designed to support business continuity management.
Maturity	Maturity: A measure of the Reliability, Efficiency and Effectiveness of a Process, Function, Organisation, etc. The most mature Processes and Functions are formally aligned to Business

	Objectives and Strategy, and are supported by a framework for continual improvement.
Recovery	The process of rebuilding data after it has been damaged or destroyed. In the case of remote copy, this involves applying data from secondary volume copies.
RPO	The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data protection strategy is developed.
Recovery Time	The period of time from the disaster declaration to the recovery of the critical functions.
RTO	Recovery Time Objective: The period of time within which systems, applications, or functions must be recovered after an outage, e.g. one business day. RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. Similar Term: Maximum Allowable Downtime
SLA	A Service Level Agreement (SLA) is part of a service contract where the level of service is formally defined.

1. Introduction

1.1 Background

Globally, there is a growing reliance on IT systems and services. As the world has become more technologically advanced, IT has grown and developed to be a central part of conducting business. However, this over-dependence on IT has also presented major challenges for organisations. Microsoft's marketing failed spectacularly when the blue screen of death displayed across a diverse spectrum of screens for a four-day period in November, 2007 (France 24 News, 2011). There are many similar examples of setbacks resulting from IT failure (Nielsen, 2008; Mawson & McConnachie, 2011).

The insurance industry has not been excluded from setbacks resulting from IT failure. With the changing market place, customer demands and legislative requirements, this industry is increasingly forced to harness IT resources to stay in business. Consequently, many information-intensive services have been automated, and the internet is used extensively by insurance firms for marketing, policy administration, claims settlement and on-line advice (Baur, Birkmaier, & Rüstmann, 2001). Obtaining accurate information quickly and efficiently remains an integral component of the insurance sector. However, these developments also expose many insurance firms' risks and IT failures or disasters.

A complete Business Continuity Plan consisting also of an IT Continuity Plan must be in place for an organisation to recover after a disaster (Botha & Von Solms, 2003; Woodman & Kumar, 2009). IT Continuity comprises the preparation and planning to make sure that an organisation has the ability to survive a disaster, and this includes ensuring the recovery of data, continuing business operations, and protecting their reputations (Al-Badi, Ashrafi, Al-Majeeni, & Mayhew, 2009).

1.2 Problem Statement

Though the need for continuity plans has been emphasised over the years, not many organisations have such plans in place. Risk management practices are often built on retrospection which emphasises fault tabulation and calculating the likelihood of failure (Schopp et al., 2006). A recent study by Nielsen (2008), that collected the views of the insurance sector on business continuity, confirms this concern. The study revealed that IT is the second highest cause of disruption in the organisation. The study further showed that 25% of the respondents did not have arrangements in place for a Business Continuity Plan, and the reasons supplied could generally be summarised as "lack of the awareness of the concept and importance of BCM" (Nielsen, 2008, p.1). While interruptions to business are primarily caused by incidences of IT capacity and the loss of

telecommunications (Helms et al., 2006), there exists a real deficit in literature dealing with the planning for natural and technological disasters (Perry & Lindell, 2003).

Consistent with international studies, one of the few studies conducted in South Africa between 1983 and 2006 revealed that the primary cause of invocations was hardware failure (Stride, 2007). More than half of all invocations originated because of computer glitches or the failure of critical pieces of hardware. According to Stride (2007), South African companies frequently believe that there is no need to take out Disaster Recovery contracts because they are confident that they are protected by comprehensive existing hardware maintenance agreements. However, the statistics collated on companies who had invoked recovery plans do not give credence to this view held by companies, as almost all of the companies who invoked recovery plans had maintenance agreements in place (Stride, 2007). This tendency persists today, maintaining its position as the leading cause of declared disasters (Stride, 2007; Strydom, 2009; Holmes, 2010).

In a survey done by AT&T (2008), one third of IT executives were unaware of what their continuity or recovery plans comprised, and many admitted that their respective companies had no plans in place. A table-top (paper based) simulation held with senior management in Company X (the company in which this study was conducted) in June 2011, produced findings consistent with this statement, where management knew with certainty that continuity plans exist, but were not familiar with the detail, e.g. where the Battle box was kept and what the procedures were to invoke the proceedings in the Battle box. It further revealed that members had varying levels of knowledge of these plans, but none had sufficient knowledge about what these continuity plans entailed.

In AT&T's study (2008), where the companies had full-scale data centres, 22% of the participants mentioned that their Business Continuity plans required revision (Kadlec & Shropshire, 2009). Company X also identified the need to revise their continuity plans. Company X has two data centres adjacent to each other, where Data Centre 2 provides redundancy for Data Centre 1, the primary data centre. It was thought that High Availability (HA) testing could be performed, where the failover capability of the critical systems in Data Centre 1 could be verified by forcing the unavailability of the primary nodes to failover to the secondary nodes in Data Centre 2. Therefore, the plan for the 2011 HA test was to power-down or shut down one data centre completely, so as to emulate a real-life scenario of losing a data centre. While preparing for the 2011 HA test, input was invited from all stakeholders, namely IT, business, as well as all the service providers, to identify potential issues that such a test could encounter. The issues raised indicated that this kind of test was not feasible, due to the fact that the data centre design did not enable full failover capability. Another problem highlighted was that there were legacy systems which had never been re-booted and, because the

technology was archaic, it was uncertain how these systems would react when they were to be powered-up again. In terms of the preparedness of Company X, it served as clear warning that the Company was vulnerable to disaster destroying either data centre, as the other data centre was not capable of sustaining full failover capability. The data centres were originally built in this manner by design, with the associated risk the design introduced acceptable to the Company. Whatever the initial basis for the design decision, e.g. cost, it does infer doubts about the level of commitment to IT Continuity.

Organisations continue to be complacent on the subject of continuity (Srivantaneeyakul, 2007) and this reality has far-reaching consequences. IT Continuity faces various challenges, the most conspicuous being that "like life insurance, IT Continuity is a 'grudge' insurance" (Regensberg, 2008, p.8), and since IT continuity is regarded as an expense which safeguards a company against an event which may never happen, it is problematic to demonstrate a Return on Investment (ROI) in IT continuity (Vision Solutions, 2009; Strydom, 2009). Furthermore, IT Continuity does not contribute directly to 'the bottom-line' (Schopp et al., 2006). Consequently, it increases the efforts to procure funding for investments in information availability, e.g. technology resilience, back-ups, etc., and has a negative impact on the time and resources which are allocated to continuity efforts. In the long run it amounts to ineffectual continuity plans (Toigi, 2003). In Company X the difficulty in procuring funding for continuity efforts is evident in the fact that the Remote Data Centre has approximately twenty five percent diminished capabilities as opposed to that of the primary data centres.

1.3 Purpose

The issues that were identified during the preparation for the 2011 HA test, led to a re-assessment of the test reports of the High Availability (HA) and Remote Data Centre (RDC) tests over the previous two years. The analysis indicated a number of recurring issues, where each successive HA and RDC test encountered significant problems which resulted in resources spending time trouble-shooting issues experienced yet not documented in a previous test.

The time inefficiencies and tests which closed unsuccessfully resulted in situations where acceptance sign-off of test results could not be obtained from business areas. Furthermore, the resources who participated in these tests (both IT and business) were negative, often uncooperative, and showed their irritation at being called away from pressing production issues and other day-to-day operational tasks.

This study therefore investigated those factors contributing to the recurring issues which impede the effectiveness (and preparedness) of a disaster recovery unit (specifically in the IT Continuity

Management portfolio) in Company X. The research also aimed at identifying ways by which these issues might be mitigated in Company X.

This study begins with a review of literature on Business Continuity Management and IT Continuity Management. It encompasses a brief overview of definitions and types of disasters. A section is dedicated to a review of the theoretical analysis which explain disasters, the causes of disasters and the management required to mitigate disasters. The study then looks at the methodology used to conduct the research, and concludes with a comprehensive discussion on the findings.

1.4 Research Importance and Benefits

Company X is dependent on information technology (IT) as it integrates into all functions of the organisation. This accentuates the need for data to be continuously available, and the dependency on the IT professionals to maintain fully-functional services. The study was prompted by recurring errors experienced during Disaster Recovery tests conducted by Company X which resulted in unsuccessful Disaster Recovery testing. IT Continuity is to enable the Company to restart IT services proficiently in the event of a disaster, to minimise prospective economic losses, to reduce possible exposure as a result of technological disasters, and to reduce the probability of a disaster, and this may be achieved by understanding and mitigating recurring issues. Moreover, the Company benefited from the research because the analysis highlighted risks and proposed methods to manage-down the impact of unavoidable disasters.

The research is also of potential benefit to IS researchers because it could add a layer of transparency to IT Continuity issues which is currently unavailable. According to Stride (2007), South African companies are bombarded with statistics from foreign sources, which show causes for foreign disasters. However, in Africa, conditions are different from those of our European and American counterparts, i.e. South Africa has a less stable infrastructure and perhaps fewer skills available to ensure stability. The problem facing South African companies is the unavailability of reliable statistics (Stride, 2007), because of the lack of a regulatory body and a single source of reliable and unbiased information. The results of the dissertation could add a level of statistical visibility which might be useful to researchers and guide future research.

Continuity practitioners, e.g. members of the South African Business Continuity Forum (Western Cape), may also benefit from the research in the event of their experiencing similar issues within their respective organisations. The research highlighted factors which cause IT discontinuity. It may thus enable them to better manage the continuity process by understanding the frustrations resources experience with continuity efforts, and understanding the underlying causes of recurring

issues. By understanding the common origins of downtime and how these disasters unfold, practitioners are empowered with tools to minimise the impact a disruption may have on mission-critical functions. If these tools are implemented properly, it may help reduce the number of overall disruptions. Pre-planned recovery steps will reduce the time taken to make critical decisions (Toigi, 2003, p.347). Central to the research is the emphasis on the importance of continuity, which might enable these practitioners to build a business proposition to defend the need for continuity within their respective organisations. The theoretical discussion around how disasters are caused and managed may allow them to position themselves more favourably in averting disasters and ensuring the continuity of their organisations.

Internal and external IT auditors may also benefit from the research. IT Continuity in Company X is audited every year, and these audits are traditionally based on the issues highlighted during the HA and RDC tests. Therefore, the audit findings are very much a reflection of the reports compiled during the tests. During the past year, when the initial findings from the study became apparent, these observations were shared with the auditors, and the scope of the audits broadened, highlighting the risk of technical disruptions from which the Company would not recover easily, including human risk such as apathy. The auditing sphere became more than just a reflection of the test reports, but became rich in addressing issues which should be of genuine concern to the Company, e.g. the fact that, while the Company could recover the IT components in the event of a disaster, it was useless if people could not access these systems, and thus the audit highlighted the importance of specific business unit recovery measures which needed to be put in place. Looking ahead, the research could aid internal and external IT auditors in their discovery, as well as in highlighting the issues with management. It would also help with putting particular continuity management and disaster recovery factors on their radar screens for the next audit.

A significant contribution of the study is the awareness which the research creates about the problem (recurring issues) in the insurance sector. Generally, there are very few studies of this kind in existence and, in fact, this could well be the first of its kind in South Africa. None of the research undertaken for the Literature Review yielded any previous such study.

Organisations which do not have a comprehensive continuity plan in place have a diminished prospect of continuing to conduct business after a disaster (Wong, 2006). Consistent with this finding, a study done confirmed that forty three percent of companies which are subjected to a disaster will not pull through, while ninety percent which lose data during a disaster will cease operation within two years of the event; eighty percent of organisations without a Disaster Recovery Plan (DRP) will go out of business within twelve months of experiencing a fire or flood (Al-Badi et al.,

2009). These statistics confirm that there is a need for raising Disaster Recovery and Business Continuity Planning awareness.

1.5 Research Motivation

My motivation for completing this research is to fulfil, on a personal level, an understanding of the recurring issues currently experienced in the field of IT Continuity. I currently hold the portfolio of IT Continuity in the company I work for, and thus the subject is of specific interest to me.

IT Continuity faces various challenges, the most conspicuous being that it is problematic to demonstrate a Return on Investment (ROI) since IT Continuity is regarded as an expense which safeguards the company against an event which may never happen. My experience has been that people are loath to participate in continuity efforts because they do not see the benefit, or rather, they are only able to experience the benefit of continuity plans in the face of a disaster and, because of the lack of huge scale disasters, they are unable to align their mental paradigm with the effort associated with continuity. Thus the motivation in undertaking such a study was in part to understand what was required to build a value proposition for IT Continuity within Company X. The consequence of not being able to prove ROI increases the efforts to procure funding for continuity efforts, and has a negative impact on the time and resources which are allocated to such efforts (Toigi, 2003). I am often told resources cannot attend to IT Continuity efforts due to more urgent and pressing day-to-day operational tasks. This becomes even more problematic when the resources are contractors and their time is billed to a particular project: no-one wants to foot the bill for these resources spending time on IT Continuity efforts.

The motivation in undertaking thus study also stems from the confusion in accountability and responsibility for IT Continuity within the Company. Business sees it as an IT responsibility (because they are responsible for the hardware and the software), while IT sees it as a business responsibility (given that business controls the expenditure on IT Continuity efforts). It is my belief that IT Continuity is the concern and obligation of the whole Company, and necessitates the buy-in and sincere commitment from every single manager, regardless of rank. IT cannot do its Business Continuity Planning in isolation from the rest of the organisation.

2. Literature Review

The literature review commences with a brief definition of Business Continuity and IT Continuity, with the aim of clarifying any unambiguity which may exist and to elucidate the core role of IT to business. An overview on disasters is given, after which a number of theoretical models on disasters, and how various models describe the formulation of disasters, are discussed. The role of the concepts of Risk and Time-in disasters is also described. The attributes or causes of technological disasters are reviewed, and this section concludes with a few disaster management models to manage, contain and mitigate disasters. The aim is to give a background so that we can better understand the recurring issues within Company X that impede effective IT continuity management, what causes them, and how they can be mitigated.

2.1 Business Continuity Management

Business Continuity Management (BCM) is defined by the British Standards Institution's Code of Practice for Business Continuity Management (BS 25999-1) as "a holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause; and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities" (Woodman & Kumar, 2009, p.3). Business Continuity Planning (BCP), one of the processes executed under BCM, is the process of planning for the recovery of overall business operations in the event of a business interruption (Best Computer Practices, 2009). BCP is, therefore, "the pre-planning which focuses on business processes (rather than IT infrastructure) required to ensure that a company can continue to exist despite a crisis, thereby mitigating the impact of the crisis" (Toigi, 2003, p.457).

IT Continuity (ITC) is also a subset of Business Continuity Management, with the primary focus on the pre-emptive and reactive procedures to restore the IT infrastructure which is used to deliver IT Services (Toigi, 2003, p.3), i.e. it comprises the activities which ensure that IT Services can carry on in the event of a serious incident (Hammond, 2007). It consists of the procedures in preparing for, establishing, testing and implementing the courses of action required to reduce the effects of service unavailability on customers, in accordance with service level agreements (Hinca, 2006). The intent of ITC is to anticipate and reduce the impact of protracted system unavailability by means of "developed, pre-defined, documented and tested continuity procedures" (Hiles, 2011, p.229).

Information Technology Disaster Recovery Planning (ITDRP), a subset of ITC, plans for those activities which the Company must undertake to increase its ability to recover IT systems and services following a disaster, and this includes IT disaster identification and notification, preparation of

organisational members, IT services analysis, recovery processes, backup procedures, offsite storage, and maintenance (Kadlec & Shropshire, 2009). It describes and lists the actions a company must perform in reaction to an IT-related crisis (Toigi, 2003). Typical activities would encompass the retrieval and salvage of data, hardware and software, i.e. those steps required for the recovery of critical business operations after a disaster. Simply put, BCP are those endeavours which take place before an incident occurs, and Disaster Recovery (DR) is what happens during and after the incident (Al-Badi et al., 2009).

There are no precise and clear distinctions between the definitions; however, the inter-relationship of the defined processes, with the introduction of a definition for contingency planning, are depicted in Figure 1.

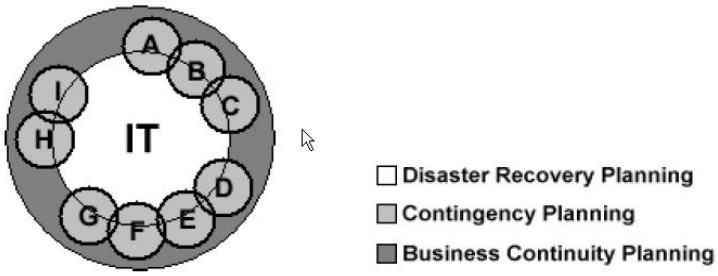

Figure 1. BCP and DRP Relationship (Botha & Von Solms, 2003)

The smaller circles labelled A to I represent various business processes. These processes are all dependent on services and infrastructure provided by the IT Department, depicted by the innermost circle, labelled IT (Figure 1). Some of these processes are also dependent on others, as depicted by the overlapping circles. The outermost circle represents Business Continuity planning, a combination of the disaster recovery plan for the IT department and the contingency plans for these various business processes (Botha & Von Solms, 2003). The present study focuses on the central element of Figure 1, i.e. IT, and how failure to manage its continuity may adversely impact on other organisational activities. For the purposes of this study, we will continue with the term IT Continuity (ITC).

2.2 Disasters

A disaster is generically defined as a severe interruption of the functioning of society, producing extensive human, material or environmental losses which surpass the capacity of the affected society to survive while depending on its own resources (Shaluf, 2007a). From an organisational perspective, Toigi (2003, p.4) defines a disaster as the unplanned interruption of normal business processes resulting from the interruption of the IT infrastructure components used to support them.

This includes information systems and networks and their hardware and software components, as well as the data itself.

Three types of disasters can be identified, namely natural disasters, man-made disasters and a hybrid between natural and man-made disasters (Figure 2). Natural disasters are those catastrophic events resulting from natural hazards which can originate internally beneath the earth's surface, externally (topographical), as well as weather-related (meteorological/hydrological) and biological phenomena. Natural disasters are beyond human control and are often termed an "Act of God" (Shaluf, 2007a, p.687). Man-made disasters, also known as technological or socio-technical disasters, are those disastrous events which arise from human decisions. Hybrid disasters are an amalgam of human decisions and natural forces. Regardless of the type, all disasters have a common denominator, which is the severity of their impact on people, property, and the environment (Shaluf et al., 2002, 2003b, 2003c; Shaluf, 2006, 2007a, 2007b).

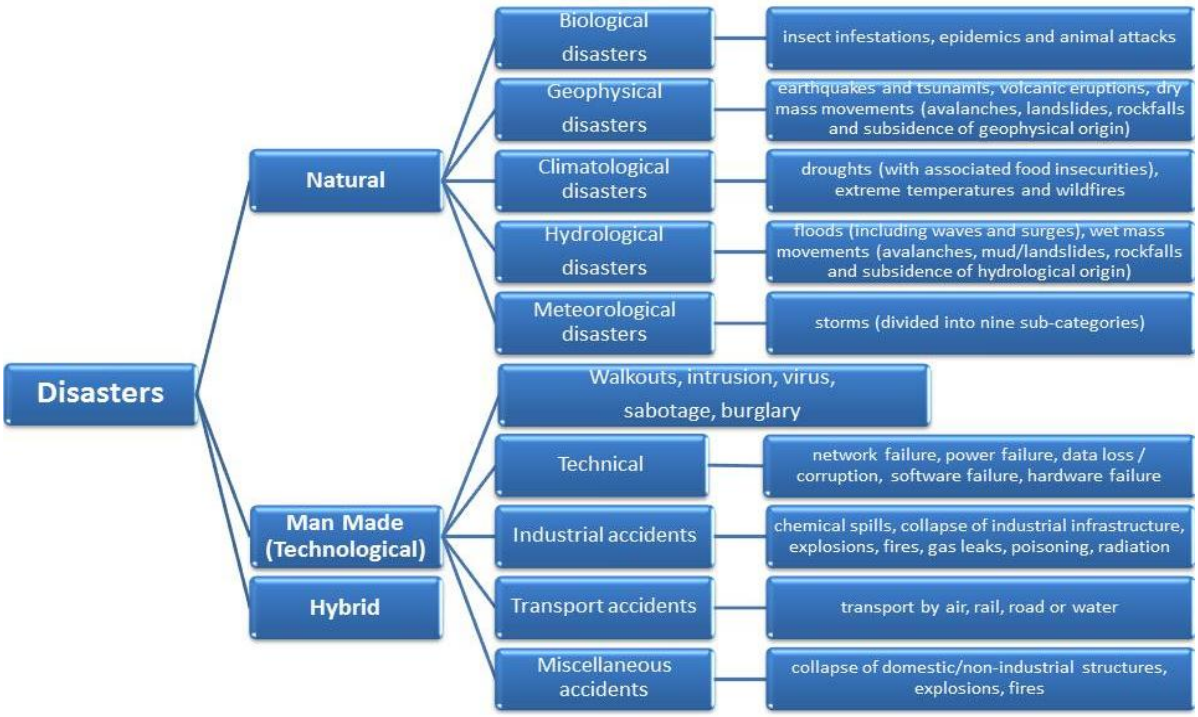

Figure 2. Diagrammatic representation of the types of disasters (compiled fromToigi, 2003, p.3; Shaluf et al., 2002, 2003b, 2003c; Shaluf, 2006, 2007a, 2007b)

A disaster is an unexpected incident which impacts on the critical processes of the organisation (Hinca, 2006). Typically, the nature of such an event is that it disrupts business-as-usual to the extent that monetary losses can be incurred, and these losses can be quantified (Maiwald & Sieglein, 2002). From a business continuity perspective, a disaster is declared when an event or chain of events results in the inability of an organisation to provide critical business functions for a period of

time, and which causes the company to move from using standard operating procedures to employing its disaster recovery procedures (Wong, 2006).

This present study focuses on man-made (also known as technological) disasters, which range from the accidental deletion of a file to recovery from the loss of a building that houses the data centre along with the IT infrastructure, e.g. due to a hurricane or flooding, etc. Other examples of IT services which could be disrupted include internet connectivity, telecommunications, data storage and processing, hardware, software, data, human resources, and utilities (Kadlec & Shropshire, 2009).

2.3 Disaster Models

A number of theoretical models exist which aim to explain how disasters are formed. Models are useful in gaining insight to complex matters.

2.3.1 Deterministic Models

Determinism assumes that reality conforms to cause and effect relationship, where disaster is classified as the end result (Gibb, et.al, 2002). There is a general philosophical theory which states that for everything that happens there are conditions such that, given them, nothing else could happen. William Heinrich posited the Sequences-of-events theory in 1931, which purports that a disaster is considered to be the outcome of a sequence of events, i.e. the conclusion of a sequence of events. In this model, events preceding the accident happen linearly, in a fixed order, and the accident itself is the last event in the sequence. The deterministic model is also known as the 'domino model' for its depiction of an accident as the 'end point' in a string of falling dominoes, which holds that an accident or incident is an event or chain of events resulting in the inability of the organisation to provide IT services. In this linear model, events occur akin to that of having a domino effect, i.e. when one of the dominoes falls, it triggers the next one, and the next, but that removing a key factor such as an unsafe condition or an unsafe act prevents the start of the chain reaction. In the deterministic model, a disaster is depicted as the last of the sequence of events. The concept is widely used in risk analysis, fault-tree analysis, probabilistic risk assessments, Petri nets, critical path models, etc. (Hollnagel, 2008; Ho, 2010).

Deterministic models with a technological interpretation espouse the theory that technology is an objective external force which has a deterministic influence on humans and organizations (Leavitt & Whisler, 1958; Blau et al., 1976; Hiltz & Johnson, 1990), i.e. technology governs what we do, and transforms our social activities. The assumption was that the adoption of technology would bring about inevitable changes at the organisational level, e.g. by enabling decentralisation or

centralisation. Decentralisation, among other benefits, allows organisations to take advantage of division of labour by sharing decision-making across the organisation, coordinating efforts and communicating. Decentralisation comes with a cost, and may also present challenges which could lead to disasters, e.g. by federating many business processes, it also has an impact on creating schisms in decision-making or processes, which could result in duplicating technology procurement efforts. The adoption of technology could, however, also enable centralisation, e.g. by consolidating various business data into a single warehouse would ensure that technology, e.g. monitoring and alerting software, is standardised across all the business units which share the warehouse, thus reducing effort and cost. Orlikowski (1996) posited, however, that the centralisation of technology may also enable disasters, e.g. migrating everything to a single warehouse would create a single point of failure, where the unavailability of the warehouse due to a disaster would have an impact on several business processes.

Many have progressed to developing models based on this notion alone. However, the danger is that, by focusing on technology only, systems or models are developed that have limited consideration of other organisational and socio-technological aspects. Consequently, these technology-based models and control systems break down, resulting in disasters. The shortfall of the deterministic model is that it looks at disasters at the end of a sequence of technological events; hence it is not cognizant of the organisational and social aspects that take place concurrently with technological aspects, and which can also contribute to disasters. An example is the loss of NASA's Mars Polar Lander, where spurious computer signals (during the deployment of the landing legs) were interpreted by the on-board software as an indication that the craft had landed, and hence shut the engines down prematurely, causing the spacecraft to crash into the Mars surface (Lloyd, 2009). The landing leg extension and software executed according to specification; however the accident materialised from unforeseen interactions between leg deployment and descent-engine control software (David, 2005).

2.3.2 Contingency Models

In contrast to the deterministic viewpoint, contingency models hold that the structure of an organisation depends upon (is 'contingent' upon) the kind of task performed rather than upon some universal principles which apply to all organisations (Perrow, 1967). The theory embraces the assertion that technology influences are mediated by contextual variables and, as such, are a component of a broader system of organisational changes. While IT can impact corporate strategy internally, regarding its competitiveness and business portfolio IT does not independently influence organisations (Perrow, 1981; Wunnava & Ellis, 2009). Many socio-technical studies which have examined contextual factors such as environmental uncertainty, size, management objectives or

political strategies, have yielded insight into the fact that the technological impact on organisations is contingent on other forces in the organisation. IT impact on the organisation is contingent upon powerful organisational actors, who can make decisions that suit their short-term or temporary views. However, these decisions could prove catastrophic in a disaster situation (Bharadwaj, 2000). For example, two data centres intended for high availability, built next to each other, provide redundancy to each other in mitigating the most obvious risks such as power failure, but should a disaster occur which affects the entire area, both data centres are vulnerable and exposed to the same issues simultaneously.

2.3.3 Systemic model

In the systemic model (also known as the man-made disaster theory), disasters are perceived to emerge from a confluence of conditions, occurrences and/or activities, i.e. a combination of a number of elements which work together and which yield disaster as a combined effect (Dekker et al., 2008). This model is contrary to deterministic theory (sequence-of-event theory) which is rooted in Newtonian visions of cause and effect, i.e. Newton's third law of motion, which states that for every action (force) in nature there is an equal and opposite reaction (Louth, 2011). Numerous theorists have developed disaster models to control the effect (sometimes called excess energy), e.g. airbags in the car, security controls, etc. However, to conceptualise disaster or risk, as energy to be contained or managed using barriers or counter-measures, does not explain the organisational and socio-technical factors behind system breakdown. Because of such limitations, researchers such as Turner started to focus on systemic views, e.g. the man-made disaster model (MacIntosh-Murray & Choo, 2002).

According to Barry Turner, incidents materialise from conditions and occurrences, each necessary and usually related with the pursuit of success which, when combined, are sufficient to trigger failure instead (Turner, 1976; Turner, 1994; Dekker et al., 2008). Thus, Turner looked systemically at more than just the end result: he looked at other elements which contribute to disaster, and acknowledged that disaster was not an end result; instead, disaster was a gradual build-up of conditions, occurrences and/or activities over time. Turner (1976, 1994) explored a succession of ‘man-made disasters’, and observed that they had been preceded by a legacy of warnings which had been disregarded, and which, had they been acted on, would have obviated a disaster. He then postulated a theory that disasters were ‘failures of foresight’, and began a process to explain why warnings go unnoticed (Choo, 2005; Downer, 2010). Turner concluded that disasters were neither chance events nor acts of God, nor were they triggered by a few events or unsafe human acts immediately before the occurrence. He postulated that man-made disasters frequently commence with small, ostensibly trivial, operational and managerial decisions, after which there was an

incubation period. Over a long period problems accumulated, and the organisation's view of itself and how it managed its risks, grew increasingly at odds with the real state of affairs, until this mis-match actually exploded into the open in the form of an accident (Dekker et al., 2008). Turner's Model (Figure 3) focused on describing the sequence of events associated with the development of technological (man-made) disasters (Shaluf et al., 2003b).

Stage I in Figure 3 is the notionally-normal starting point where the company and employees adhere to standards and norms, and operations function as normal. Stage II relates to the incubation period where errors occur and accumulate. Stage III relates to events which serve as warnings which, if not mitigated, lead to stage IV, the onset of a disaster. The rescue and salvage stage (Stage V) refers to activities which bring the organisation to a point where it may resume basic operational functioning, and Stage VI is where activities are focused on attaining full operational business functioning.

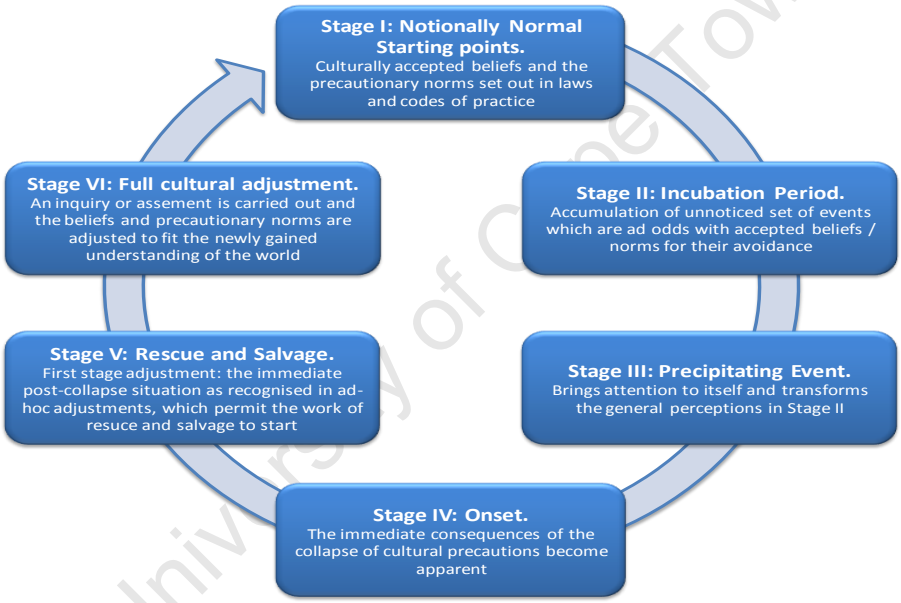

Figure 3. Diagrammatic representation of Turner's Model (compiled from Turner (1976) and Shaluf et al. 2003a).

Turner's model is useful in that it has the potential to highlight insidious risk factors which are more difficult to identify, and which may remain hidden until disaster (false assumptions about reality) strikes (Sullivan & Beach, 2003). It may further serve to specify organisational safety and security cultures, e.g. by highlighting or exposing vulnerabilities. It guides the organisation into taking specific precautions which, if done consistently, yield a culture or norm which is concerned with providing a safe environment (Genserik, 2009).

2.4 Importance of Time and Risk

The concepts of risk and time are two vital factors in defining an integrative IT continuity approach. Risk comprises two factors, namely, the likelihood of the occurrence of an incident, and the impact the incident has when it does occur. These two factors determine the mitigating measures which should be in place to address the IT risk (Helms et al., 2006). Time is mentioned as a by-product in Turner's model; however, the concept of time is important because it is the management of disaster stages over time, one of the central themes of the causes of disaster and its mitigation. Time is a multiplier of loss, e.g. the longer a company is without critical and vital business functions, the greater the costs of the outage, and the less likely the possibility of full recovery (Nelson, 2000). An understanding of how disasters unfold within the specific phases associated with time will aid the planning and corrective actions an organisation must put in place to mitigate or manage down its vulnerabilities.

Disasters or incidents follow typical patterns (MacIntosh-Murray & Choo, 2002). These patterns can be depicted graphically (Figure 4), with the aspect of time being divided into four phases, plotted on the X-axis, and operational level (expressed as a percentage of full operational levels) plotted on the Y-axis (Helms et al., 2006).

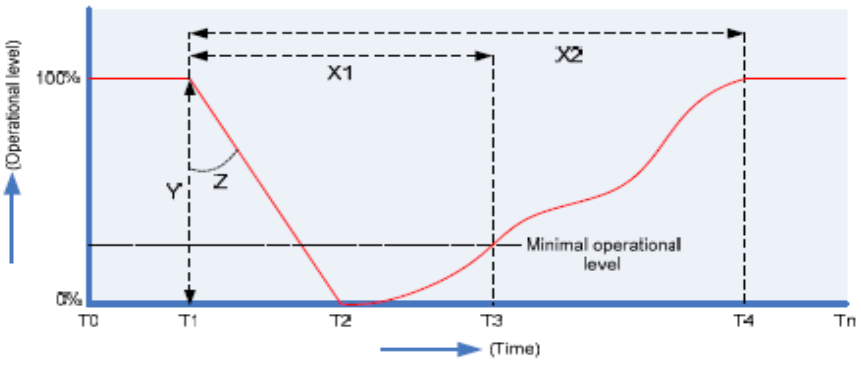

Figure 4. Disaster time-frame (Helms et al., 2006)

T0 -T1 represents normal operations (pre-disaster stage). T1-T2 shows the effect of an event or incident which negatively impacts on the operations of the organisation. If the impact of the incident is of such a nature that the operational level falls below minimal operational level (also known as threshold level) then business operations will cease (triggering event). T2-T3 depicts the effect of those activities which are required to return business operations to above the threshold level so that business activities may resume (disaster stage), and T3-T4 refers to efforts and activities which are required to return business activities to a normal state corresponding to that prior to the incident (post-disaster stage).

The advantage of looking at disasters in time-related stages is to grant the continuity practitioners, researchers, and IT resources the ability to understand more clearly the processes and actions which influence each stage. Depicting the time-frame graphically yields the benefit of understanding where an organisation is at any given time, as well as mapping the consequences of not taking action on time. Phase T0-T1 shows that if the company is in the pre-disaster phase, actions required to mitigate threats should be preventive in nature, i.e. precautionary measures taken to prevent a threat from becoming an incident (e.g. normal operational activities such as backups and restores are required to keep the organisation functioning). Phase T1-T2 illustrates the incident stage where the focus should be on detection, i.e. procedures required to diagnose an incident as soon as it happens, e.g. monitoring the backups, and the alerting processes which should be in place should a backup fail. Phase T2-T3 portrays the damage segment in the time flow, where repression, i.e. the measures to respond to an incident in the early stages to limit the damage, and corrective actions to overcome the incident and recover the damage, are performed. Phase T3-T4 is concerned with the Recovery stage following the incident, where evaluation and correction measures are put in place to increase the amount of knowledge about the incident, e.g. a post-mortem or a root cause analysis of the event.

Lengthy incubation periods (Figure 3, stage II) have the potential to conceal warning signs vital to risk analysis in large-scale systems, and may signify that latent i.e. difficult to notice, embedded, failures can subsist unobserved in systems for extended time periods, diminishing the effective windows of opportunity in which intervention and risk mitigation measures might be introduced (Shaluf, 2008). The Ibrahim-Razi Model (Shaluf et al., 2003c) focuses on the incubation stage and breaks it down into various phases (Figure 5).

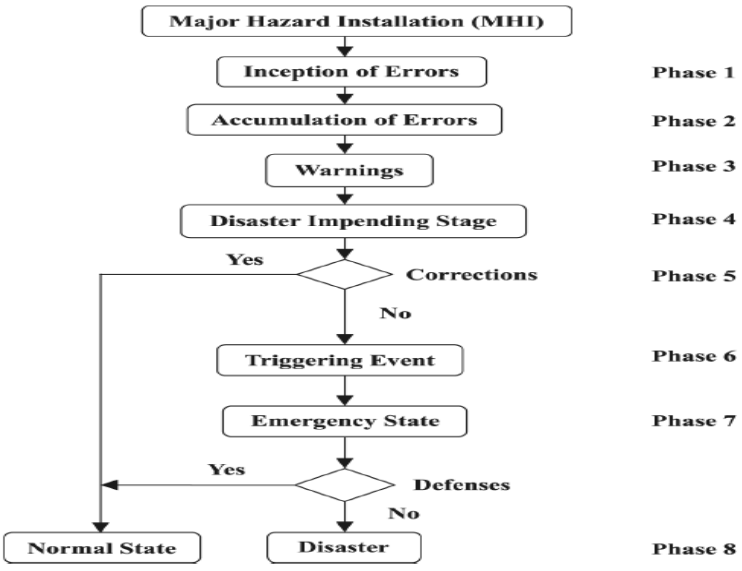

Figure 5. Summary of the Ibrahim-Razi model (Shaluf et al., 2003, 2003c; Shaluf, 2008).

In the Ibrahim-Razi Model the disaster pre-condition is known as the Major Hazard Installation (MHI) comprising phases that precede the technological disaster (the trigger event in Figure 4).

Phase 1 contains the inception of errors which, if unmanaged, accumulate over time (Phase 2). Warning systems will highlight the impending disaster (Phase 3) and, if corrected, the organisation will continue to operate normally. However, if the warnings are ignored and no corrective actions are put in place to fix the errors (Phase 5), an action or mistake will be the trigger to the disaster (Phase 6). The organisation consequently finds itself in the disaster stage or emergency state (Phase 7). If the company has the relevant IT Continuity strategies and plans in place and has made the necessary preparations, it will have the required defences to deal with the emergency and return to a normal state of operations. If, however, the company has made no plans or taken no disaster precautionary efforts, the disaster can plunge the operational levels below the minimal operational level (X1 in Figure 4), and operations can cease.

Using disaster models can be beneficial to companies, as they provide the ability to look at complex events in a simplified manner by differentiating between critical elements. Theoretical models also have the ability to facilitate deeper insight into the situation, and can therefore aid the planning process and the comprehensive completion of disaster management plans (Kelly, 1999). This is especially important because reacting to disasters often has to take place within constrained time limits.

Compared with the Turner Model (Figure 3) which describes disaster as a sequence of stages which included pre-disaster or crisis conditions as part of the escalation or creation of the crisis itself, the Ibrahim-Razi Model is more comprehensive in that it illustrates the actions and reactions within a company which could lead to disasters. The Ibrahim-Razi Model is more practical, because it concisely breaks down the disaster timeline into a set of processes which must be managed. The Ibrahim-Razi Model, however, does not make provision for the causes of errors or the actions which a company may undertake to manage the errors before it reaches the disaster-impending stage.

2.5 Causes of Technological Disasters

IT Continuity as a discipline is ultimately concerned with those mitigating activities that prevent disaster-causing errors to accumulate. The typical major accident does not come into existence fully formed. It comprises preconditions, also known as pathogens, which fall into place over an extended period of time (Werlinger *et.al*, 2009). Factors external to an organisation, such as economic, environmental, political and social factors, are known to cause technological disasters. However, factors internal to an organisation, such as human, organisational and technological (HOT)

factors, can also combine and act together in various permutations during the incubation period (Figure 3, stage II) to yield large-scale incidents and technological disasters (Shrivastava *et.al*, 1988) (Figure 6).

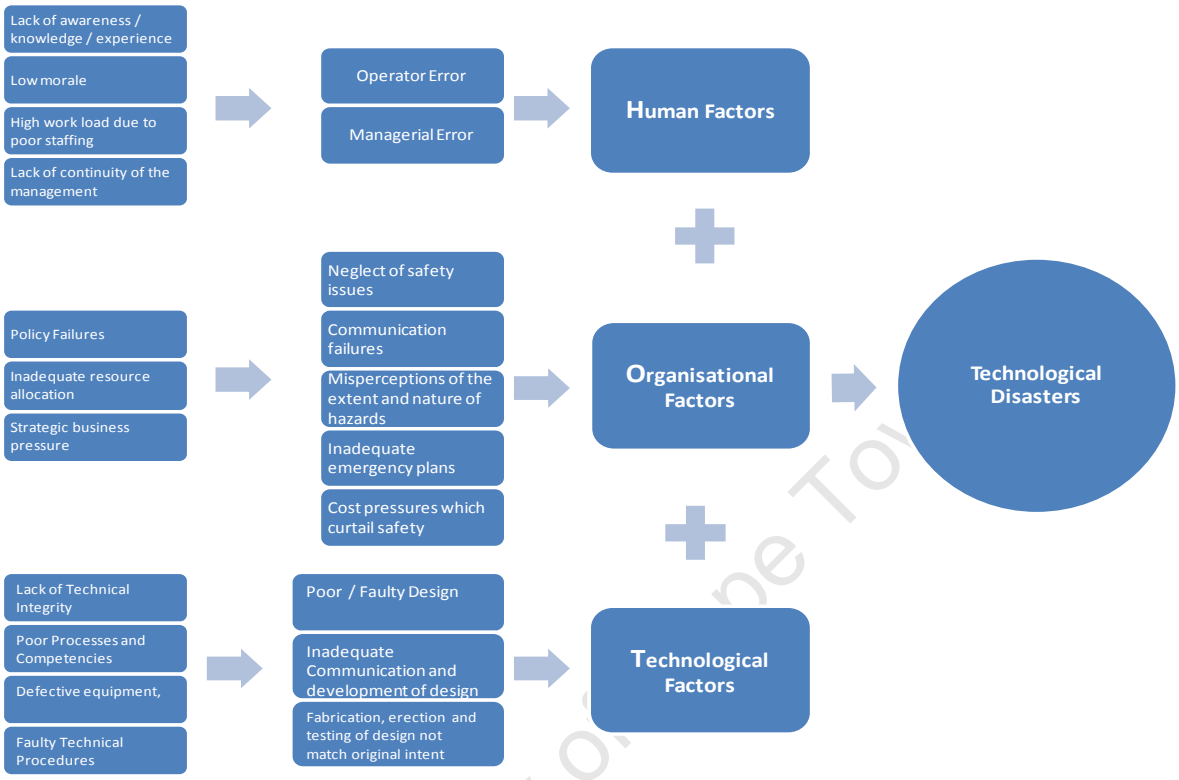

Figure 6. Human, organisational and technological (HOT) factors which cause technological disasters (compiled from Shrivastava et.al., 1988; Shaluf et al., 2003c; Werlinger et.al., 2009)

A multiplicity of minor causes, misperceptions, misunderstandings and miscommunications accumulate unnoticed during the incubation period (Figure 3, stage II). They remain in place in the organisation, ready to contribute to a major failure unless something happens to neutralise them by bringing them out into the open. Until the point at which they combine and react in undesirable ways, misconceptions about the world which such pathogens embody provide elements which are available to contribute to a disaster. They constitute an accident waiting to happen. If they are not uncovered, the pre-conditions are brought together by a trigger which sets off a disaster (Turner, 1994; MacIntosh-Murray & Choo, 2002; Downer, 2010).

Human error (Human factors, Figure 6) is defined as the inappropriate or undesirable human decision or behaviour that reduces, or has the potential for reducing, effectiveness, safety, or system performance. It comprises, but is not limited to, employee morale, number of people staffing each unit, quality of training, and the manager's experience. Organisational inadequacies (Organisational factors, Figure 6) comprise policy failures, insufficient resources allocations, strategic business

pressure leading to a neglect of safety issues, communication breakdowns, etc. Technological factors (Figure 6) enkindle the processes and competencies which are necessary to make sure that communication and development of that design, fabrication, erection and testing match the original intent and intended use (Shaluf et al., 2003c).

The HOT Factor Model (Figure 6) excludes causes of disasters which are external to the organization, such as environmental factors ('Acts of God'), political factors (riots, etc.), social factors (poverty, etc.) and legislation factors. It is a useful model when looking at internal causes of technological disasters. As this study was concerned only with technological (man-made) disasters in the IT sphere, the model is both relevant to the study and an appropriate means of determining the factors relevant to IT continuity within an organisation.

2.5.1 Human Factors

Human factors (Figure 6) which comprise poor control procedures, failure to recognise an incident for what it is, and freezing at crucial decision-making processes, take human operator and managerial errors into account (Richardson, 1994). Human error accounts for 56% of all total system downtime and data loss, and the financial services, manufacturing, telecommunications and healthcare sectors are more at risk than any other (Continuity Central, 2010).

All complex technologies are involved in some form of production, and there are five basic elements to any productive system:

1. decision makers, e.g. architects;
2. line managers, i.e. departmental specialists who implement the operational strategies such as training, sales, maintenance, finance, etc.;
3. pre-conditions, e.g. a skilled and knowledgeable workforce;
4. productive activities, i.e. the temporal and spatial coordination of mechanical and human activities needed to deliver the right product at the right time; and
5. 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 (Reason, 1990).

Therefore fallible decisions are part of the design and management processes, and the focus should be on ensuring that any adverse consequences are detectable and recoverable. Another school of thought highlights the fact that any human errors that may have finally triggered the accident, are themselves the result of problems that have been brewing inside the organisation for a much longer period of time (Dekker et al., 2008).

Prior to a disaster there are many clues which may indicate that a disaster is looming. Examples are management systems that are failing to keep up with operational realities, e.g. toleration of gaps in important information; and a failure to reveal information, or information being available only to members of the organisation who do not understand its significance. Recurring communication issues between diverse specialist departments may stockpile and contribute to a major failure. Rigid hierarchies may serve to impede the course of information and contribute to the wide range of problems which build up during an accident incubation period (Turner, 1994; Shaluf et al., 2002b, 2003c; Shaluf, 2007a, 2008).

People's individual actions are directed by their perceptual paradigms of how things work, i.e. deeply ingrained assumptions, generalisations, or even pictures or images that influence how they understand the world and how they take action. These practices include retention of knowledge which may be out of date and which may no longer be applicable, acceptance of defective sources of information at face value, failure to notice critical information due to poor communication within the workplace, human performance errors, inexperience and cognitive bias (Chapman, 2005). It is the unnoticed accumulation of these "many human errors and failures, too much reliance on an 'old boy' network and some very ill-defined and poor communications" which can lead to technological disasters (Turner, 1976, p.387; Downer, 2010).

When looking at the human factors which can cause recurring problems, several additional factors come into play such as low morale, high workloads due to poor staffing, lack of awareness and/or knowledge and experience (Figure 6). The increasing complexity, rapid change, and growing size of technical systems affects the capability of designers to predict and supply the means to control the relevant disturbances to an acceptable degree of completeness, and consequently the ability of the operating staff to cope with unforeseen and rare disturbances (Rasmussen et al., 1990). These errors are exacerbated by the very human tendency to blame individuals for bad outcomes. Blame is the most tenacious and the most pervasive of harmful effects upon organisational safety (Reason et al., 2001).

The attribution of error to an individual's personality, ability or attitude (careless, silly, stupid, thoughtless, irresponsible, incompetent, or reckless) is one of the chief reasons why people are so ready to accept the phrase human error as an explanation rather than as something that needs further explanation (Funder, 1987; Maruna & Mann, 2006). Just world propositions are based on the belief that bad things happen only to bad people and further drives the blame cycle (Maes, 1994). The hindsight bias—or the knew-it-all-along effect—is the universal human tendency to see past events as somehow more foreseeable than they actually were (Sanna et al., 2002). These

psychological factors are perpetuated in the organisation by two principles, namely the principle of least effort, i.e. human error is the cause of the mishap and hence any further investigation is not required; and the principle of administrative convenience, i.e. restricting the search to the actions of those directly in contact with the mishap. It is therefore possible to limit the blame accordingly and thus minimise any institutional responsibility (Reason et al., 2001).

Disasters are caused by the adversarial concurrence of many causal factors, each one necessary, but singly insufficient to achieve the catastrophic outcome. Although errors and violations of those at the immediate human-system interface often feature predominantly in the post-accident investigations, it is evident that these 'front-line' operators are rarely the principal instigators of system breakdown. Their part is often to provide just those local triggering conditions necessary to manifest systemic weaknesses created by fallible decisions made earlier in the organisational and managerial spheres (Reason, 1990; Tetzlaff, 2001).

2.5.2 Organisational Factors

Organisational failures (Figure 6) look at the organisational shortcomings which contribute to a crisis, and include inadequate resource allocation, strategic business pressures leading to a neglect of safety issues, communication failures, misperceptions of the extent and nature of hazards, inadequate continuity plans and cost pressures (Richardson, 1994; Shaluf et al., 2003c). The organisational domain addresses those factors which impact on the organisation as a whole, e.g. policies and practices, organisational culture, planning and staff participation.

Failures and near misses can be seen as occasions for shame or as incidents to be covered up, but they can also be understood as learning opportunities (Turner, 1994). This latter view is the one best suited for the development of highly reliable operations and for the prevention of disasters. An attitude of openness and a no-blame culture make it possible to treat near-miss incidents as providing information which may improve standards of operation or uncover failure preconditions before they lead to major disasters. In a corporate culture of this kind, there is a greater likelihood that covert ‘pathogens’ will be uncovered and dealt with before they lead to large scale failure. In such a climate, sensibly designed safety audits can also help to improve management practices Turner, 1994). Nelson (2000) reinforced this idea and stated that learning is possible from incidents, but only in an environment which is tolerant of people making mistakes. It is important that lessons are transferred to future incidents, the effectiveness of which may be measured in non-events, i.e. disaster potentials that have been minimised or eliminated.

Common causal features of organisational disasters (Figure 7) are: (a) rigidities in institutional beliefs, which create a particular culture; (b) distracting decoy phenomena; (c) neglect of outside

complaints; (d) multiple information-handling difficulties; (e) exacerbation of the hazards by strangers; (f) failure to comply with regulations; and (g) a tendency to minimise emergent danger (Turner, 1976, 1994; Shaluf et al., 2003a, 2003b, 2003c; Shaluf, 2007a, 2008).

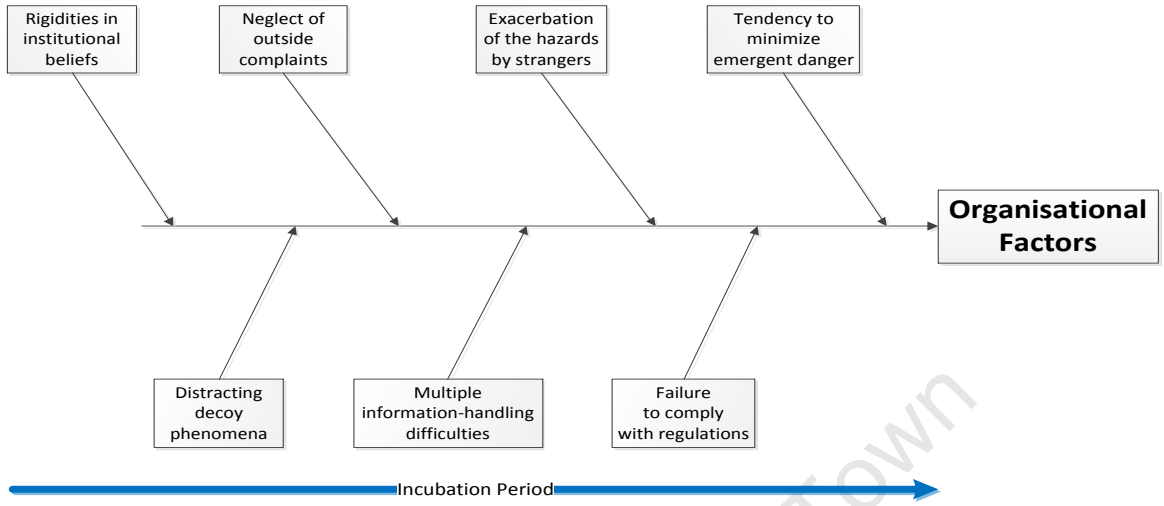

Figure 7. Common causal factors of organisational factors (compiled from Turner, 1976; Shaluf et al., 2003a, 2003b, 2003c; Shaluf, 2007a, 2008))

The 'it won't happen to us' syndrome prevalent in large companies is an example of 'rigidities in institutional beliefs' posited by Turner (1976, 1994). It is this belief, often held by senior management, that the organisation is safe from crisis, which relegates contingency planning to the realm of the unimportant, where preparedness to contain or prevent a crisis is negligible (Nelson, 2000). Bias affects patterns of decision-making and affects the amount of effort taken to solve a problem. Historic and institutional precedents are reinforced by sets of industrial beliefs which give little consideration to preparedness. A situation is therefore reinforced where the perception of potential dangers is dimmed (Turner, 1976). Once this failure of perception is created and structured, it is reinforced by a set of institutional, cultural (or sub-cultural beliefs) and their associated practices (Turner, 1976; Shaluf et al., 2003a, 2003b, 2003c).

All organisations develop within themselves elements of continuous culture which are related to their tasks and their environment (Turner, 1976). A portion of the success of organisations originates from their ability to develop such cultures; however, this very attribute also carries the risk of a collective blindness to issues of great magnitude. The danger is that some vital factors may have been excluded from the framework of bounded rationality. When a widespread and deep-rooted set of beliefs is present within a company, these beliefs sway and guide the viewpoints and opinions of the employees. They may influence the decision-making processes and shape organisational arrangements to the point where it becomes a vicious, self-reinforcing circle, e.g.

where an issue is detrimental, but the belief is held that the area is not important or problematic (Turner, 1971; Shaluf, 2007a, 2008).

In looking at past disasters, Turner (1976, p.384) proposed that the main causal factors of the disasters occurred when "a large complex problem, the limits of which were difficult to specify, was being dealt with by a number of groups and individuals usually operating in separate organisations and separate departments within organisations". This translates to the fact that the necessary knowledge about the procedures is available, but is circulated to a small number of people; hence, the nature of the problem is not generally appreciated.

Self-perception also plays a role in technological disasters (Gopalakrishnan & Okada, 2007), i.e. the perception of the role a department may have in terms of its contribution to preparedness. An example of this is that the business may relegate the responsibility of IT Continuity to the IT department because they perceive themselves not to be technically inclined. Therefore, they do not fully participate in IT Continuity testing, or they are lax about creating test matrices for disaster recovery testing.

Past disasters which have been analysed, have shown how individuals outside the principal organisations highlighted dangers which were dismissed with ambiguous or misleading statements, or subjected to public relations exercises. Such dismissals were based on the assumption that the organisations knew better than outsiders about the hazards of the situations which they were dealing with (Turner, 1976; Gherardi et al., 1999). An example of this statement was Toyota's denial of all culpability in the 2010 accelerator issues which resulted in several fatalities. Despite professional and technical warnings and advice, Toyota only ceded partial accountability once a tribunal pointed out that they had ignored prior expert warnings about the accelerators malfunctioning (Gold, 2010; Wright, 2010).

Patterns of responsibility and awareness of statutory obligations and communications between top management, middle management and operational resources are often lacking (Turner, 1976). The ability to consolidate the information at hand and make the danger visible, is hampered within a complex set of organisational responsibilities and communications. This failure in creative problem-solving is compounded by a passive administrative stance adopted by parties involved, who receive the information necessary to avert the disaster but who fail for a number of reasons to consider it actively. Additional factors exacerbating the failure are the extent to which informal contacts between the community are developed at the expense of more formal procedures, and the extent to

which the need to implement mitigating actions are done, cutting corners because of other work pressures (Turner, 1971; Shaluf, 2007a, 2008).

Wrong or misleading information may be shared between parties, which may originate from interpersonal difficulties, so that information is unintentionally distorted. Even when information is available, it is not always utilised, either because recipients do not attend to it, or because they fail to see its significance (Nakamura & Kijima, 2008).

Failures in the training department could potentially manifest in a myriad of precursors: high workload, undue time pressure, inappropriate perception of hazards, ignorance of the system, and motivational difficulties (Reason, 1990).

Another problem is the failure to see or to appreciate fully the magnitude of some emergent danger. When potential hazards are recognised, they are commonly underestimated; even when the danger is clearly visible, many individuals and groups still undervalue it (Turner, 1971). Ambiguity and disagreement among parties ('strangers') about the status and significance of the evidence pointing to possible danger further contributes to the undervaluing of evidence (Reason et al., 2001). The Toyota accelerator problem (Gold, 2010; Wright, 2010) is an example, where the technical resources had highlighted the defective mechanism, but the decision-makers felt that the probability of the accelerator malfunctioning was low enough to be ignored.

When the full scale of developing danger becomes impossible to ignore, the straightforward act of strengthening precautions is seldom done; instead, individuals often begin to take action to shift the blame, while others seek to take control of the situation by wholly inappropriate means. Managers should be uncompromising in their efforts to seek 'to know what they don't know', to devise reward and incentive systems to identify the cost of failures and the benefits of reliability, to communicate the big picture to everyone, and try to get everyone to communicate with each other about how they fit in the big picture (Roberts et al., 2001).

2.5.3 Technological Factors

In a review of Charles Perrow' theory of Normal Accidents, which states that "catastrophic accidents with high-risk technology systems are inevitable over time if the systems are complex and tightly coupled", Sagan (2004, p.17) notes that "no individual component, human or mechanical, is perfect. We know this, so we load our complex systems with safety devices in the form of buffers, redundancies, circuit breakers, alarms, bells, and whistles. In complex and in tightly coupled systems, however, these redundant safety devices are not independent of one another: The alarm rattles the bell; the bell shatters the whistle; the whistle explodes; and suddenly the whole system

collapses". The human reliability community is tasked with unearthing a method of identifying and neutralising these latent failures before they coalesce with local triggering events to breach the system's defences (Reason, 1990; Tetzlaff, 2001). It is the loading of the systems with these redundant safety measures, e.g. alerting and monitoring software which creates or increases the complexity of the system which could produce hidden common-mode errors, and it is these hidden errors which Turner's theory (1976) refers to as pathogens. Technological problems which include defective equipment and faulty design play a part in the creation and amplification of crisis (Richardson, 1994).

Disasters are expected to grow due to the increasing intricacies of human-made socio-technical systems in modern societies, because there is a bigger chance that a substantial flaw will be built into at least one part of the system. Complex systems are ambiguous, to the extent that those who work in and with them are only partially aware of how the different parts of their system are interlinked (Chapman, 2005).

The barriers to catastrophe which are carefully designed may contain vulnerabilities that no-one has thought of (Swuste, 2007), and these vulnerabilities are sometimes like "holes in slices of Swiss cheese" (Reason, 2000, p.769) (Figure 8). Just as one can sometimes see a hole all the way through even a thick block of Swiss cheese, the little problem gets through all the barriers and becomes a big problem.

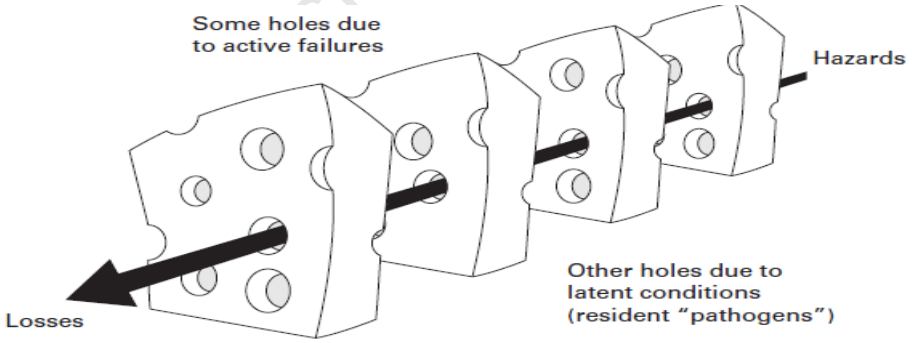

Figure 8. The Swiss cheese model of accident causation (Reason et al., 2001)

What makes this alignment problem particularly difficult to avoid completely is that some holes or vulnerabilities are present all the time, while others may open and close depending on the circumstances. When a problem cascade begins, the holes suddenly line up and a catastrophe occurs (Roberts et al., 2001). The Swiss-cheese model can be used to explain how a process, which had been working for years, seemingly encounters so many issues.

Companies are complex, tightly coupled systems (Reason et al., 2001). Their complexity derives from several factors, the most noteworthy of which is the existence of several defences, barriers,

safeguards, and administrative controls designed to protect potential victims from local hazards. Within systems which are well safeguarded, disasters have a low chance of happening, and thus need help from chance to produce a disaster (Reason, 1990). The more complex the system, the greater the likelihood that defensive gaps and weaknesses will align to create a disaster (Reason et al., 2001).

Companies use redundancy or backup procedures to defend themselves against malfunctions (Keeton et al., 2004). However, these redundant defences may result in a deceptive appreciation of security and an over-confidence in the integrity of the mechanical system. A result of this phenomenon is that companies may ignore the warning signs and alarms, because people associate them with testing or malfunction rather than with genuine emergencies (Chapman, 2005).

Over-confidence has been connected to organisational and group culture in situations where prevailing beliefs, attitudes and norms decrease awareness and responsiveness to risk factors (Chapman, 2005). South Africa is historically not prone to severe natural disasters such as earthquakes, etc., and the Western Cape particularly is not prone to flooding on the scale at which it has affected companies in other parts of the country. Therefore, one of the subsidiary companies of Company X, has opted to have both primary and secondary (backup) systems in adjacent data centres in the same building. This is a huge risk, even though the probability of a natural disaster is low. The executive board of this company has acknowledged and accepted this risk. The absence of huge natural disasters in South Africa has made them less responsive to risk.

In most organised systems, especially technologically complex ones, everything is intertwined; the tighter the intertwining, the more susceptible the system is to disaster if anything goes wrong in any part of the system (Roberts et al., 2001). The propensity for disasters can be viewed as normal because the interdependencies in a system are so great that a small glitch in one place can lead to a large failure somewhere else (Roberts et al.). Root causes of catastrophes are inadvertently embedded in operational systems, latent until an undesirable combination of events occurs. This means that small problems can cascade into disasters if they are not stopped by pre-planned organisational, technical, or procedural defences (Swuste, 2007; Reason, 1990). These pre-planned processes and defences are contained in the holistic management of IT Continuity.

2.6 Disaster Management

Some strategies for disaster management are presented. Shaluf (2008) defines disaster management as a collective term encompassing all aspects of planning for and response to disasters, including

pre-disaster and post-disaster activities. It may refer to the management of the risks and consequences of disasters. Nelson (2000) reinforces this notion, and defines IT Disaster Management as the process of examining the possibilities of losing an IT system and formulating the procedures and strategies to minimise the damage. As elaborated on by Holmes (2010), the definitions encompass several fundamental concepts which are key to the management of disasters, namely: (a) threats, i.e. the identification and reduction of risk; (b) impacts, i.e. the understanding of the consequences of an occurrence; (c) resilience, i.e. the reduction of vulnerabilities to enable the company to survive; (d) response, i.e. the examination of the how of recovery; (e) effective, i.e. whether the recovery solution can be tested; and (f) interests, i.e. the protection of all stakeholder interests.

Mitigation is the collective activity which prevents a disaster, reduces the probability of a disaster happening, or lessens the damaging effects of unavoidable disaster. Preparedness relates to the planning which needs to be done to respond to a disaster. Planning includes the DR exercises and training in which all stakeholders involved in IT Continuity must participate. People need to understand their respective roles, and testing is vital to ensure that the DR plan is realistic and workable. Response enkindles the actions before, during and after a disaster, in order to minimise the impact of the disaster, and is accomplished through the actions taken in response to warnings. Recovery pertains to the immediate and long-term activities undertaken to return organisations to a pre-disaster state or improved state (Shaluf et al., 2003a, 2003b; Shaluf, 2007a, 2008). Mitgation, preparedness, planning, response and recovery can be mapped back to the Ibrahim-Razi Model in Figure 5, i.e. they are the control measures required to manage the steps to prevent a disaster, or to enable efficient recovery from a disaster. Insight Consulting (2008) offered six key principles that enable the management of risk to ensure the continuity of technology and data (Table 1).

Principle	Definition
Protect	Protecting the ITC environment is critical to maintaining the desired levels of availability for an organisation. The services are at threat from environmental failures, hardware failures, operational errors, and malicious attack.
Detect	Detecting incidents at the earliest opportunity will minimise the impact to services, reduce the recovery effort, and preserve the quality of service.
React	Reacting to an incident in the most appropriate manner will enable an efficient recovery and keep any downtime to a minimum. Reacting poorly may result in a minor incident escalating into something more serious.
Recover	Recovery of services should be performed in a controlled and predetermined fashion. Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the quality of data.
Resume	Understanding the recovery priorities as well as the recovery point and recovery time objectives allows the most critical services to be reinstated first. Services of a less critical nature may be reinstated at a later time or in some circumstances not at all.
Return	The process of returning from disaster mode to normal operations is often neglected by organisations. All IT Continuity plans should have an exit strategy that allows them to vacate their ITC disaster recovery centre when the time comes.

Table 1. Six Key Principles of IT Continuity and Definitions (Insight Consulting, 2008)

According to Insight Consulting (2008), the six principles of Protect, Detect, React, Recover, Resume and Return concisely consolidate the entire disaster management cycle phenomenon without introducing redundancy or repetition, or losing any of the important factors. 'Protect' is related to the activities, processes and plans to defend against threats, e.g. backups, so that a secondary copy of the data is always available. 'Detect' relates to the tools and processes put in place to uncover vulnerabilities, e.g. monitoring and alert tools used to detect capacity deficiencies such as running out of memory or storage. 'React' refers to the plans put in place to respond and counter the impacts of a disaster, e.g. the pre-defined procedure the operator has to communicate alerts to the relevant parties to fix, and if they do not, the procedures to escalate the issues. 'Recover' relates to activities which must be performed in a controlled and pre-determined fashion to bring the business processes and systems back to a point of operation. 'Resume' enkindles the activities, plans and documentation used to re-commence business operations, e.g. should the DR environment run out of storage, assess the growth, understand why it was over-subscribed, and put in the necessary mitigations to ensure that storage caters for long-term growth. 'Return' is the process of going back to normal operations and to returning to the facilities which were damaged during the disaster.

Irrespective of which Disaster Management strategy is followed in companies, they all have the benefit of showing, in an ordered and structured manner, where shortcomings in the disaster management Disciplines are, and which can be addressed with appropriate actions.

2.7 IT Continuity Management Model

ITIL (Information Technology Infrastructure Library) and CobiT (Control Objectives for Information and Related Technology) are among the many international standards which explain desirable functions of the IT Continuity unit (Ridley et al., 2004; Saint-Germain, 2005). ITIL for instance, propagates continuous service as the control over IT processes, with the business objective of making sure that IT services are available as needed, and to ensure minimum business impact in the event of a major disruption. It further holds that continuous service is facilitated by putting into practice an operational and tested IT Continuity Plan which is aligned with the complete Business Continuity Plan and the associated business requirements (Heschl, 2006).

IT Continuity operates within a framework encompassing various components such as governance and legal aspects which guide and determine the realm in which it operates (Heschl, 2006). To this end, there are several best practice guidelines promulgated for Continuity Management, e.g.

(a) BS 25999, the British Standard for Business Continuity, which was launched in 2007 and provides a basis for understanding, developing and implementing IT continuity within an organization (Woodman & Kumar, 2009);

(b) The King II/III reports which recommend good corporate governance practices which companies should pursue for the purposes of continuity;
(c) ISO/IEC 27031, an ICT-focused standard on business continuity (Hill & Haslag, 2010; Holmes, 2010).

Effective IT governance practices can be achieved through the application of recognised frameworks, methodologies, continuous assessments and monitoring (Kana et al., 2009). The Hill & Haslag Model (Hill & Haslag, 2010) has been selected to illustrate some key functions of IT Continuity Management (Figure 9).

Figure 9. IT Continuity Management Model as proposed by Hill & Haslag, 2010.

Business Process Analysis (BPA) identifies the critical business functions of the organisation, and seeks to underscore those functions which serve as the life-blood of the company. It must be emphasised that IT Continuity Management can only be effective when it is business-driven, i.e. the Recovery Times Objectives (RTO) and the Recovery Point Objectives (RPO) must be driven by business recovery requirements and not by IT capabilities (Toigi, 2003). IT capabilities should evolve to achieve business recovery requirements (Botha & Von Solms, 2003). The Business Impact Analysis (BIA) identifies the impact a disruption may have on a business, and defines the allowable outage times. It further serves to characterise the impact on critical roles if vital resources are unavailable, and identifies the maximum acceptable period that the resource could be unavailable before unacceptable impacts result (Gregory, 2008). It aids the prevention of losses by issuing warning to business and individuals. The BIA would typically bring to light those critical IT systems or operations which recovery capabilities are insufficient, i.e. do not meet the RTO and RPO of the business. The BIA is valuable, as it uses objective measures to prioritise systems and operations by how urgently they need improved recovery capabilities, which provides a focus for applying limited resources such as personnel and funding (Hiles, 2011).

The Risk Analysis or Assessment (RA) provides protection to the critical business functions identified, and evaluates the threats which serve as risks to those functions, i.e. it identifies the assets, threats, vulnerabilities and counter-measures for each IT service (Helms et al., 2006). It further serves as a plan to implement mitigation strategies to contain the risks. The management of hardware (servers), network, and applications must be done with the appropriate level of diligence. The response to customer requests must be accomplished within acceptable time-lines. Data must always be backed up, and Service Level Agreement (SLA) must be negotiated within the company

among the various business departments. The maximum acceptable level of downtime must be agreed. An important component is setting the standard for critical services, non-critical services and ring-fenced services (which require additional attention), with the ultimate aim of protecting the business from the threat of data loss (Shields, 2009).

Vital to the process is a cost assessment, which should encompass not only the financial aspect of creating a viable continuity framework, but also include the non-financial aspects. Legislation came into effect in South Africa in 2008 and 2009 which pertains particularly to IT continuity (Nielsen, 2008). Executives, who make poor decisions regarding continuity practices which lead to disaster, will be seen as negligent, and such negligence is a criminal offence (Nielsen, 2008). It is this kind of factor which must be taken into the cost assessment, e.g. having the CEO jailed and the impact it has on the share price of the company, brand, loss of customers, etc.

The certification of solutions is not just about compliance, it is about demonstrating recovery readiness and accountability. To re-commence business operations, organisations must have running IT systems, and the business data must be up-to-date and recovered. All the factors of the IT Continuity Model must be taken into consideration, and planned to demonstrate readiness. These plans must be implemented and tested, and if the organisation cannot resume operation within a realistic time (as measured by the RTO and RPO) after a disaster, the continuity plans are inefficient (Best Computer Practices, 2009). The certification process includes the knowledge of procedures, as well as the competence with the recovery software and hardware tools and Interfaces of IT human resources and testing staff (Vision Solutions, 2009).

The 'Develop Enterprise solutions' function recognises that IT Continuity requires an in-depth understanding of the IT services offered in terms of: 1) how the technology works; 2) how the technology is configured; and 3) how the systems are used within the organisation. Without the knowledge of all three domains, a service may not be restored to provide the functionality that was once there (Kadlec & Shropshire, 2009). It is not operational unless it is usable and encompasses all aspects of recovery. The 'Evolve Solutions, Services and Strategies' appreciates that recovery is a continuous process that needs to be maintained and ingrained into the organisation.

2.8 Conceptual Model

Examining how technological disasters are formed, the Turner Model (Figure 3) and the Ibrahim-Razi Model (Figure 5), highlighted areas where disasters may be averted if the necessary actions are taken to mitigate the exposure. In the Turner Model it is found in the precipitating event, and in the Ibrahim-Razi Model it is in the warnings and corrections phases (Phases 3 and 5, respectively). The Human, Organisational and Technological factors at play often hinder corrective actions, to the extent that they allow errors to accumulate. These become repetitive patterns which serve as warnings which, if not corrected, align to create a disaster.

A Conceptual Model (Figure 10) which consolidates concepts discussed in the literature review, such as the causes of disasters, the HOT factors, and the disaster mitigation strategies, has been developed, and forms the basis for the research of this study.

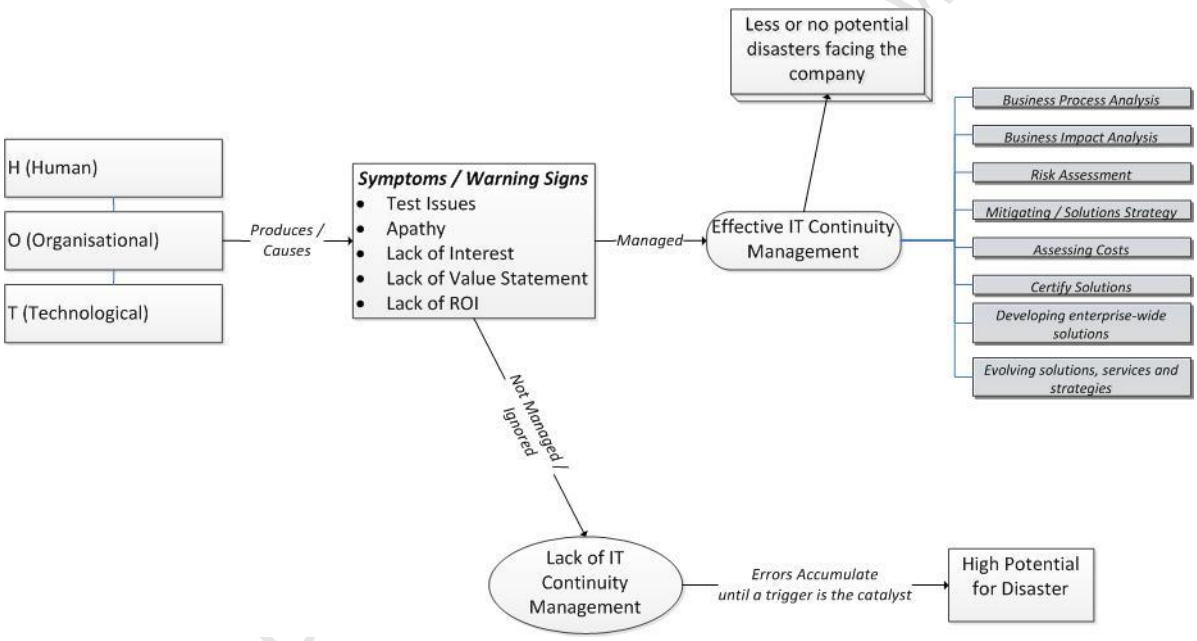

Figure 10. Conceptual Model of the Research (compiled from the Literature Review, Figures 3, 5, 6, and 9)

The Conceptual Model recognises the incubation period (Stage 2 of the Turner Model in Figure 3, and Stages 2-4 of the Ibrahim-Razi Model in Figure5 as the key element which needs to be managed. It is in this phase where unmanaged elements accumulate to trigger disasters. This is the phase where vital warning signs can be misread, evidence can be disregarded or misinterpreted, and where organisations fall into the incompetence trap and learn to do the wrong thing better. This period is characterised by sufficient time for all the minor events to interact and accumulate to produce major system failure (Shaluf et al., 2002b, 2003b; Shaluf, 2008).

An IT disaster is an event, or chain of events, resulting in the inability of an organisation to provide IT services. Disasters often start in a small way with seemingly insignificant operational mishaps and

managerial decisions. There is then an incubation period, and eventually problems accumulate until the organisation's view of itself, and how it manages its risks, grows increasingly at odds with the real state of affairs. Ultimately this mismatch explodes in the form of a disaster. The recurring problems serve as the warning signs, as proposed by the Ibrahim-Razi Model. If these problems remain uncorrected and unmitigated, one trigger event is the catalyst which will plunge the organisation into disaster. These recurring problems are caused by human, organisational and technological factors (HOT factors).

As far as IT disasters are concerned, the mitigation strategies reside in resilience engineering. Resilience is an IT system's ability to effectively adjust to hazardous influences, rather than resist or deflect them. Failure relates to the inability of the system to adapt to and absorb variations, changes, disturbances, disruptions and surprises. The following essential functions of IT continuity management are required to be effective:

a) business process analysis which identifies the critical business functions of the organisation;

b) business impact analysis which identifies the potential harm caused by threats to, and vulnerabilities of, the organisation;

c) performing a risk assessment or analysis for each of the IT services in order to identify the assets, threats, vulnerabilities and counter-measures for each service;

d) planning mitigation strategies and assessing costs;

e) certifying solutions which are not based on compliance, but rather on demonstrating recovery readiness and accountability;

f) developing enterprise-wide solutions which cannot become operational unless they are used and entail all aspects of recovery; and

g) evolving solutions, services and strategies.

Once these IT continuity management processes are in place, the company is then required to build the environment, first by designing the solution, certifying it, and implementing it in accordance with the information yielded by the above mentioned processes. The process is an iterative one, i.e. once HOT factors/issues which service recurring issues are identified, the necessary action, processes and plans need to be implemented in the disaster management life-cycle.

IT Continuity Management can be effective only when it is business-driven. Recovery times and recovery points must be driven by business recovery requirements, not by IT capabilities. IT capabilities should evolve to achieve business recovery requirements. Therefore, recovery is a continuous process that needs to be maintained and entrenched in the organisation.

3. Research Questions

This study seeks to understand the recurring issues within Company X that impede effective IT Continuity Management, what causes them, and how they can be mitigated. The conceptual model (Figure 10) suggests that HOT factors cause warnings or symptoms which, if ignored or mismanaged, lead to a set of recurring issues. The objective, then, is to establish if HOT factors are indeed the cause of recurring issues. The research question can thus be postulated as follows:

- *What are the recurring issues that impede effective IT continuity management at Company X, and what factors cause them?*

The research further seeks to understand what Company X can do to deal with the flaws and limitations that have been exposed during IT Continuity testing and how the organisation can prepare for disasters. The research question can thus be postulated as follows:

- *How can these recurring issues be mitigated?*

3.1 Propositions

The propositions set out below are to test the validity of Human, Organisational and Technological factors in terms of their contribution to recurring issues experienced in IT Continuity within Company X. The HOT factors interact with each other and influence the justification and success of IT Continuity efforts in Company X. The company name has been withheld due to privacy issues. A representation of the link between research propositions to the literature on HOT issues may be found in Appendix B.

3.1.1 Human Factor Propositions

Human error is defined as the inappropriate or undesirable human decision or behaviour that has the potential for increasing disasters (Turner, 1976; Choo, 2005; Dekker et al., 2008; Werlinger et al., 2009). It is comprised of, but not limited to, employee morale, the number of people staffing each unit, the quality of training, and the manager's experience. The human factor propositions relate to the recurring experiences within the company and are illustrated below.

Proposition 3.1.1.1: Credibility

The concept of credibility is borrowed from the open source community, where product gurus and large corporates lend credibility to open source products to the extent that companies adopt them (Glass, 2004; Ven & Verelst, 2006). The concept of credibility was used in this study to test if senior management professing a strong business continuity ethos lend credibility to the IT Continuity unit

in Company X, i.e. is apathy attributed to a lack of management support? The proposition can thus be postulated as follows:

- Where there is an observed credibility bestowed on IT Continuity via the support of senior management, it increases the propensity in lower management to adopt an interest in IT Continuity efforts.

Proposition 3.1.1.2: Terms of Reference

Apathy regarding IT Continuity is a recurring problem in Company X and, according to Shaw et al. (2004), not until a disaster happens and severe losses are experienced do people realise the need for disaster preparedness. The study tested whether the mental paradigms of people are only attuned to disaster preparedness if they have previously been affected by a disaster; and conversely, that the lack of previous exposure to disaster events results in an inadequate allocation of time and resources and incomplete/ineffective continuity plans.

- The lack of previous exposure to disaster events puts the concept far out of reach of people's understanding and terms of reference, and this negatively influences the attitude and effort toward IT Continuity.

3.1.2 Organisational Factor Propositions

Organisational inadequacies are comprised of policy failures, insufficient resources allocations, strategic business pressure leading to a neglect of safety issues, communication breakdowns etc. The organisational factor propositions relate to the recurring experiences within the company and are illustrated below.

Proposition 3.1.2.1: Available Resources

Available resources (also known as slack) comprise two factors: human, i.e. the resources have the time available (slack time), and financial, i.e. the budget has additional capacity to explore, invest in, and adopt technologies (Zhu et al., 2003; Dedrick et al., 2004). Slack relates to the Business Analysis, Business Impact Analysis, Cost Assessment and Risk Assessment phase of the IT Continuity Management Model (Figure 9). The study explores the concept of slack, which has traditionally been used in the technology innovation, to understand how slack correlates with IT Continuity. Since available resources, e.g. resources do not have the time to dedicate to IT Continuity efforts, is a recurring feature in Company X, the thinking behind this concept is to understand if proper IT Continuity Management, as depicted in the Conceptual Model (Figure 10), is dependent on slack in the organisation to ensure that resources are available to commit to the necessary work effort required. The proposition can thus be postulated as follows:

- The greater the degree of available slack, the greater the propensity of a coherent IT Continuity effort in the company.

Proposition 3.1.2.2: Legislation and Standards

Legislation imposes mandatory adherence to, and implementation of, IT Continuity. It is prescriptive in imposing mandatory adherence, but offers no guidance on implementation. While the literature is rich in providing statistical sources regarding the lack of interest in IT Continuity displayed by companies, it is scarce in supplying the underlying reasons behind the lack of interest displayed. Reinforcing this problem statement is the fact that, because we have no view as to why this problem exists, we thus cannot treat or rectify it. Hence we are left to speculate at the apparent reasons, be they lack of government involvement and not promulgating the appropriate laws, lack of industry standards and best practice guidance (or the extremely high number of standards and best practices), or whether people in the IT industry are simply ignoring them (Honour, 2007). The study examined whether the lack of implementation guidance by the various IT Continuity standards negatively influences the stance Company X takes in adopting, implementing and enforcing IT Continuity practices, and is postulated as follows:

- The many available best practices in IT Continuity, e.g. ITIL, CoBIT, ISO, BS99100, obscure companies and negatively impact on the propensity to enforce IT Continuity standards properly.

Proposition 3.1.2.3: Cost Justification

IT Continuity faces many obstacles, the most prominent being that, similar to life insurance, IT Continuity is a “grudge” insurance (Regensberg, 2008, p.8; Vision Solutions, 2009). It is very difficult to prove a Return on Investment (ROI) because IT Continuity is viewed as a budget overhead, protecting against something that may never happen and not contributing directly to ‘the bottom-line’. Of the values that IT Continuity delivers, ROI is the most tenuous and difficult to quantify, and the insurance benefit of a continuity investment is earned only if a disaster occurs (Schopp et al., 2006).

- The difficultly in justifying the costs of IT Continuity or proving Return on Investment negatively impacts on IT Continuity’s ability to secure funding for investments in information availability.

3.1.3 Technological Factor Propositions

Technological factors enkindle the processes which are necessary to ensure that the design, build, implementation and testing of technology match the original intent and intended use. Since the majority of recurring problems emerge during testing (when the greatest focus is placed on IT Continuity efforts in the company), the technological factor propositions explored are an impediment to IT Continuity efforts.

Proposition 3.1.3.1: Compatibility and Complexity

Compatibility and complexity speak to the 'Develop Enterprise solutions' in the IT Continuity Management Model (Figure 9). End of Life (EOL) Technology, i.e. technology which has reached its full depreciation cycle in production, e.g. 4 years for a server, is used in the Remote Data Centre (RDC), and therefore the infrastructure is old. In addition, the capacity in the RDC is about 80% of that in production. Thus testing is not always on like-for-like technology (servers of a later generation in production). This introduces a level of complexity. The study determined whether compatibility and complexity influenced the propensity of resources to embrace IT Continuity efforts, i.e. were these factors inhibitors to the processes and competencies necessary for the effective management of IT Continuity? The relationship is stated below:

- The greater the Compatibility with existing technologies, skills and tasks, the greater the propensity to adopt IT Continuity measures. Where the technology is considered an appropriate fit for the task, it influences the decision to adopt positively.

Proposition 3.1.3.2: Trialability/Testability

As stated in the IT Continuity Management Model (Figure 9), the 'Evolve Solutions, services and strategies' phase appreciates that recovery is a continuous process that needs to be maintained. Trialability (also known as testability) is the demonstration of recovery readiness and accountability ('Certify Solutions' phase in the IT Continuity Management Model (Figure 9)). The study undertook to understand whether trialability enables Company X to learn and understand the functionality of the hardware and software, thereby removing a significant amount of risk from the software development lifecycle process, consequently allowing for a deeper understanding of both the software and the requirements (Guliani & Woods, 2005). The Remote Data Centre (RDC) IT Continuity tests are conducted bi-annually and, because the Mainframe in the Remote Data Centre is unavailable outside of these slots, testing between the RDC tests is not possible. This study would like to further examine the correlation between the ability to test and the attitude toward IT Continuity.

- IT Continuity is more likely to be adopted if technologies can be tried and assimilated in small portions over time.

4. Overview of the company

Company X is one of South Africa's leading financial services groups. The company has its main operations at a central campus where two adjacent data centres, providing fail-over for each other, are housed in the same building. It has a remote data centre facility in Midrand. The company has about 6000 resources and annual revenue in excess of R100m. Its vision is to be the leader in wealth creation and protection in South Africa, leading that process in the emerging markets and playing a niche role in the developed markets. Table 3 portrays key metrics of Company X.

Company X has a strong Business Continuity ethos, having an established Business Continuity Advisory Board (BCAB). The Board prescribes minimum standards and requirements for IT Continuity to ensure effective vertical and horizontal disaster recovery abilities, consistent with business priorities, to deal with disasters and related contingencies. The Board meets quarterly, to monitor adherence to IT Continuity efforts, to confirm the adherence to Group Business Continuity standards, to provide a framework for the company to support compliance with Group requirements, and to establish company-specific processes and requirements where necessary.

Until 2009, Company X used Service Provider A as a third party vendor for their disaster recovery solution. In January 2010 Service Provider B took over the Disaster Recovery (DR) services. Both third parties (Service Providers A and B) evaluate their disaster recovery readiness by assessing their ability to keep the mainframe environment running. The disaster recovery site is a 'warm site', the definition of which is that which "provides an environment and basic infrastructure to enable the facility to be reinstated before its absence becomes critical for business survival. It may have most of the equipment required for normal operations except for items that can be supplied quickly from stock" (Hiles, 2011, p.376). A warm site "has systems and communications ready to go, but it requires that data be restored before they are ready to be used" (Wallace & Webber, 2011, p.321).

The study was undertaken during the transition phase between Service Providers A and B, where Service Provider A hosted the infrastructure and Service Provider B provided the DR services. Because this model was based on availability of hardware and not the criticality of applications, disaster recovery readiness appeared deceptively high. In addition to two Remote Data Centre tests performed per annum, Company X also performs two High Availability tests per year to ascertain its Disaster Recovery readiness.

4.1 Overview of the Remote Data Centre (RDC) Test

The main objective of each Remote Data Centre (RDC) Test is to establish current and up-to-date company IT Continuity capability. To accommodate this, bi-annual tests are contracted with the IT Service Providers for the offsite site recovery exercise.

The Remote Data Centre (RDC) test is a fully integrated test covering all critical applications hosted in the remote data centre in Midrand. The test involves IT development resources, service providers and business users. Testing is conducted from the Disaster Recovery (DR) laboratory at the Head Office of Company X. The DR laboratory is on an isolated wide area network with 6 megabyte connectivity to the Remote Data Centre in Midrand. It is furnished with sixteen desktop PCs, from which all testing is conducted. In preparation for the DR test, the desktops must be built to accommodate all the user profiles of the various IT and business department resources, incorporating all the software required by these respective parties.

4.1.1 Test Process

Extensive preparation is undertaken for the RDC Test. The current DR test approach is depicted in Figure 11. The Recovery Point Objective (RPO) Service Level Agreement (SLA) is no more than a four-day data loss. Backups to tape are taken twice every a week, on a Wednesday and on a Sunday, ensuring that there will never be a data lag greater than 4 days. The backups are transported to the remote data centre in Midrand on the following day, and the restore of these backup tapes commences on arrival.

Figure 11. The current DR solution in place taken from Company X internal documentation.

At the start of the RDC test, Service Provider A, supporting the RDC facility, brings the mainframe and open systems environment online and prepares the RDC for the test. Once the mainframe is brought online, the database agents restore the Microsoft SQL, UDB and DB2 databases and complete the database restores approximately 18 hours later. Service Provider B then performs health checks of the RDC environment before handing the remote data centre over to the ITC

Coordinator for Company X, who in turn calls in various IT resources to perform their IT Operational Readiness testing. All tests are performed from a dedicated DR laboratory on the main campus of Company X. All sixteen computers in this laboratory are on an isolated wide area network (WAN) and connected to the RDC.

Once the IT teams have signed off their respective environments, the business representatives are called in to perform business testing. For the purposes of the RDC test, business is instructed to prepare all their test cases against the last restore. Business testing runs for a full week from Monday to Friday afternoon at 4pm. A full batch process is performed post business online testing to test the transactions performed during business testing and these results are verified by the business the following Monday morning. Once all business areas have signed off, the ITC coordinator for Company X hands control of the RDC environment back to Service Provider B. Full backups are taken of the production environment on Sunday evening, and these are transported to the remote data centre on Monday. Once the tapes arrive at the remote data centre, the restore starts. This restore is specifically designed to test the Recovery Time Objective (RTO), as the SLA in place currently stipulates a 24 hour recovery in the event of a disaster.

The results of the tests are published in a report released daily during the RDC test, and a summary report of all the critical applications tested during the test is released at the end of each respective RDC test. A sample of the report can be viewed in Table 2. Each application is marked with an RAG indicator (Red: not successful, Amber: partially successful, Green: successful) for 24 hour readiness, i.e. the SLA (Service Level Agreement) with the business that, in the event of a disaster, the application will be ready in 24 hours; and for business readiness, i.e. the RDC test spans 10 days and once the application is brought on line and tested by the respective IT teams it is ready to be handed over to the business testers for testing to ensure data integrity against production data.

Nr	Application	RAG for 24 Hour Readiness	RAG for Business Readiness	Log Number	Issue	Short Term Resolution	Long Term Resolution
1a	Application X			2228863	Issues with Workflow with Case	-SQL DB of workflow resolved -Can sign-on and work but cannot view images (related to the Content Manager DB which is being restored) -Tested successfully	**CAUSE:**Application XYZ Queue Definitions on the Mainframe DR site incorrect **Mitigation:** Add a job to Production Scheduling that will run a job every night to backup these definitions

Table 2. Sample of one of the application areas represented in the daily/summary report (Company X, Internal documentation).

The issues encountered are listed on a high level, and the short and long term resolutions are noted with input from the IT Development teams. The report is signed off by the respective application

area managers to confirm the integrity of the report and to take responsibility for the corrective actions which stem from the report.

4.2 Overview of the High Availability (HA) Test

Company X has two data centres adjacent to each other, in one building. The focus of the HA test is on the fail-over capabilities of the critical applications (open systems) deployed in a high availability cluster. The primary nodes of all these applications are deliberately shut down to force the secondary nodes to take control as primary nodes, irrespective of whether the primary node is resident in Data Centre 1 or Data Centre 2. The HA test includes environments that are not clustered and are configured on Virtual Machines. In addition, all components which support the critical applications must also be tested, e.g. network, telephony, etc. This recovery exercise is a functional test only, and no stress testing or load testing is included. The metric for determining the success of this exercise is whether there is a 100% recovery success rate of the different production services, of interconnectivity, and of recovery time.

Testing for HA purposes is conducted on site from the IT and business users' workstations. HA tests are conducted on a Sunday to avoid minimum interruption to the production availability of systems. The HA test is run in controlled and predetermined fashion within stringent time-lines (as there is only one day in which to fail the systems to the secondary data centre and test on both IT and business levels; and fail-back to the primary data centre and test on both IT and business levels to ensure that the production landscape is ready for business on Monday).

4.3 Overview of RDC and HA testing management

For the duration of each test (both RDC and HA), a dedicated helpdesk resource captures all incidents, issues and problems in a problem-management tool. Each issue is logged against a particularly category, be it a server issue, a database issue, etc. Reporting is done at the end of each day for the duration of the test. At the end of the test a summary report is generated in which all the issues experienced during the test period are recorded. A post-mortem is held after each test, the results of which are included in the research, and this includes the participants' comments and/or suggestions for improvement. The IT continuity test results may change over time from test to test, and may therefore yield different results.

4.4 RDC and HA test preparations

Planning for a remote data centre or high availability test starts approximately five months prior to the test. Meetings are held with the architects, service line managers and service providers to determine the scope of the tests. These interactions yield a scope document, which is presented to

the heads of the respective service lines, e.g. head of data centre, head of telecommunications (including network services), head of security, head of architecture and planning, and head of operations. These service line heads are collectively known as Manco. Manco vets the scope document and confirms the feasibility of the proposed test.

Once the scope document is signed-off, it is distributed to the IT Executives, Portfolio Heads and IT Application Owners. Further detailed planning and amendments are done to the scope document during several iterations of meetings. Actions in preparation of the tests are confirmed, e.g. confirming backup and restore instructions, and issues stemming from previous tests are highlighted to ensure ownership has been assigned and issues are able to be mitigated. IT Application owners have the responsibility of informing their respective teams (IT Development) of the test, contracting the resources that participate in the test, and ensuring responsibility for the actions in preparation of the test.

The IT Executives are the custodians of all the applications, i.e. they ensure that the applications defined by business as being critical are covered in the scope of the test and, where the applications are out of scope or failed in a previous test, etc., ensure that these are either raised on a risk register or that the relevant pressure is applied to IT Development to ensure that the application is included in the test. The service providers who supply the services ensure that the respective environments are ready for the test, e.g. that the data centre is ready, the network is available, and the desktops are built and ready. A month prior to the test, the confirmed scope (including all the applications which are included and excluded from scope) and the issues are distributed to the Business Continuity Board, Chief Information Officers of the various companies, and all the above-mentioned parties. This is the final stage in preparation for the tests. All issues at this stage should have defined mitigating actions or corrective actions against them.

On the business side, the project manager liaises with the Business Disaster Recovery Coordinators (BDRs), who contract time and availability with the business testers and ensure that the test cases are prepared. Once the tests are performed and conducted, reports are produced with RAG (Red, Amber, Green) indicators as to how each application has performed during the test. Once a year, following a test, the IT auditors audit IT Continuity and review the test processes. Each audit culminates in a findings list (or log), which must be mitigated before the next test.

5. Research Paradigm and Methodology

5.1 Research Paradigm

5.1.1 Strategy

The Case Study research method was chosen because it has seen extensive application in Information Systems (IS), and because the approach seeks to understand the problem of recurring issues within IT Continuity being investigated (Gable, 1994). Case Study strategy provided the opportunity to ask penetrating questions and to capture the richness of the organisational behaviour. Case Study was used to explore causation of recurring issues within IT Continuity in Company X. The method provided a systematic approach to looking at events, collecting data, analysing information, and reporting findings, and its results aided the researcher in gaining a refined insight into why the recurring issues were being experienced test after test.

Case study was deemed the most appropriate method because it is concerned with how and why things happen, which allowed the investigation of contextual realities as well as the differences between what was planned and what actually occurred, namely:

(1) the study of information systems in their natural setting. Thus the resources could be observed in the laboratory during the RDC test, on the existing infrastructure.

(2) The method allowed an opportunity to understand the nature and complexity of the process taking place; and

(3) valuable insights could be gained into new topics emerging in the rapidly changing information systems field.

Case Study also allowed examination of the flexibility to retain the holistic characteristics of real life events within the Company X while investigating empirical events. Furthermore, Case Study as a research strategy attempts to examine: (a) a contemporary phenomenon in its real-life context, especially when (b) the boundaries between phenomenon and context are not clearly evident. As an experiment, it deliberately divorces the phenomenon from its context (Yin, 1981). Case Study attempts to explain a phenomenon.

The use of Case Study in Company X was not proposed as a study of the entire organisation. It was intended to focus on particular issues and features within the sphere of IT Continuity. This method enabled the researcher to understand the complex real-life activities in which multiple sources of evidence were used. Case Study is particularly useful when one needs to understand some particular problem or situation in great-depth, and where one can identify cases rich in information (Baharein & Noor, 2008).

Qualitative research implies an emphasis on processes and meanings that are not rigorously examined, measured (if measured at all) in terms of quantity, amount, intensity, or frequency. Hence there are occasions, particularly in the social sciences, where researchers are interested in insight, discovery and interpretation rather than hypothesis testing (Saunders *et al*, 2003). The value in undertaking qualitative research in this context is because relatively little is known about what a given piece of observed behavior means, e.g. apathy to IT Continuity, until Company X has developed a description of the context in which the behaviour takes place, and has attempted to see the behaviour from the perspective of its originator. Such contextual understanding and empathetic objectives are unlikely to be achieved without direct, first-hand, more or less intimate knowledge of the research setting.

The study is cognizant of weaknesses with qualitative research, namely: (1) the inability to manipulate independent variables, (2) the risk of improper interpretation, and (3) the lack of power to randomise. In addition, four corresponding problems with Case Study research add to the criticism: (1) a lack of Controllability, Deductibility, Repeatability and Generalisability (Gable, 1994; Flyvbjerg, 2006).

To counter the above criticisms and to establish rigour, the research was systematic, and employed self-conscious research design, data collection, interpretation, and communication. To this end, the researcher sought to achieve two goals: to create an account of method and data which would stand independently so that another trained researcher could analyse the same data in the same way and come to essentially the same conclusions; and to produce a plausible and coherent explanation of the phenomenon under scrutiny (Mays & Pope, 1995).

Case Study also supports the use of multiple types of evidence, namely by using a combination of qualitative and quantitative evidence. Blending qualitative and quantitative findings could potentially produce useful insights; and there are advantages to mixed-methods research in that it conveys a sense of rigour. The evidence may come from fieldwork, archival records, verbal reports, observations, or any combination of these (Yin, 1981).

5.1.2 Research Philosophy

Positivism is defined as an approach to the creation of knowledge through research which emphasises the model of natural science: the scientist adopts the position of objective researcher, who collects facts about the social world and then builds up an explanation of social life by arranging those facts in a chain of causality (Baharein & Noor, 2008). The philosophy applied was positivist because the research worked with an observable social reality (established by the various models engaged, and by the reality experienced in the IT Continuity unit studied) which could be measured

with the aim of producing law-like generalisations (laws of cause and effect). Mere observable phenomena can yield reliable data, therefore the data collection strategy is aided by usage of existing theory to develop propositions and research questions. This can lead to further development of theory that can be tested by further research. The results were derived from detached interpretations of the data collected, and attempted to be value-free. The models utilised lend the structured methodology required for replication, resulting in the qualitative observations and conclusions.

The research was interpretive because it was also a quest to understand the fundamental meanings which underlie IT Continuity. Trying to ascertain the attitudes of the sample population toward IT continuity would involve interpreting and transposing the results of their responses to a coded framework. Interpretive research focuses on the knowledge of reality gained through social constructions, as well as on the complexity of human sense-making, and highlights that interpretive research does not pre-define dependent and independent variables.

5.1.3 Research Approach

The research approach was deductive because it used the scientific principles of established theory to generate data, i.e. the various models employed shaped the approach adopted to the qualitative research process and to aspects of data analysis. The data gathered was explored and explained the casual relationships between variables, i.e. several models are utilised which offered several propositions and gave context against which a relationship measuring success or failure was derived.

5.1.4 Research Purpose

Explanatory research may be useful in studying processes in companies (Baharein & Noor, 2008). The research is explanatory because it sought to establish relationships between variables, i.e. by looking at the various models proposed, it determines how closely the organisation mirrored and adhered to the processes depicted by the models to achieve the goals of the research.

The research is also exploratory in that it endeavoured to seek new insights into the attitudes toward IT continuity, with the aim of yielding results which could be implemented to change the unfavourable paradigms in which the discipline currently operates. An explanatory Case Study comprises (a) an accurate rendition of the facts of the case, (b) some consideration of alternative explanations of these facts, and (c) a conclusion based on the single explanation that appears most congruent with the facts (Yin, 1981).

5.2 Research Methodology

The research conducted comprised two activities: (1) an analysis of the results of previous RDC and HA tests to establish the extent of recurring ITC testing issues that had been observed in Company X, and (2) a survey to establish the reasons for the recurring issues that had been observed.

5.2.1 Timeframe

The research was longitudinal because it analysed the results of four Remote Data Centre tests (Disaster Recovery tests) and three HA (High Availability) tests, as depicted in Table 3:

Remote Data Centre Test	High Availability Test
October 2009	November 2009
May 2010	May 2010
June 2010	October 2010
November 2010	

Table 3. DR and HA Tests used for the research

5.2.2 Survey Instruments

The instruments to collect data were questionnaires and documentary analysis. The results of seven IT Continuity tests (four Remote Disaster Recovery tests and three High Availability tests), captured in the problem management tool, were extrapolated into Microsoft Excel spreadsheets. These were analysed and yielded a list of recurring issues.

The sources of data used in documentary analysis included scope documents, audit findings, IT Continuity board reports, minutes of meetings, and the IT Continuity policy. The format in which these documents were presented was Microsoft word documents.

The data was recorded in a standardised template to present data for different sample types in a single document. The template contained the purpose of the source document, how it related to the research question and why it was important, and a list of key points covered by each document. The template also included a checklist of factors to ensure that the evidence collected from each sample was complete. Each document type was categorised into components so as to ensure easy accessibility and reference, should the need arise for further clarification and for data capture. The documentary analyses were captured into both Microsoft Word documents and Microsoft Excel spreadsheets (using pivot tables to outline emerging themes).

Documentary sources were important to complement and to compensate for the limitations of other methods. Documentary evidence acted as a system to cross-validate the information gathered from the questionnaire, focus groups and for observation, given that sometimes what people say may be different from what people do. Additionally, the documents provided guidelines in assisting the researcher with the inquiry during discussions. Official and unofficial documents and records

pertaining to the process of testing activities in the organisation were analysed. Thus, corroboration of multiple qualitative techniques for this Case Study research enhance the validity and reliability of findings.

Two qualitative methods were used, namely participant observation and focus groups. Each method used was suited to obtaining a specific type of data. Participants were observed during the Remote Data Centre tests in the DR Laboratory as well as during the on-site HA tests. This method was appropriate for collecting data on naturally-occurring behaviours in their usual contexts, allowing the researcher to observe both IT and business users during the tests. Initially, IT operational readiness testing is concluded with sign-off a test checklist to signal that systems have been brought up and that they are ready for hand over to business testing. Business testing then commences and concludes with a sign-off sheet on which comments could be entered. The researcher was able to take note of both verbal and written comments during the tests.

Various executive forums served as focus groups to discuss recurring issues. Results of the discussions of the focus groups were captured into Microsoft word documents, and transposed into the standardised template developed for this study (Microsoft Excel spreadsheets).

The Questionnaire was developed to understand why recurring issues were experienced, and distributed in Microsoft Excel. The findings were captured into the standardised template developed for this study (Microsoft Excel spreadsheets). Results of the questionnaire were reflected back to various executive forums in Microsoft Powerpoint presentations, and in various board reports in Microsoft Word documents.

In addition, participants were observed during the respective tests, and the results of these observations were captured into Microsoft Excel spreadsheets. This was effective in eliciting data on the cultural norms of the group and in generating broad overviews of issues of concern to the cultural groups or sub-groups represented.

5.2.2.1 Development of the Questionnaire

To understand what the underlying causes of the HOT factors were, a questionnaire (Appendix C) was distributed to a portion of the sample population, as described in Table 5. Each of the questions in the questionnaire was designed to provide insight into the research questions and the propositions stated earlier. In most cases the questions could also be mapped to an HOT factor. Table 4 shows the mapping of the research questions and propositions, and also expounds on the rationale for each particular question.

Table 4. The mapping of the questions on the Questionnaire to the research questions, propositions and HOT factor categories together with the rationale for each question

Nr	Question	Research Question (RQ)	HOT Factor
1	Why do we experience recurring issues during DCN and HA tests and how do we prevent these from occurring in future?	RQ 1	-
2	Which factors contribute to resources not taking corrective actions which stem from previous DCN / HA tests?	RQ 1	-
12	What must we stop doing? What must we continue doing? What must we start doing?	RQ 2	-

Questions 1 and 2 stem directly from the Research Question: What are the recurring issues that impede effective IT Continuity Management at Company X, and what factors cause them?

Question 12 is based on the popular 'Stop/Start/Continue Model' which is often used with teams and individuals (Mills Consulting Group, 2005, pg. 1). It is an effective way to identify and move individuals from positions that are creating some level of conflict or have become obstacles to performance (Mills Consulting Group, 2005). In this context, it aims to solicit input on how recurring issues could be mitigated.

Nr	Question	Proposition	HOT Factor
3	IT Continuity is viewed as an overhead, protecting against something that may never happen and not contributing directly to 'the bottom-line'. In your view, why is this statement justified / not justified?	3.1.2.3: Cost Justification	Organisational

Question 3 was postulated in an open-ended manner to elicit the underlying attitude of the respondent toward IT Continuity. The idea was to extract a view of whether justification differed per organisational level, i.e. did management perhaps have a different view from that of the IT developers, and would this then perhaps have had some kind of an impact?

Nr	Question	Proposition	HOT Factor
4	Remote Data Centre: End of Life (EOL) Technology is used in DCN and thus the infrastructure is quite old. Thus testing is not always like-on-like technology (servers of a later generation in production). What is your opinion of the statement and how does it impact on you?	3.1.3.1: Compatibility and Complexity	Technological

Question 4 concerns the issue of whether compatibility (like-on-like technology) introduces a level of complexity (additional effort required because the environments are not the same) to testing, and whether this additional effort has influenced the participants' view of participation in the test. The question was phrased to solicit an opinion.

Nr	Question	Proposition	HOT Factor
5	In your experience / view, what are the frustrations with IT Continuity?	3.1.2.1: Available Resources	Organisational

The negative, open-ended way in which Question 5 was presented had the objective of eliciting all frustrations the testers experienced in order to determine in how many cases lack of time and money would be highlighted as obstacles.

Nr	Question	Proposition	HOT Factor
6	What must be done to alleviate the frustrations? i.e. How can we improve your experience with Continuity? How do we increase the focus and commitment to Continuity efforts?	3.1.2.1: Available Resources	Organisational

Question 6 also relates to the proposition around available resources, but, in contrast to Question 5, it was phrased in a positive manner to establish what change was needed in the organisation to remove obstacles and change the mind-set toward Continuity efforts?

Nr	Question	Proposition	HOT Factor
7	What is your manager's view of IT Continuity efforts? How does this impact on / influence your outlook toward continuity efforts?	3.1.1.1: Credibility	Human

Question 7 was developed around the concept of whether management lend credibility to IT Continuity, i.e. if the manager was well disposed toward IT continuity, did it automatically infer that staff would be well disposed toward continuity efforts? It also attempted to see if there were discrepancies between levels of management, and how their staff performed.

Nr	Question	Proposition	HOT Factor
8	Have you ever experienced a disaster?	3.1.1.2: Terms of Reference	**Human**

Question 8 was developed to see if experience of a disaster influenced disposition towards IT continuity efforts. Thus, the answer to this question has been relayed back to previous answers to establish a relationship between experience of a disaster and attitude.

Nr	Question	Proposition	HOT Factor
9	Is IT Continuity justified?	3.1.1.2: Terms of Reference	Human

Question 9 was posed to counter the cost aspect of IT continuity, i.e. was continuity important to the company beyond the cost factor? It was also positioned around the opportunity cost of effort on IT continuity versus the ability to spend time on other activities such as production matters.

Nr	Question	Proposition	HOT Factor
10	The DCN tests are bi-annual and because the Mainframe is unavailable outside of these slots, testing between these phases is not possible. What impact does this have on you?	3.1.3.2: Trialability / Testability	Technological

Question 10 was developed to find out if the inability to test outside of designated test slots had an impact on the focus on IT continuity. The aim was to understand if the 6-month gap between tests in

any way influenced the fact that people did not take corrective actions post-tests, whether it related to apathy, or were the gaps between tests too long to keep the momentum going in IT Continuity.

Nr	Question	Propositions	HOT Factor
11	Do you receive the necessary support during tests from vendors, managers etc. If not, please substantiate your answer	Proposition 3.1.2.1: Available Resources	Organisational

Question 11 related to the availability of support from managers and from service providers during tests, from an operational perspective.

Nr	Question	Propositions	HOT Factor
13	"IT Continuity is mandatory and the company can be fined if we do not adhere"…are you aware of policies, SLA's etc.? If not, what must be done to ensure that such awareness is raised?	Proposition 3.1.2.2: Legislation and Standards	Organisational

Question 13 was developed to try to understand what the level of awareness was around the governance of IT continuity, and to understand if people were aware of the repercussions to the company and management in their personal capacities if the company did not adhere to continuity practices.

5.2.3 Sample and Target Population

Purposive sampling was used in this research as a sampling strategy. Participants in the research were identified by the management of each department based on their job responsibilities, position, and involvement in IT Continuity. Additional respondents were also selected on the basis of the researcher's individual judgment on the grounds that they could provide the necessary information needed for the research. The research targeted people who had direct links with IT Continuity in the capacity of providing services, had a dependency on the services rendered by IT Continuity and who could, based on experience, provide valuable and relevant input to the research. The research thus also identified specific groups of people who either possessed characteristics or circumstances relevant to the social phenomenon being studied. Informants were identified because they enabled exploration of a particular aspect of behaviour relevant to the research.

Table 5 depicts the representation of the population which was reached for the purposes of this research. They were chosen based on position (depth within IT/business) and from a horizontal perspective to include both IT and the business. In addition they had been chosen based on their involvement with disaster recovery tests and IT Continuity efforts, whether they had direct dependency on IT continuity or provided a service to IT continuity.

Role	Staff Compliment	Designation / Reason
IT Executives	3	The main role of the IT executives is to assist with the desired positioning of IT as a business partner to Company X. They represent both IT in business, and business in IT. They ensure that IT understands the business requirements and that business understands the IT capacity and capabilities.
IT Portfolio Heads	3	Heads of IT Development Departments
CIO's	4	Chief Information Officers, who are the Heads of the IT Execs, IT Portfolio Heads and the Services Line Managers.
IT Application Owners	15	IT Managers within various application areas and infrastructure domains.
IT Developers	20	Developers of code, support the infrastructure etc.
Business Disaster Recovery Coordinators (BDR's)	15	Representatives within the business units with the added responsibility of coordinating the testers / business expectations around anything Disaster Recovery related especially with the bi-annual Remote Disaster Recovery tests and High Availability tests
Project Managers	1	Project Manager involved with the bi-annual Remote Disaster Recovery tests and High Availability tests
Testers	30	Testers who test business data in bi-annual Remote Disaster Recovery tests and High Availability tests
Architects	2	Architects for Disaster Recovery
Service Line Managers	9	Managers of the various Service streams. All have some dependency on DR and have some contribution to DR in terms of DR e.g. the network, data centre infrastructure, design etc.
Risk	2	Risk Managers who typically assess and monitor the risks to the company and have input into DR
IT Internal Auditor	2	Perform audits on IT Continuity
Business Continuity Board	5	Board Members who are the custodians of Business Continuity for the company
Service providers	3	Provide Services, Hardware and Network Connectivity within the Data centres as well from head office to the Remote Disaster Recovery site in Johannesburg
Manco	9	Management Company of the department which provides IT services to the company (and subsidiary companies). IT Continuity is a stream in Architecture and Planning portfolio.
Total	**144**	

Table 5. Sample employed in the research

Engagement with resources occurred on several levels, before and during the tests in discussions, via the questionnaires, and in follow-up meetings post the findings. Several rounds of verification were done with IT Management to ensure that the results of the test (as depicted in the study) were representative of the recurring issues experienced. The findings were also discussed at this level to ensure that the results were reflected fairly and without bias. Questionnaires were distributed to Service providers, Service Line Managers, IT Development and Application Owners. Results of the questionnaire were presented to focus groups for discussion (Manco and IT Portfolio Heads) and then deciphered and presented to IT Executives, the Business Continuity Board and the respective CIOs.

Initially, data was gathered employing Participant Observation, where the researcher observed phenomena of interest in the environment studied, to draw information which was not obtainable

from other methods. These observations came from the Remote Data Centre and High Availability tests, where resources participating in these tests were observed and notes taken regarding the experiences and attitudes. What had been observed by the researcher was related to the physical setting and environment within which the test activities took place. Observation generated insight and better understanding on the phenomenon under study.

In quantitative research the concern with similarity and difference leads to the use of statistical sampling so as to maximise external validity or generalisability. Hence, Purposive or Judgmental sampling enabled the selection of cases which were particularly informative to the research. In the case of this research, Company X was used and chosen based on the fact that the Company has strong senior management commitment to IT Continuity: it does regular tests and subscribes to all the best practices as prescribed by COBIT and ITIL. This approach best enabled the research questions to be answered appropriately, and enabled the objectives of the research to be met.

A homogeneous sampling strategy, or non-probabilistic sampling strategy, was employed to focus on particular sub-groups within the organisation, where the sample members are similar so as to add depth and commonality across the case study. The sample was geographically clustered, as all participants in this research are confined to one location within one company. To maintain rigour, these participants were chosen to provide the raw material for a comparative analysis, based on the fact that they are theoretically informed and hence relevant to the research questions.

Consideration was given to the issues of Bias and Representativeness, which were mitigated by including a broad spectrum of people from various disciplines, various business units and various interests in the research, thus mitigating the bias which stems from selecting a sample based on convenience. From an ethics perspective, the research was not biased in terms of gender, race/ethnicity, age, location or any other aspect. The characteristics of the participants involved in the research were company employees, ranging from age 18 to retirement age.

5.2.4 Types of Data and Analysis

The first round of data analysis entailed deriving the recurring issues from the reports generated post the Remote Data Centre tests and High Availability tests. All issues logged during the tests, as well as those issues highlighted in the reports stemming from the tests, were captured in Microsoft Excel spreadsheets and categorised according to the incidents logged on the Problem Management Tool (a tool used to manage the incident flow in Company X). A sample of the report generated by the Problem Management Tool can be seen in Appendix A. Each issue then underwent an analysis process to map them to a HOT factor. The end result yielded a list of issues mapped to HOT factors.

Pivot tables were employed to gain a comparative view between all the tests and thus yielded recurring issues.

Further data analysis was undertaken to establish the link between respondents' replies and the HOT factors. The analysis was aided by concepts borrowed from grounded theory. The three stages and what they entail are depicted in Figure 12. Stage one, Open Coding, refers to dis-aggregation of data into units, i.e. the results of the issues logged on the problem management tool were consolidated and pooled into units across the recovery stack. They were categorised as belonging to hardware, software, network, data, telephony and infrastructure units. The units were further broken down to a more granular level, e.g. in the network unit, items were grouped according to slow network response or active directory issues, etc. Stage two, Axial coding, refers to the process of recognising relationships between categories. In this case, each unit was examined and relationships in the unit were analysed, e.g. if the network response was slow due to a 2 megabyte connection between the Remote Data Centre and Head Office, potential causes such as cost were assigned. Stage three, Selective Coding refers to the integration of categories to align with the research purpose. In the case of this study all the items were assigned to a HOT factor, e.g. cost was an organisational factor. A sample may be seen in Appendix A.

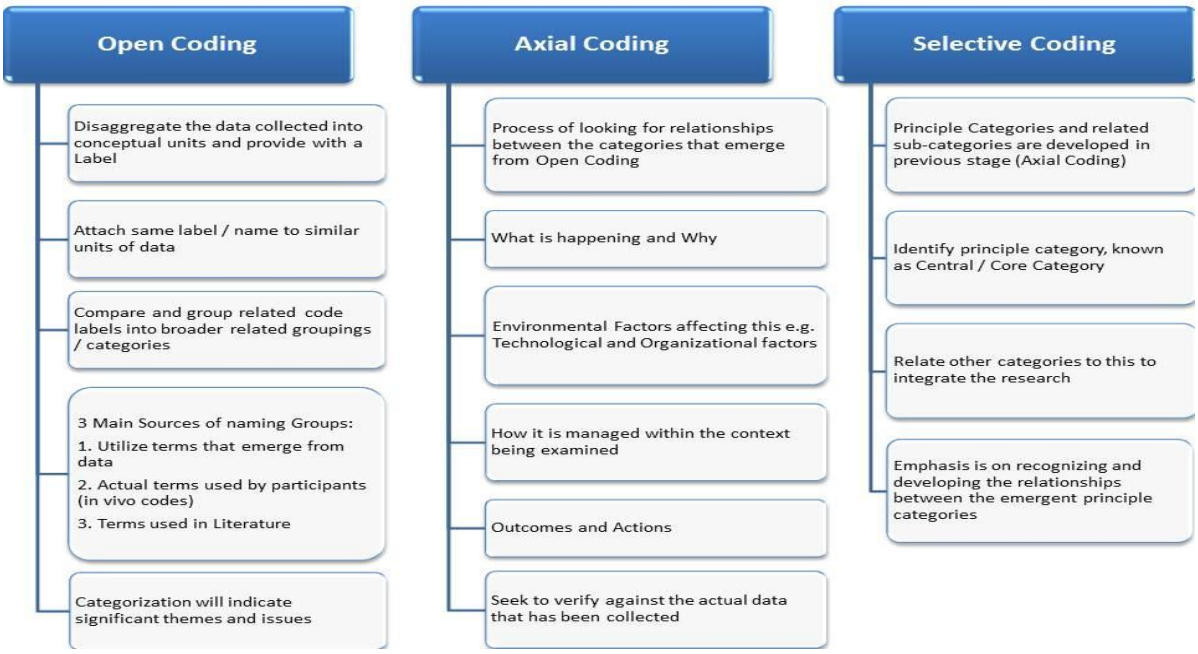

Figure 12. Three stages of coding borrowed from grounded theory

"In quantitative research, the emphasis is on collecting data that lead to dependable answers to important questions, reported in sufficient detail that it has meaning to the reader. The proto-typical qualitative study is the ethnography which helps the reader to understand the definitions of the situation of those studies" (Firestone, 1987, p.17). The main ways in which qualitative researchers

ensure the re-test reliability of their analyses is in maintaining meticulous records of observations, and by documenting the process of analysis in detail (Mays & Pope, 1995).

The data was recorded using various methods, e.g. Microsoft Powerpoint presentations to graphically depict the recurring issues, Microsoft Excel spreadsheets to record questionnaires, and the data collected was stored in a Microsoft Access database. Hard copies were stored in a file and soft copies were stored in a folder on a local drive. Backups were made to an external drive. Access to the data was password-protected, and several other levels of security were imposed, e.g. Windows logon authentication. I foresee no potential problems with storage or access. The data is confidential and hence strict security measures are in place.

In addition, the reliability of the analysis of the qualitative data which emerged from the study was enhanced by organising an independent assessment of the transcripts by additional skilled qualitative researchers (supervisor) and comparing agreement between the participants.

6. Findings

This section contains the findings of comparative year-on-year analysis of the Remote Data Centre and High Availability tests, as well as the findings from a questionnaire which were developed in response to the findings of the tests.

6.1 Remote Data Centre (RDC) and High Availability (HA) Test Results

The results were established by analysing the results of seven IT Continuity tests (four Remote Disaster Recovery tests and three High Availability tests) which enkindle the recovery of the entire IT stack, namely hardware, software, network, etc. All the incidents logged on the Problem Management Tool were extrapolated and analysed, and a comparative analysis was done between the successive years, namely for 2009 and 2010. The data yielded the results as depicted in Figure 13.

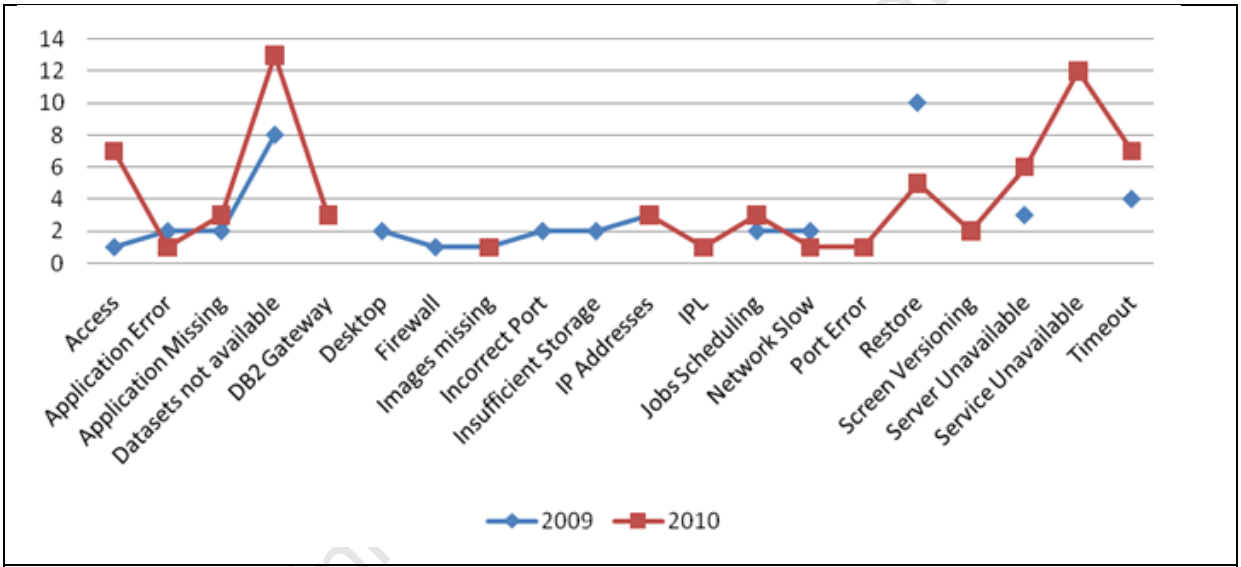

Figure 13. Year-on-Year comparison of issues encountered with the Remote Data Centre and HA Tests

Overall, 2010 fared worse than 2009 in several areas. There were unique issues identified in 2009 and 2010, but more worrying is the fact that the overwhelming majority of incidents reported were recurring issues in 2009 and 2010. The number of incidents reported in 2009 which did not occur in 2010 may have been reduced due to the focus placed on resolving issues prior to the May/November 2010 test. The recurring issues, albeit higher in 2010 than in 2009, are depicted in Table 6:

Unique 2009	Unique 2010	Recurring 2009 and 2010
• Desktop • Firewall • Incorrect ports • Insufficient storage	• DB2 Gateway • IPL of the Mainframe • Port Errors • Screen versioning	• Access to systems (logons etc.) • Application errors • Applications missing • Datasets not available

	• Service Unavailable	• Images missing • IP addresses • Job scheduling issues • Slow network response issues • Servers being unavailable • Timeouts

Table 7. Incidents reported during the RDC tests, year on year comparison

The test results of issues encountered in 2010 are depicted in Figure 14:

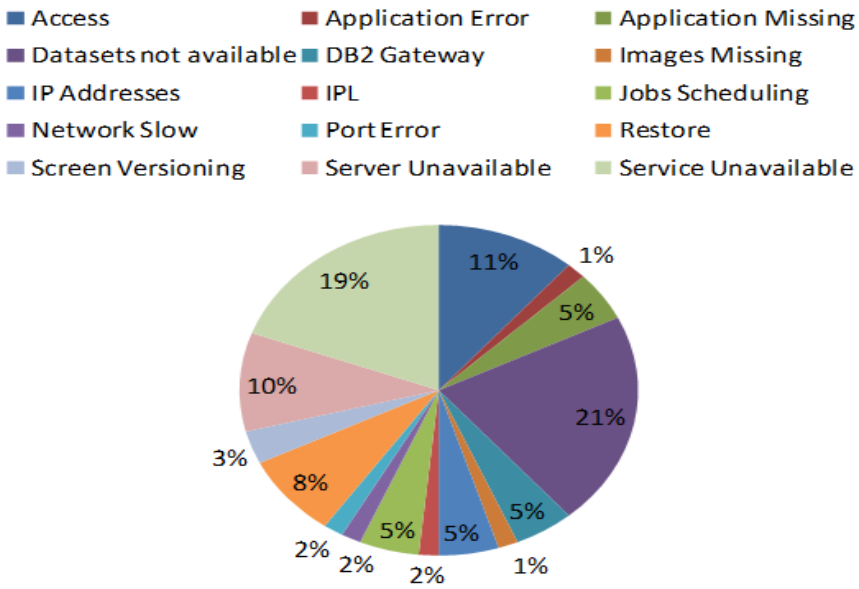

Figure 14. The main issues encountered during 2010

Testing is a critical process which should have enabled Company X to validate the disaster recovery processes, validate the documentation, allow practice for the employees who participate in the RDC and HA tests, and to identify weaknesses in the planning and infrastructure. Recurring issues were sensitive because the premise with which tests were approached was that new issues signaled learning and progress, making the Company more resilient to disasters. Where recurring issues were encountered, it meant that mistakes and errors had been ignored, i.e. we have done nothing to mitigate the issue since the last test and ultimately this means we fail the respective RDC and HA tests.

6.1.1 Recurring response issue

The network response in the DR Lab was extremely slow, to the point that users were unable to login and test. The Company (Head Office) connects to the Remote Data Centre (RDC) via a 2mg line. It could be that this issue was related to the network; alternatively it could have related to the multiple connections the applications make in RDC (the way in which the infrastructure is set up). To resolve the slow response, diagnostic tests were run on the line, i.e. the network service-provider

monitored the network. In addition, although the respective infrastructure teams and the DR architect re-visited the deployment of the hardware in the Remote Data Centre to aid in the resolution of the slow response, neither investigation yielded any insights. The 2mg line was increased to 4mg for the latter (2010) test and, generally, the network response improved. However, two applications struggled to sign-off within the agreed SLA. This was attributed to the decreased capacity in the Remote Data Centre, i.e. the Remote Data Centre has about eighty percent of production capacity.

In 2009 the Company experienced the same problem with an application and, after the network was monitored, they moved the server to an older host, ESX01, which resolved the issue. A Root Cause Analysis yielded no insights into why the application was so slow on the newer host.

6.1.2 Access Issues

Service provider A experienced RACF issues when logging onto the Mainframe and other applications. Both IT Development resources and business users experience issues logging on because of passwords, etc. One of the recurring errors was the fact that the password file was not restored in the RDC. The security issue must be addressed both on the database and desktop space. A process was implemented to schedule an active directory refresh prior to each test, and this partially solved the issues of users and passwords updating in the Remote Data Centre. However, in addition, Application Owners did not submit updated employee codes for people who should have been testing in the DR Lab, and hence these resources were not activated to test.

6.1.3 Documentation/Skill level

Recurring errors make up the bulk of the time delays during testing. The Battlebox currently contains documentation which is not standardised. Errors and rectification methods are not documented, and hence the Battle box documentation is not on par. The fear is that in a real disaster, where the Company could potentially lose key staff, the available staff would not be able to recover applications based on documentation in the Battlebox.

The BIA (Business Impact Analysis) defines the criticality of the application. The problem is that people verbally justify why the application is critical, but nothing concrete exists for any of the legacy systems in the Battlebox to justify why the application is on the critical list.

6.1.4 Apathy to IT Continuity

Extensive focus is placed on giving IT an opportunity to resolve all issues stemming from the RDC tests. A week prior to the Remote Data Centre test, an Active Directory (AD) Refresh is scheduled to

run and complete over two days, giving the IT Development resources 3 days to test the critical applications in the Remote Data Centre. This event is scheduled precisely a week prior to the Remote Data Centre test to resolve any application/security-based problems. Generally the response of the IT Development resources was poor, with only 2 out of 62 application areas (3%) testing if their applications were available. The direct effect is that many of the issues encountered during the Remote Data Centre test could have been mitigated during the AD Refresh if testing had been done as scheduled.

IT operational readiness testing normally commences on a Sunday when Service Provider B hands over the RDC environment to Company X. During the May 2010 test, the RDC environment was handed over to Company X only late on Monday afternoon. Immediate notification was sent to the IT Development resources to commence testing. 27% of IT Development resources started testing immediately, while 73% started testing on Tuesday. The direct impact resulted in delays as resources were not available to test. A secondary spin-off was that, as some areas are dependent on others to complete before starting their tests, their testing was also delayed.

Taking into account the previous RDC tests, an audit finding for 2011 noted that, while technical resources sign off on the IT Operational Readiness testing, there is no evidence of the detail of what they sign off on.

The results of the RDC tests in 2009 and 2010 prompted investigation into the factors which cause recurring issues and the perceived apathy in the IT Continuity environment. Based on the results of the RDC tests, a questionnaire was developed and distributed to 59 resources, from whom 38 responses were received, a return of sixty five percent. This number excludes the audit findings which were also taken into account for the purposes of the study. The results of the respondents were captured, consolidated and analysed. The emergent findings, which are discussed in the next section, were reflected back to the Application Owners, IT Executive Committee, IT Infrastructure Management Committee and the Business Continuity Board for verification.

6.2 Results of the Questionnaire

Based on the results of the comparative year-on-year tests done above, a questionnaire was developed and distributed to participants of the test. The input from the questionnaire was consolidated, analysed and grouped according to emergent themes. The findings of the questionnaire were reflected back to the executive committee for comment, on both a group level and on an individual level. The section below contains the results of these interactions. The following section contains direct quotes from participants in the study, and it was felt that tampering

with the quotes could affect the authenticity of the results, hence there may be grammatical errors in some of the quotes.

6.2.1 Question 1: Why do we experience recurring issues during the RDC tests and how do we prevent these from occurring in future?

Table 7 lists all the factors cited by respondents for the existence of recurring issues during the Remote Data Centre (RDC) tests. The lack of documentation was cited as the top factor for the experience of recurring of issues during DR tests. It seems the lack of visibility into what caused previous issues, how they were mitigated, and what short-term fixes were implemented to negate the issues, are the greatest shortcomings in dealing with issues. One of the respondents succinctly summed-up this sentiment in the statement "we do not learn out of previous mistakes". Three themes seem to emerge as the solution for documentation, namely that a registry should exist for documentation which contains a list of all the problems experienced, the registry should be in a central location so that all people are able to access and view the registry, and the registry should be maintained and updated on a regular basis.

Factor influencing Recurring Issues	Comments from respondents
Documentation	There is no register on how the problems was solved or what work around was implemented
	Resolutions are not properly documented
	Issues and the fixes don't get properly documented
	Update documentation i.e. problems and solutions in a central place easy for lookup by all
	The impression I get is that issues are raised, sorted out so that testing can continue, but not documented and as a result does not become part of BAU (Business as Usual)
	All problems should be listed
	Different resources performing DR test and not being aware of previous issues
Lack of Time	Not enough time
	Dedicated time is not made available for this
Processes	Lack of a clear cut process
	Update process where required, i.e. to improve the sequence due to interdependencies
	Need more structure for initial setup process, in other words, time frames for installation of: 1. AD Refresh 2. MQ 3. Mainframe 4. Workflow 5. DB2 6. SCCM Profiles available 7. DBA 8. Lamda 9. Terminal Services Setup
Accountability	Nobody is looking at problems experienced during previous exercises
	Someone must make sure those problems are addressed before the next exercise.
	DR accountability must be vested in teams
	KPAs must be linked to it
Communication	Lack of communication. Set up processes to promote this.
Lack of Focus	All personal must be made more aware of the reasons why we have a DR site
Resource Unavailability	Dedicated resources are not made available for this.
Planning	Bad Planning
	Sourcing of technical resources according to responsibility

Change Management	Changes in the South not necessarily applied in RDC (the remote data centre)
	DR must be seen as production
	Keep DR North in sync with Prod i.e. especially with the clustered environments
Environment	Unavailability of environment during the year
Low Priority	Too many higher priority tasks
	DR is seen unnecessary and has low priority with everyone
	DR is not really a focussed area for Business - it is an "IT problem"
Follow up	Have a post mortem to Identify follow-up actions

Table 7. Responses to Factors which influence the recurrence of issues during tests

Lack of accountability was also cited as a cause of recurring issues during RDC tests. Accountability for the documentation of issues experienced, and for the subsequent corrective actions that stem from these issues, "must be vested in teams". In a follow-up discussion with the Head of Architecture and Planning, "the respective application teams must take accountability by signing off on the reports which are generated during the tests, i.e. that they accept the report and the consequent corrective actions to mitigate the issues, or they reject the report and provide the justifications" (personal communication). The issue which arises out of this is that, despite the current process in place to sign off on the report, there are no "consequences" for not taking the necessary corrective actions, and the potential solution would be to "link the KPA's (key performance attributes) to the RDC".

The change management process is cited as contributing to the experience of recurring issues. Changes made in production are not applied to the RDC, and hence the RDC lags behind in terms of patches applied, versions of the software in production versus versions running in the RDC, application changes, etc., and accounts for most of the issues experienced during the RDC tests. Currently, in Company X, the Change Management process is automated via a tool which has an "RDC impact" checkbox which, if ticked, would spawn a child log for the change to be applied to the RDC. However, this check box is rarely checked, hence the changes are not applied to the RDC, resulting in the impact experienced during the next RDC test. One respondent made an important observation by stating that "DR must be seen as production", i.e. from an IT point of view there should be no distinction made between production and the RDC, and the RDC should form a natural part of day-to-day tasks. As a corrective measure, it was suggested that the "RDC impact" checkbox be made a mandatory field to "force the IT Development teams to think actively about applying the changes to critical systems in the RDC". An additional suggestion is to routinely flag all critical systems to be automatically updated in the RDC.

Central to the Change Management Process is the lack of time and resources available for the RDC. Respondents concisely summed up the situation: "there is not enough dedicated time and resources made available for RDC" and "there is just not enough time". The unavailability of the disaster

recovery environment between the bi-annual tests meant that there were only two opportunities to test and verify that the production and RDC environments were in sync. This had an impact on recurring issues in that corrective actions could not be tested before the next scheduled test. RDC and HA testing is a bi-annual occurrence, and it has a direct impact on the focus which resources place on IT Continuity. Consistent with this idea is that "social hazards" encountered on a daily basis, or whose existence and implications are reiterated through regular attention, are perceived as more salient, and thus during quiescence periods when readiness work must take place, natural hazards will compete with their social counterparts for attention, with the salience or otherwise of a hazard (natural or otherwise) evident in how much people think and talk about it. The relative importance of natural hazards will be reflected in the frequency with which people discuss them, and this renders critical awareness as a potentially important precursor variable (Paton, 2003). A comprehensive and continuous focus on IT Continuity should be maintained, and it was mentioned that: "we are not talking about it enough, we are not testing enough and hence the awareness not there". Respondents also felt that the solution would need to include more focus and awareness: "all personnel must be made more aware of the reasons why we have a Disaster Recovery (DR) site".

The lack of commitment to IT Continuity is substantiated by three factors, namely: "Too many higher priority tasks", i.e. production issues take precedence (because of the above-mentioned factors). This is substantiated by the comment "To me it is a job that has to be done so the sooner I can get it done the sooner I can get back to the live environment and other projects that is on my plate"; "DR is not really a focused area for Business - it is an 'IT problem'", i.e. business only feels the impact of production issues and does not directly feel the impact of an application not working in DR. Because they are not affected they place minimal focus on DR and it becomes an IT responsibility; and "DR is seen unnecessary and has a low priority with everyone". Another respondent stated "we are all very positive about it, but it is a side show at present".

The lack of clear processes before and during tests, the lack of communication, and the lack of the RDC test as a project have also been cited as affecting planning and focus for IT Continuity. A collaborative Project Team must be incorporated into planning: "My suggestion is that all the people involved should meet daily during the DR exercise, and next steps should be communicated and issues addressed, as if in a real DR situation". And a "party from IT *Infrastructure* and *IT Development* should be accountable to table the report with mitigation actions and timelines".

6.2.2 Question 2: Which factors contribute to resources not taking corrective actions which stem from previous RDC/HA tests?

As portrayed in Table 8, one of the biggest factors which contribute to resources not taking the necessary corrective actions which stem from previous RDC tests, is the lack of time and resource availability. Production, day-to-day tasks and project priorities place constraints on the capacity of teams to devoting effort to corrective actions. One respondent aptly described the current scenario as "things (*DR related tasks*) are neglected during BAU which in turn affects other priorities and resource time". Another respondent stated "Yes I know when the next RDC test is, but we get busy with other tasks and tend to forget because it is not on our 'normal' task list".

The time and effort required to apply corrective actions in the RDC is also constrained by the fact that applications have infrastructure and other application dependencies, and it becomes difficult to coherently coordinate the time and efforts of the respective teams outside of the RDC/HA tests. This frustration is especially evident when new resources step in and are perhaps not as efficient or experienced as the regular resources who normally test DR. In addition, changes made to RDC cannot be tested in full because all systems are available only in a RDC exercise.

Factor influencing Corrective Actions	Comments from respondents
Lack of Time and Resources	Not enough time, too many higher priority tasks
	Team capacity constraints
	Dedicated time/resources are not made available for this.
	Workload in south and effort "applying" in in RDC
Application and Infrastructure Interdependencies	The fact that we all have dependencies on each other. However each department focuses on their part of the DR. Many a time other departments signed off on their part of the DR and when we start testing we still find "errors" emanating from their applications.
Accountability	Nobody takes control and make sure that all problems are addressed on a permanent basis
	Resources do not take ownership
	Not managed by accountable managers
	DR accountability must be vested in teams
	Nobody takes responsibility and there are no "repercussions"
Low Priority	DR is seen unnecessary and has low priority with everyone
	Maybe the sense for importance of DR capability is not vested across all levels of resources
	Production support takes priority
	DR is not really a focussed area for Business - it is an "IT problem"
New Resources	Often new people involved which do not help continuity
Skills and Knowledge	Not all knowledge in one person. DR requires a person who has knowledge of the interfaces and open systems. An architect to orchestrate the successful flow of events and dependencies.
	Central person / architect to take control that understands and has knowledge of systems and interfaces.

Table 8. Response on Factors which contribute to resources not taking the corrective actions from previous RDC tests.

Respondents also cited lack of visibility into, and presence of, an end-to-end architect who is intimately familiar with inter-dependencies between applications, infrastructure and interfaces as a source of recurring issues. Recurrent is the theme of lack of accountability as a reason why corrective actions are not taken and hence recurring issues being prevalent.

Consistent with the view that "people tend to be uninterested in and unwilling to take action for preparedness and to reduce the risk" (Tekeli-Yesil, 2006), respondents cited that "DR is seen unnecessary and has low priority with everyone". Interesting to note are the potential differing levels of DR priorities across teams. However, this was not a focus of the investigation.

An absence of belief in the effectiveness of the measures (outcome expectancy) and fatalism were mentioned in past studies as factors discouraging preparedness (Tekeli-Yesil et al., 2010). From the research, fatalism does not emerge as a factor prohibiting the efforts associated with preparedness. The absence of belief in effectiveness came through quite strongly: "IT Continuity is never a true reflection of what a DR situation is. Memory sticks and 'ad hoc' restores do not reflect our ability to 'continue' with business in RDC" and "Not as it is done currently – Currently it is smoke and mirrors".

6.2.3 Question 3: IT Continuity is viewed as an overhead, protecting against something that may never happen and not contributing directly to 'the bottom-line'. In your view, why is this statement justified/not justified?

All respondents cited the statement as not justified: "We are in the Insurance business so there is no reason why we should not understand that we need to make provision for future disasters in our lifetime with appropriate plans in place". The comments, as depicted in Table 9, yielded insights into why respondents thought DR is important, e.g. the lack of preparation and planning could affect the share price, bottom line and sustainability of the company.

Comments from respondents

A real disaster will have a major effect/impact on the company's bottom line if we are not prepared.
It is necessary because if a disaster strikes and there is no IT Continuity plans in place there will be no bottom line
Disasters can happen at any anytime and could leave a company crippled
Is required as a safety measure
DR capability has an impact on our share price
It is necessary in case something should happen
It is for the same reason people have house hold insurance. This can have a critical impact on the business if not in place.
IT Continuity is a form of Business Insurance

This is part of my company's bottom line.

Table 9. Reasons why DR is important.

There was no difference in the strong sentiment shared between the levels of people surveyed, with comments such as “this (DR) is a must for all businesses; it must happen; it is a must do; we must be prepared”. However, despite the strong sentiment, there are negative connotations associated with IT Continuity as indicated by the statement “it is not justified, but in many cases it is unfortunately how it is perceived” and “this will always be a necessary evil for IT guys. Evil because we have to make do with an environment that is ‘half baked’ because of cost”. A solution was proposed by a respondent: “To cater for the work that IT Continuity need from the different areas, each area head must "budget" for continuity testing. This must also be taken into account with the supply and demand processes and the allocation of resource time”.

Given that no BIA has been completed for any of the legacy systems which are critical and exist in the Battlebox, a subsequent BIA process, with documentation, was designed in conjunction with Risk Management to ensure that departments look holistically at the reasons why an application is deemed critical. In this regard, BIA documentation was requested for a “like for like” replacement of Lotus Notes (old legacy) with Exchange (new). The response from a very senior IT executive was “sorry, this is red-tape and I am not going to participate in it - waste of time”. The response from the architect was equally negative. The frustration from the IT Continuity Coordinator’s perspective is “if you cannot justify why an application is critical, it is akin to not being able to justify why IT Continuity exists. I have nothing concrete to justify the existence of anything on the critical list. People are loathe to transfer their implicit knowledge and experience to something tacit like a BIA because they see it as a waste of time. If the senior executives think it is a waste of time, imagine the struggle to convince people lower down to complete the documentation”.

6.2.4 Question 4: Remote Data Centre: End of Life (EOL) Technology is used in RDC and thus the infrastructure is quite old. Thus testing is not always like on like technology (servers of a later generation in production). What is your opinion of the statement and how does it impact on you?

Fifty four percent of respondents felt that “problems encountered are not related to so-called ‘old technology’". Forty six percent of respondents felt that they are directly impacted by the infrastructure differences and technology, which is not mirroring production as indicated by the statement “I personally feel DR infrastructure is not really capable of supporting Business Continuity. The hardware is outdated, slow, and potentially problematic and will most probably crack at the first sign of load”.

Most of the respondents felt, however, that, while they were not directly impacted, the different environments logically mean that in the event that the Company experiences a disaster, it would be problematic: “In order to re-create the Prod environment, the Lab (RDC) must equal production, otherwise the test does not make sense”, “I think that DR centres should be the same as the 'live' data centres. This could heavily impact application/service integrity if a disaster should occur” and sentiments are summed up in the statement “It is important to simulate a DR exercise as real as possible”.

The real impact of not having the environments mirror each other relates to the work effort which must be undertaken to get things to work in the RDC environment: “this impacts negatively on the developers who try and keep the systems (applications) the same. If it is a long cumbersome process the systems will most likely drift apart as a lot is done in 6 months between the tests” and “The setup is not exactly the same as Production, hence changes cause delays, e.g. Terminal Services requires specific changes each DR because of the unique DR setup”. Suggestions to improve the different environments relate to “consider documenting the differences between DR and PROD”.

6.2.5 Question 5: In your experience/view, what are the frustrations with IT Continuity?

The results of the survey have yielded four classifications which cause frustration, namely culture, Process/focus, resource/time availability, and environment/infrastructure.

“Culture is not a static ‘thing’ but something which everyone is constantly creating, affirming and expressing. Organisation culture is the emergent result of the continuing negotiations about values, meanings and proprieties between the members of that organisation and with its environment”, i.e. culture is the result of all the daily conversations and negotiations between the members of an organisation (Seel, 2000). According to this theme, from an organisational error perspective, the culture (as depicted in Table 10) of blame, commitment and communication can be changed by engaging and negotiating constantly and consistently.

Culture	Process / Focus	Resource / Time Availability	Environment / Infrastructure
Communication and organizing of the DR. Mails that are sent out late for example.	Big focus before tests which causes "panic", Rush jobs to do "catch up"	Not enough time	Infrastructure and connection speed is frustrating
Blame	Structured project plan with realistic timelines	Too many higher priority tasks	Inadequate hardware and resources
Too much focus on petty stuff (SLA missed with 30 minutes with valid reason)	Need more detail planning regarding testing	Lack of resources	Slow Lab and response speed & capacity
Finger pointing	Bad planning from business	It is a part-time job which always happens at the wrong	Environment (emulators) was not ready last time

		time	
Communication	Lack of a test plan and Project plan with dates, times and names of people involved	Not always opportune time to test	Speed - the more users, the slower the response
Commitment	Communication: consider booking a timeslot in each manager's calendar to emphasize the kick-off of a DR	Knock-on effect of initial delays and then having to come in over weekends	Quick, temporary solutions. Not having remote access.

Table10. Greatest frustrations with IT Continuity.

The results reveal that constant and consistent focus be maintained throughout the year in the IT Continuity sphere to prevent the hype and panic which is created before each test. The communication of a concise test plan will alleviate the frustrations encountered with planning resource availability. From a technological error perspective, the environment causes frustration in that the 2Megabyte link between RDC and the laboratory where the tests are conducted are slow, especially when multiple users are testing simultaneously. Providing remote access for resources to nurse the backups and restores from home will ensure that people are less frustrated with having to spend 54 hours, the time it takes to execute the DB2 restores, at work to get the jobs through. Hardware, sufficient storage and capacity are also cited as causes of frustration.

6.2.6 Question 6: What must be done to alleviate the frustrations? i.e. How can we improve your experience with IT Continuity? How do we increase the focus and commitment to Continuity efforts?

From the responses below, depicted in Table 11, it became apparent that constant communication, education and awareness are necessary to maintain the focus on DR. The organisations we create to build and manage economies, infrastructure and communities incubate hazards with the potential to trigger incidents and disasters (Chapman, 2005). To manage this effectively, clear processes are required to plan and manage the DR tests which include the Project Management Office as well as the Change Management Process. The end-to-end process should include not only the report which highlights issues encountered during the tests, but the corrective actions required, and a follow up to ensure that corrective actions are implemented and that the issues have been resolved and the risk mitigated.

Factor	Comment
Awareness and Education	Awareness. Strategy shift in times of EOL (End of Life) hardware. We can just prolong the periods between hardware refresh.
	DR readiness must be understood
Focus	Ensure DR has the required focus
	The commitment is there, but the focus could be improved
Corrective Actions	All problems encountered must be attended to before next exercise.

	Check all previous post-mortem activities completed.
Communication	Better communication - what is the expected outcome, what is being tested when
	Communication: consider booking a timeslot in each manager's calendar for a kick-off meeting (pre-test meeting)
	All the people involved should meet daily during the DR exercise, and next steps should be communicated and issues addressed. As if in a real DR situation
Project Office / Task	Allocate time with PM/Task manager to be included in plan long before testing date.
	It must be done. If it was planned better and added to task plan, the morale will not be so low.
	Structured / Project plan to get DR up
	Having a Test Plan / Project plan with all setup activities according to their interdependencies, dates, times and names of people involved.
Recognition	Reward and recognise people or departments that have done great. Yes it is a short term motivator but it can lead to long term success.
	Give credit where it's due. Don't slap a person (provider) for breaching with an half hour while the issue causing it was raised to all powers to be.
Infrastructure	In the Document Management environment we have applications with a DR capability but it must be on the "live" company WAN, not separate as in DR
	Explore replacing Terminal services (TS) with VM or other similar like production
	Provide remote access
	Provide more bandwidth
Backup and Recovery	By making the process to keep the systems in sync as fast and painless as possible for developers.
	A process to continually update Terminal Services in DR
Business buy in	What I'm going to do myself in the new year is to ensure that we get much better buy in from the users and ensure that training/communication happens properly going forward. That should overcome the issue of testers arriving unprepared
Follow up	Have a proper follow up process in place to make sure all issues are resolved as soon as possible after an exercise
Documentation	Frequently Asked Questions
Change Management	Continuous updating of software as production software is changed

Table 11. Factors and Actions to alleviate the frustrations/issues within IT Continuity

Regarding the environment and infrastructure frustrations, respondents felt that more resources (network, hardware. etc.) need to be implemented to provide an environment which is conducive to testing. This can only be achieved by a closer relationship between IT and the business, and a clearer focus on the importance of DR as a business fund DR initiative. It is not only a money issue, but a process issue as well, e.g. If business and IT define and manage backups and restores effectively, the funds required to procure additional storage requirements could be diverted to improving the infrastructure.

Recognition is one of the major issues lacking in DR. The Company is so prone to laying issues on scapegoats that no effort is directed at rewarding or recognising DR efforts.

6.2.7 Question 7: What is your manager's view of IT Continuity efforts? How does this impact on/influence your outlook toward continuity efforts?

Forty per cent of respondents were unaware of their manager's perception of IT Continuity, while, of the sixty per cent who were aware of their manager's perceptions, 4% responded that the manager

perceived IT Continuity as "inconvenient". Forty per cent indicated that they share the views held by their managers, with comments such as: "We share the same sentiments as it is the cornerstone of sustainability", "100% commitment" and "DR is on both our KPA's. Need I say more?". The gap between board level commitment and the lack of commitment operationally could be attributed to the lack of communication filtering down. As a respondent succinctly put it: "It could be that senior management doesn't spread the commitment and message of importance".

6.2.8 Question 8: Have you ever experienced a disaster?

In response to the question "Have you ever experienced a disaster", 63% of respondents indicated that they had never experienced a disaster, and of the 37% who indicated that they had experienced a disaster, only 4% indicated that the disaster was of a serious nature, while the balance indicated that the disaster was not significant enough to merit an invocation of the RDC. Table 12 reflects the magnitude of disasters experienced by people who participated in the questionnaire.

Magnitude of Disaster	Comments from respondents
Severe	Fire at one department years ago
Non Severe	Personal PC (data loss due to hard drive crash)
	Only on small scale.
	Not in a business sense
	Backed up data was corrupt. Resulting in massive rework and loss of time and money and effort to business
	Only on small scale. When the server was not available for a full day and a half due to connection problems.
	Only on small scale e.g. power outage, localised issues etc.

Table 12. Experiences of Disasters

Not until a disaster happens and severe losses are experienced do people realise the need for disaster preparedness, i.e. efforts are made after the event, and pre-disaster preparedness is not high on the list of priorities in the absence of this (Shaw et al., 2004). Consistent with literature, the sentiment was succinctly summed up in the statement "we have not had a DR yet - so no pain no gain. People do not understand that our DR capability has an impact on, for instance, our share price. No one has really been put to the sword on DR" and "because people do not fully understand it, they see it as it will never happen". The survey also reflects that fifty percent of companies implemented disaster preparedness plans after experiencing an outage and/or data loss, while only 28 percent have actually tested their recovery plans (Continuity Central, 2011).

Concerning disasters and participation in preparedness, some level of fatalism is prevalent in society, which mean that all deeds are believed to be pre-ordained and arranged by God, and hence the individual can do little to change the course of action. When taken in the context of disaster management, individuals in fatalistic societies would perceive that there is little or no use in taking

preventive measures, such as preparedness and mitigation. It also reflects a relief strategy that focuses on what to do *after* the disaster rather than focusing on what can be done *before* the disaster (Inelmen et al., 2004).

Literature suggests that, despite the acknowledgement of the threat, the level of personal risk perception is low, and it could therefore account for the low level of commitment. "Disasters can happen and did happen in Company X years ago when a whole department was burned down". Risk perception is related to three major factors: dread, familiarity and exposure (Shaw et al., 2004). As indicated from the results above, familiarity and exposure to disaster are extremely low, hence the factor of dread is also low. This could account for the dichotomy between awareness indicated by comments such as "Disasters can happen at any time" versus the reality of commitment to preparedness.

6.2.9 Question 9: Is IT Continuity justified?

Risk reduction behaviour is not only delivering the information or message, but is related to a complex factor of personal evaluation process including prior attitudes. The risk communication process depends on socio-economic and cultural issues. These factors relate to preparedness: perceived risk, amount of relevant information, level of past damages, salience of hazard, and level of knowledge about the threat (Shaw et al., 2004).

A large number of respondents (88%) acknowledge that IT Continuity is justified. Table 13 reflects a few of the attitudes regarding the justification.

Respondent	Comment
R1	It's not justified but it is insurance that you need to take out if you are responsible and want to see your company as a sustainable business
R5	It makes or breaks a business should you not have it
R13	Need to be prepared
R7, R12, R21	Absolutely / Definitely / Critical

Table 13. Comments supporting the justification of IT Continuity

The rest of the respondents (12%) did not think IT Continuity was justified, although it would appear from the comments in Table 14 that this reasoning is related to processes which are failing, to insufficient communication, and to lack of focus.

Respondent	Comment
R2	DR is seen unnecessary and has low priority with everyone
R6	Not as it is done currently – Currently it is smoke and mirrors

R12	It is a side show at present
R13	It is inconvenient
R4	It must be done. If it was planned better and added to task plan, the morale will not be so low.

Table 14. Comments highlighting process failures with IT Continuity.

6.2.10 Question 10: The RDC tests are bi-annual and because the Mainframe is unavailable outside of these slots, testing between these phases is not possible. What impact does this have on you?

The RDC environment is split between Mainframe (MF) and Open Systems (OSY). The OSY environment is available throughout the year and, due to the costs associated with the MF, it is brought up to 650 MIPS for the 10 days of testing only. Hence all OSY applications which have MF dependencies are affected as well as those applications which are fully MF dependent. The question was to ascertain the impact the unavailability of the MF outside of RDC tests had on recurring issues. It was indicated by 16% of the respondents that the unavailability of the Mainframe affected them (Table 15), while 84% of the respondents experienced no impact, or felt that changes done to production should be part of business as usual (BAU) activities and therefore should have no impact.

Impact	Percentage	Respondent	Comment
High	16%	MASSIVE! ALL OUR APPS are dependent on Mainframe, to keep them "current" and to test changes made in the South that is applied at Remote Data Centre
		The "application" requires mainframe availability
		At present it will have a big impact as a lot of our business is still on the Mainframe. However, in a year or so from now, the mainframe will not be the issue but rather the open systems Disaster Recovery
Low	84%	DR testing should be close to a formality if BAU updates are done during the year as they should be
		Not a big issue / None / Minimal / No impact

Table 15. Impact of the inability to test outside of RDC slots.

6.2.11 Question 11: Do you receive the necessary support during tests from service providers, managers, etc. If not, please substantiate your answer

The aim of this particular question was to ascertain if the necessary support was being given during the RDC tests and if the absence/presence of support had any impact on recurring issues. Of all respondents, 64% claimed that the necessary support is available during testing. Of the other 36%, several pointed to the fact that between service providers who offer the services to IT Continuity, the lack of knowledge and trust is a factor which hampers continuity efforts and the resolving of recurring issues (Table 16).

	Comment
Knowledge	Vendor A should be more knowledgeable and should take more care when restoring data
	Ensure knowledge in the 'Vendor A' team
Trust	We share information between service providers when working together and the same information is used against us when SLA's are breached
Handover	Many a time the other applications already signed off and when we get there we get errors and they need to come back and fix it.
IT versus Business	Not always from business

Table 16. Impact of Vendor support on DR Tests

A noteworthy point is that the necessary support is not always obtained from business. The project manager who liaises with business resources regarding the test commented on the unpreparedness of business regarding the tests: "when I called the users they were surprised that they were needed as no one had informed them. Some of them come to the Lab with no test cases prepared or documentation of any sort. Some of them had absolutely no idea of what they should be doing much less testing". This would indicate that the support of management on the business side is absent and that the necessary communication is not taking place.

6.2.12 Question 12: What must we stop doing? What must we continue doing? What must we start doing?

In response to the behaviour that must be discontinued, activities under three emergent themes were highlighted, as depicted in Table 17. There is a perception of blame and a negativity culture in the Continuity sphere which respondents have highlighted. An organisational blame culture is defined as "the team is so busy engaged in guerrilla tactics to survive, that they do not perform anywhere near their capacity. The organisation still runs, but often key members spend more than 60% of their time on protection tasks. Removing the blame culture not only lifts motivation and productivity substantially, it multiplies results" (Anderson, 2009).

Factor	**Comment**
Culture	Stop blaming people
	Stop hammering on stuff that's not important and focus on what is
	Stop being so negative about the DR testing
Communication / Reporting	Communication on errors and how it is communicated is not always accurate. If not communicated correctly, an incorrect impression can be created with Management
Hardware	Stop using old EOL hardware

Table 17. Behaviours/Actions/Factors that need to stop

The other aspect of the blame culture in the work environment is that "in a blame culture words are heard from that frame", i.e. negatively, and the blame "paradigm encourages certain types of

behaviour", i.e. people will behave in blaming ways (Seel, 2000). To improve on this blame culture we need to ensure that those employees who err, understand both the severity of their actions and the appropriate action they should have taken instead. This requires a behavioural change which is not part of this research. "Trust is a key element of a reporting culture and this, in turn, requires the existence of a just culture—one possessing a collective understanding of where the line should be drawn between blameless and blameworthy actions. Engineering a just culture is an essential early step in creating a safe culture" (Reason, 2000). Reporting on errors must be altered to reflect the true state of affairs so as to manage perceptions, and the hardware employed must be more up to date.

What the Company must start doing to improve the IT Continuity portfolio is to ensure that all the suggestions are taken cognizance of, and continue to strive to improve the process. An attempt must be made to multi-skill resources and expose all resources to DR. In terms of the environment, the Company should implement practical steps such as increasing the network speed and using more up-to-date technology (which mirrors production as much as possible). Improving the processes for testing such as introducing defined test schedules would go a long way toward alleviating frustrations. On a softer side, and more difficult to implement, is the fact that business needs to take ownership of DR. Since business defines the applications which are critical to them, and also carries the cost of the critical applications in DR, the accountability and responsibility for DR must vest with business and not with IT.

Table 18 represents the factors, actions and behaviours which the Company must strive for to alleviate frustration and improve continuity efforts.

Factor	Comment
Environment	Ensure we address the feedback
	Working as a team
	Continuously improve the process
	Strive to become market leaders in Continuity instead of market followers. Everyone has got Continuity, what makes the company's plan unique in the Financial sector?
Resources and Skill	Much of the RDC setup is manual tasks with knowledgeable people attending to it. In a disaster those people will most probably not be available to do the setup. How to fix this with "Not enough time, too many higher priority tasks" is another issue.
Hardware	Better speed
	Start using new hardware and VMWareconsistently to deploy machines and prolong the hardware refresh periods.
	Test schedules
Accountability	Operations side of business should take much more ownership and actually own the DR solution and not IT. At present it is IT that needs to convince a very reluctant operations that this is important

Table 18. Behaviours/Actions/Factors that need to start

Table 19 represents the factors, actions and behaviours which the Company must maintain. They are the constant improvements to backup and restore procedures, the reporting during and after RDC tests, the current communication around the tests, and the focus which would(might) have been introduced the previous year.

Factor	Comment
Backup and Restore	Have a health check report on all restores in DR as to the success of each procedure that had to be completed.
Reporting	Ensure that the same problems do not occur with every DR exercise
	List the recurring issues and ensure that they do not happen again.
Communication	The communication is good keep it up
Focus	Continue to give it a high focus within IT and business.
	Make sure DR has the required visibility in all environments

Table 19. Behaviours / Actions / Factors that need to continue.

6.2.13 Question 13: "IT Continuity is mandatory and the company can be fined if we do not adhere"…are you aware of policies, SLA's etc.? If not, what must be done to ensure that such awareness is raised?

It is frequently assumed that providing information on disasters and how to mitigate their consequences will encourage preparation, but this assumption is unfounded because considerable effort and expenditure on education and levels of preparedness remain low (Paton, 2003). Consistent with this theme is the fact that, despite an IT-wide communication session, 48% of respondents remain unaware of any policies or governance around IT Continuity, indicating a need for more effort and expenditure on education. Of the 52% that are aware of the policies, etc., the majority of the respondents learned this information from the Company-wide education drive, as indicated by the statement "the insert in the communication session in the CR Louw (lecture hall) was a good beginning".

The culture of disaster preparedness is vital and, to build this culture, education is one of the key tools (Shaw et al., 2004). In terms of the latter part of the question, what must be done to increase the focus, consistent with literature, is the need to highlight these policies via constant awareness drives: "a simple communication will do; constant awareness; communicate more and make it visible to business". People are quite eager to learn more about these policies: "more information would be good like fines, policies, SLA's etc.; I would like to know more about the policies and fines that the company would face if we do not adhere". At the Company communication session, the

current SLAs were highlighted, and a comment from this was: “I must adhere to a 24 hour SLA for MF recovery; I have never seen the SLA”. This indicates that people, once aware, are seeking to increase their knowledge in this domain.

Respondents felt that managers are the predominant mediums through which these education drives should take place: “Management needs to talk to staff on a regular basis about this; Ignorant managers should be forced to take responsibility for their teams; provide the accountable line managers with enough information to understand the necessity of DR. They have to instill the awareness in their teams and DR must be in their KPAs and job descriptions (if not already there)”. Other mediums of education suggested were to “conduct workshops and add the policies, procedures and SLA to the internal website”.

An interesting observation was made regarding the motivation for this type of education, namely that “that statement alone indicates that should something go wrong a person or department will get blamed. We must move away from that mentality and not only do things because it is required by law, we must do it because we want to”. Hazard education programs could reduce perceived risks and levels of preparedness because people transfer the responsibility for the safety from self to others (Paton, 2003). This then highlights the need to be cautious so that the responsibility for preparedness is not placed on particular individuals, but that the onus rests on all resources to educate themselves. Disaster planning always requires some form of change in behaviour, and change is often difficult to bring about. Thus, getting preparedness measures developed, adopted, and accepted involves overcoming barriers that are often quite formidable.

7. Discussion

Comparative analysis of the RDC and HA tests yielded a list of recurring issues. The main proposition was to determine if HOT factors contribute to recurring issues and, if so, which factors and why? There is a special concern to identify the conditions that make it possible for unnoticed, misperceived, and misunderstood events to accumulate in a manner that leads eventually to cultural disruption (Turner, 1976). HOT factors lead to triggering events, and compound the adverse effects of crisis when it occurs (Richardson, 1994). Industrial failures have been linked to a myriad of human, social, technological and organisational issues (Chapman, 2005). In a survey undertaken, it was found that companies are "still not making disaster preparedness a priority until they experience a disaster or data loss" (Continuity Central, 2011). Institutions fail to learn that errors and non-compliances mark the starting point of an investigation, not its conclusion. The organisation also limits its remedial efforts to attempts at changing the behaviour of an individual staff member by blaming, shaming, naming, and retraining. But the fleeting psychological precursors of fallibility—for example, inattention or forgetting—are the last and the least manageable aspects of the error-producing sequence (Reason et al., 2001). Human, Organisational and Technological (HOT) factors have an impact on recurring issues, and the underlying causes have an impact on the ability of IT Continuity to manage recurring issues.

7.1 Human Factors

The human factors at play during the RDC and HA tests, and the impact they have on recurring issues, were assessed (Figure 15).

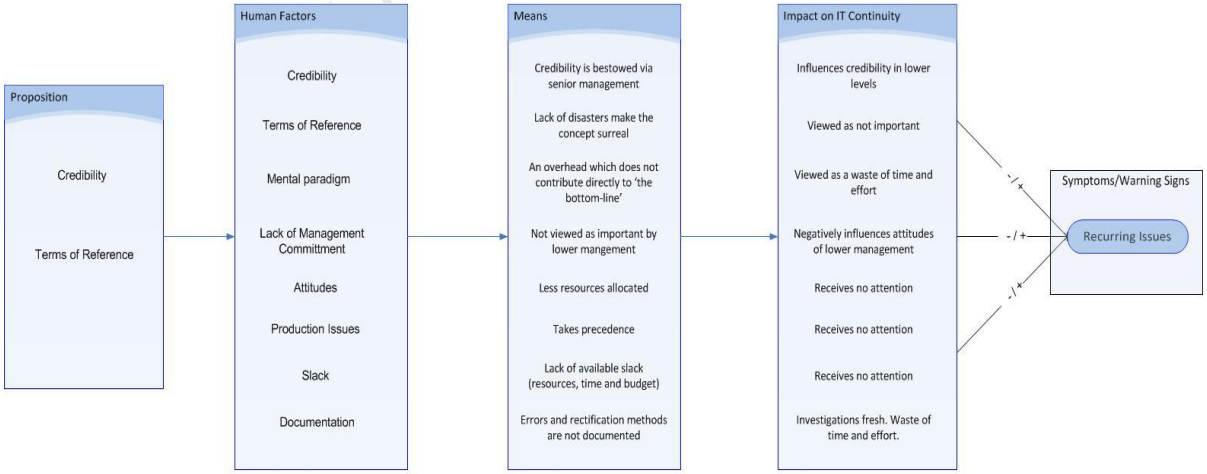

Figure 15. Human factors impact on recurring Issues The impact of Human Factors on recurring issues?

Issues of legitimacy, i.e. the credibility of IT Continuity bestowed via senior management, influences credibility in lower levels of the organisation, as demonstrated by participants who felt that

credibility via education drives and communication should be instilled by managers. The following statement by a respondent illustrated this view: “Management needs to talk to staff on a regular basis about this; ignorant managers should be forced to take responsibility for their teams; provide the accountable line managers with enough information to understand the necessity of DR; they have to instil the awareness in their teams and DR must be in their KPAs and job descriptions (if not already there) “. It would appear that the issue of accountability rests with senior management as well. All communication around the RDC test is shared with senior management, both during the preparation sessions leading up to the RDC tests and the daily reports during the tests. Reports listing the corrective actions required to mitigate recurring issues for the next test are shared with and signed off by senior management. Despite this, results of the survey highlight the lack of accountability, as respondents appear unaware that corrective actions are re-assigned to their teams.

The research also tested whether management attitudes had an influence on how resources perceive and deal with DR, but the results are inconclusive on this aspect as most of the respondents had no view of how their managers perceive DR. The percentage of respondents who indicated they did have a view was too small to be able to draw any conclusive ideas. Management commitment does, however, play a role in contracting with the necessary resources for participation in RDC tests and DR overall. The lack of time and the resource unavailability would indicate that this contracting is either not taking place or not successful, and manifests itself in the attitudes prevalent in the IT Continuity space, as illustrated by this statement from a respondent: “it is a side show, the sooner I get it done the sooner I can get back to the live environment”. Based on the perception that DR is not part of the resources’ day to day tasks, it could be argued that lack of management commitment does negatively influence the attitudes of lower management.

The research further tested whether the personal experience of a disaster had an effect on the paradigm with which respondents viewed preparedness for disasters. According to Tekeli-Yesil et al. (2010), past experience of a hazard seems to be an important factor influencing individuals’ practices regarding precautionary measures. This research confirmed that if the terms of reference are non-existent, i.e. that the lack of experience of disasters makes the concept surreal, it negatively influences the practices resources employ regarding continuity efforts.

Responses to Question 3, about IT Continuity being viewed as an overhead, reveal a strong belief in the justification of IT Continuity as being necessary and important, yet, despite the criticality, preparedness is viewed with reluctance and apparent “apathy” with associations of being a “necessary evil” and “inconvenient”, hence it is entertained and done as a “side show” with “low

priority" and "secondary to production" (quotes taken directly from responses). While this view seems inconsistent with the strong sentiment and justification given by respondents, it is consistent with the idea discussed above that the experience of a disaster is the strong factor which signifies the criticality of preparedness activities.

One of the main themes which emerged from the research is the schism or divide between the importance of production and DR. Because DR is done on an *ad hoc* basis, and is not part of BAU or daily activities, it contributed to creating the divide which negatively influences the priorities given to DR. The other theme which emerged is the absence of slack, resources, time and budget which influenced the existence of recurring issues, and the unresponsiveness to mitigating errors.

Lack of documented and clearly-defined processes was also indicated as a strong factor which encouraged recurring issues and also extended the time and effort to take corrective actions. A respondent made the following comment: "The backups failed because while they (Service Provider A) were backing up to disc, we started our process to backup to tape (Service Provider B), but their backups were taking longer than usual and we started our backups to tape while they were still backing up to disc. Nobody informed us, it was never an agreed process, we always assumed that they would be done, because they are normally done by the time we start backing up to tape". This lack of documentation extended to checklists which must be prepared for every task, as stated by a respondent: "Checks must be put in place to ensure all backups are included when we ship to the North e.g. develop CRON job" and "we need to test/check more often. Pre-checking is poor and must be rectified". In the absence of documentation, however, pre-checking is heavily reliant on existing knowledge and expertise.

Processes which were not adhered to also caused IT discontinuity, as cited by one respondent: "we were unable to test the Investment Admin.co.za component. Due to project changes, the required server was not built in the remote data centre. We must revisit the Change Management process and understand where the gap lies between making production changes and it being replicated to the North. This should be part of the project deliverable i.e. a sign off requesting that the application must be part of the remote data centre".

Human error definitely plays a role in the creation of IT discontinuity, where processes are clearly defined, but humans deviate from procedures, as stated, e.g. "the operator deviated from standard DBA procedures and the DBA started a differential job in error". The net result of this particular problem during the RDC test was a loss of 10 hours, which delayed both IT and business testing to

the point that the test closed off unsuccessfully because not all the businesses could test in the constrained time-frame.

The vital role of communication also emerged very clearly from the research, as seen from this comment: “Due to the Mainframe that had failed, not all the jobs had completed. When the Mainframe came up, only the remaining 46 jobs were run. No one told us where the jobs had stopped. This resulted in un-built indexes on the mainframe databases which meant that data which appeared to be missing was in actual fact related to the indexes which needed to be rebuilt”.

7.2 Organisational Factors

Organisational factors evident during the RDC and HA tests, and the impact they have on recurring issues, were assessed (Figure 16). The study assessed the influence of legislation on IT Continuity efforts, postulating the lack of guidance from various standards and government as influencing the credibility of DR. The lack of legislative guidance only influenced people where they were extremely involved in the governance aspect of disaster recovery, as one respondent stated: “It is extremely frustrating when there are so many standards and in South Africa we have no best practices to adhere to or any guidance from government in terms of what is relevant and appropriate”.

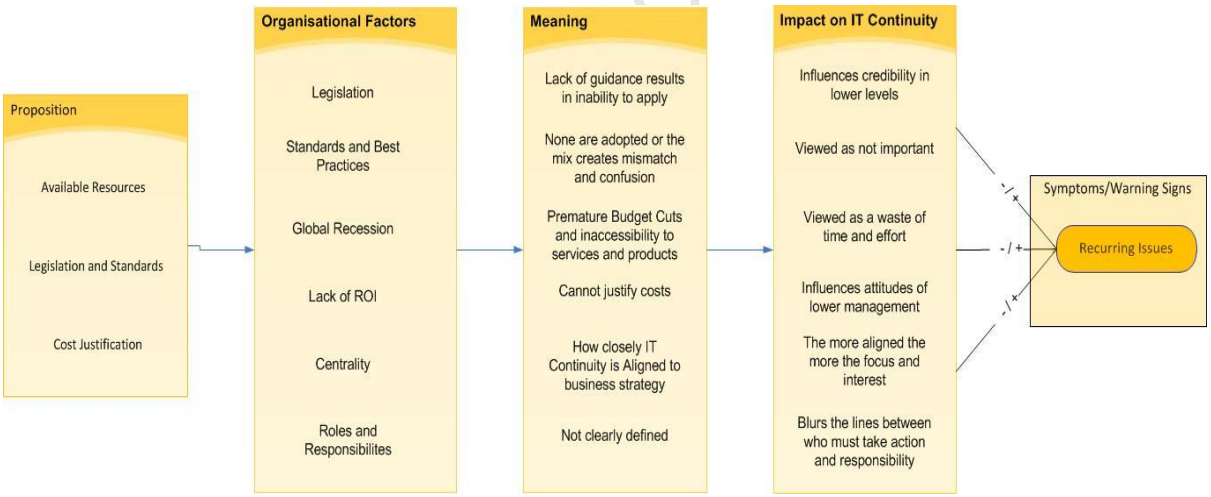

Figure 16. Organisational factors impact on recurring Issues The impact of Organisational Factors on recurring issues?

One of the respondents who participated in drawing up an IT Continuity governance document for Company X, commented on the lack of guidance from best practices relating to the minimum distance between a primary data centre and a hot site (a hot or sister site where there is real time replication), that the standards and best practices offered no guidance and resulted in conflict. The respondent gave an example: “In the United States the minimum distance for hospitals is eighty miles, but there is nothing concrete for insurance companies and especially nothing in the South African context. I suggested 25 to 30 kilometers as this is generally the trend, but I cannot justify my

suggestion. They look at me as if I have gone mad and hence people do not listen to me. They continue to have conversations about the distance and bandy about figures like 12 kilometers. I cannot vet them one way or the other, the best supporting information I can provide is to suggest that it (the sister site) is not on the same power grid". The lack of guidance from best practices and standards is a cause for concern. The research results could not verify the belief that the global recession resulted in budget cuts which impacted negatively on DR. Rather, it is the lack of proving return on investment, and hence the justifications of costly DR initiatives, which contribute to the attitude people have regarding DR.

The centrality of IT to the business emerged as a strong factor in determining the relevance of IT Continuity. DR was seen as an IT function which caused frustration when resources (including funding) could not be procured, because business was so far removed from DR. The business did not experience the impacts of DR failing/test issues, and hence did not see the need to invest more. An alternate statement for this proposition was given by a respondent as: "the closer or more direct the relationship to disaster recovery efforts, impacts the perception of DR positively", (what a dreadful sentence!) i.e. because IT is involved in the RDC and HA tests, they are impacted by the tests, whereas business is not that involved and hence far removed from the tests. Business perception of IT and DR is a potential issue for further investigation.

The centrality of IT to IT Continuity tied in very closely with the point around assigning clear roles and responsibilities, where IT felt Disaster Recovery was a business call since they also fund the DR initiatives. It also came through clearly that the roles and responsibilities of the various service providers and the IT staff should be clearly defined. During the November 2010 RDC test, the application data could not be rolled back to the test date because "the JES[1] spool logs were cleaned after the IPL[2] (UDB). This used to be the old service provider A job for capacity maintenance purposes. When service provider B took over, we (the DBA's) monitored the logs and manually cleaned the logs, because the role was never clearly specified and we simply assumed responsibility". Service Provider B was completely unaware of this function.

[1]JES: JES (job entry subsystem) is a subsystem on z/OS of IBM mainframes that receives jobs into the operating system, schedule them for processing by z/OS, and control their output processing.

[2]IPL: IPL (initial program load) is the act of loading a copy of the operating system (z/OS of IBM mainframes) from disk into the processor's real storage and executing it.

7.3 Technological Factors

Technological factors and the impacts they have on the RDC and HA tests were assessed (Figure 17). The incompatibility of the technology between production and the RDC, i.e. ensuring that technology is the appropriate fit for the task at hand, negatively influenced the attitudes people had, because the testing process became cumbersome and caused delays.

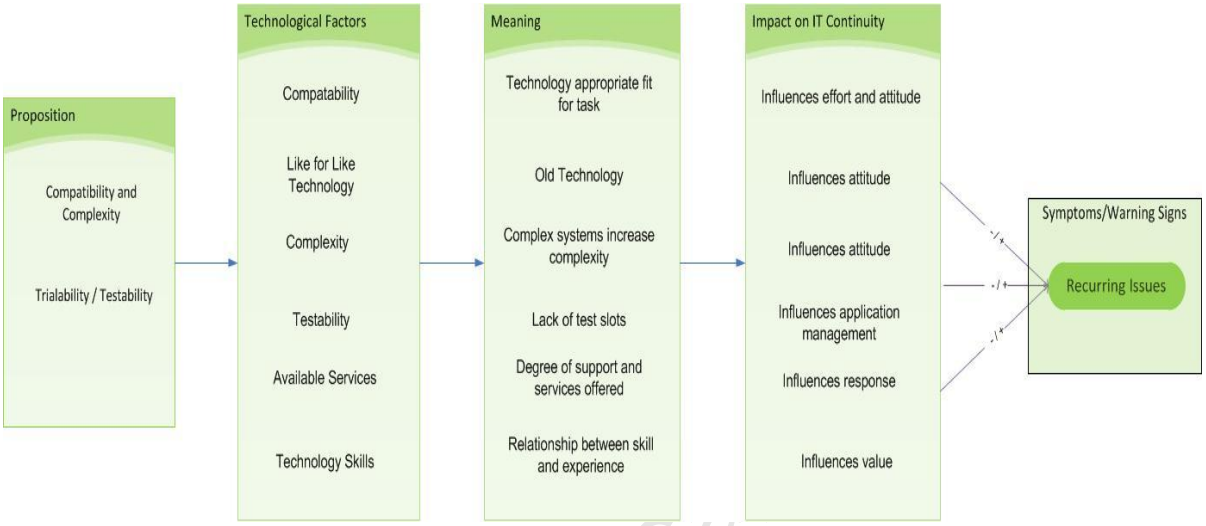

Figure 17. Technological Factors impact on Recurring Issues The impact of Technological Factors on recurring issues?

Technology between production and RDC which is not always 'like for like', affected the paradigm and legitimacy with which respondents viewed IT continuity efforts. A comment by a respondent was: "the Lab (RDC) must equal production, otherwise the test does not make sense". The IT continuity efforts were seen as fruitless (quoted from a response) when "the hardware is outdated, slow, potentially problematic and will most probably crack at the first sign of load" and negatively influenced attitudes toward IT continuity, as illustrated by the comments: "it is not capable of supporting business continuity" and "it is smoke and mirrors". When disparities exist between the types of technology in production and the RDC environment, they undermine the legitimacy of the DR capability as it "does not reflect our ability to continue with business in RDC".

Complex systems increase the effort involved in synchronising the production and RDC environments, as the findings highlighted a clear call for an architect to clarify the inter-dependencies between systems. This lack of visibility into the inter-dependencies between systems negatively impacted on the attitudes resources have regarding IT continuity efforts because of the frustrations experienced when a team hands over to the next team and errors are encountered.

Testability proved not to be an issue, as only a small percentage of respondents indicated that they were severely impacted by the unavailability of the mainframe between tests. Although the

mainframe in the RDC facility is only tested twice annually, all changes to the applications in production are backed up regularly and restored to the RDC environment. Testability seemed to affect only the confidence of the respondents with regard to the changes: “changes made to RDC cannot be tested in full because all systems are available only in a RDC exercise”.

Supportability was not deemed to be an issue. However, the lack of knowledge and trust between service providers was cited as a factor which hampers IT Continuity efforts and resolving recurring issues. Technology skills, knowledge and experience of the individual, on the other hand, did affect the experience respondents had with RDC and HA tests. The research had highlighted that the more experienced the individual resource had, the more value they were perceived to add. A statement to this effect was: “DCN setup is manual tasks with knowledgeable people attending to it”. Comments were also made about the frustrations experienced when new resources stepped in who were not as efficient or experienced as the more proficient resources who normally test DR. This may be a reflection of the additional effort required to bring the DR environment in sync with production due to incompatible technologies. While this is not an ideal state, IT continuity efforts will always be constrained by costs. DR *per se*, is usually a trade-off between 'good to have' and 'must have'. This is a very subjective evaluation, and is also dependent on budgetary constraints and management buy-in of the risk profile and mitigation recommendations determined.

Generally, IT disasters were attributed to human error. Although human error may well be the trigger which hastens or gives rise to an accident, organisational failures enkindle multiple causes. (Tense!) By concentrating on human error alone, the systemic context in which the failure transpires is not considered. Organisational disasters can be prevented, because disasters incubate over long gestation periods during which errors and warning signals build up. While these signals become painfully clear in hindsight, the challenge for organisations is to develop the capability to recognise and treat these precursor conditions before they tail-spin into failure (Choo, 2005).

The recurring issues identified through this research are summarised in Figure 18. Management attitudes (Organisational and Human) and the previous experience people have of disasters (Human and Technological), are the largest contributing factors to recurring issues. These factors create a schism between production and disaster recovery which negatively impacts on the priorities resources assigned to disaster recovery efforts. This divide is evident in past behaviour of the resources who have participated in disaster recovery tests, and explains their negative and often uncooperative behaviour. Their irritation at being called away from pressing production issues and day-to-day operational tasks is evident in their comments and demeanor during the tests, and can

be attributed to the fact that they do not see the importance of continuity efforts because they have never experienced disasters, and management attitudes further reinforce these perceptions.

Human factors such as accountability, communication, and focus; organisational factors such as resource availability, skills and knowledge, documentation, change management, IT driven DR, and processes; and technological factors such as the actual DR environment, directly contribute to and affect the experience of recurring issues. The sub-classifications are interchangeable, e.g. communication, documentation, skills and knowledge, and change management, can be attributed to both human and organisational factors: human because individuals lack the discipline to create the documentation, and organisational because the organisation does not instill, support and demand these practices. The exact classifications are a further potential point of research.

The HOT factors certainly were not the only contributory factors to recurring issues, but they were the underlying causes of recurring issues. The Company ignored warning symptoms and, by implication, allowed for the accumulation of errors which could culminate in a disaster. It would also appear that HOT factors are responsible for the schism between IT production and Disaster recovery as well as influencing the priorities of resources (Figure 15).

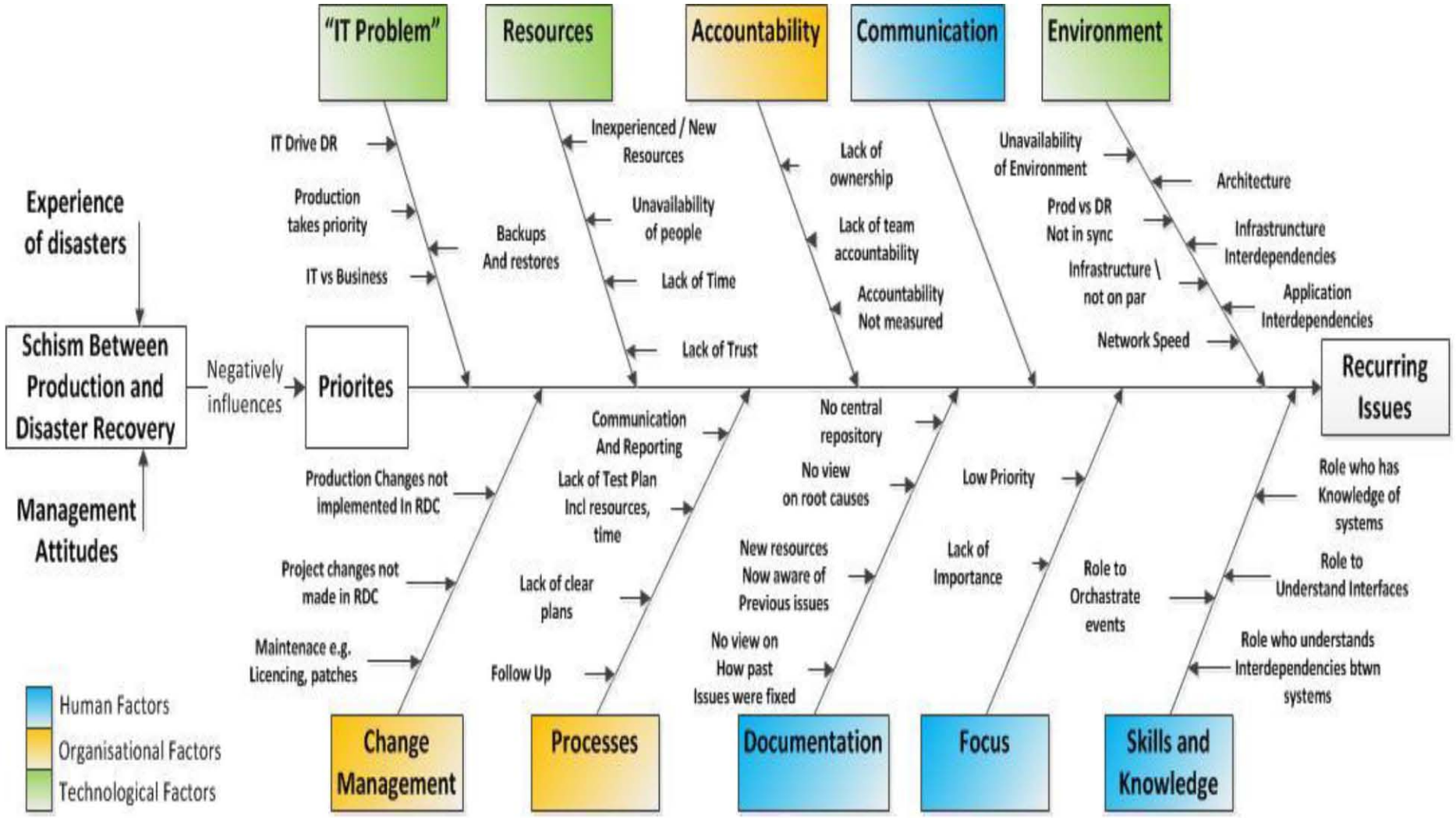

Figure 18. Cause and Effect Diagram of Recurring Issues in IT Continuity (compiled from the findings)

8. Conclusion

As the research has shown, Human, Organisational and Technological factors (Figure 6) produced recurring issues which can only be mitigated with strong IT Continuity Management practices and principles. The Conceptual Model (Figure 10) which was developed depicts this relationship, and highlighted the importance of effective IT Continuity Management principles. HOT factors contributed to the inception and accumulation of errors. The Remote Data Centre tests highlighted these errors and presented them as recurring issues. Accumulatively, they serve as warnings signs to the Company. These warnings, when documented, produce a list of corrective actions which give the Company the opportunity to rectify the issues or mitigate the risks. As highlighted by the research, corrective actions can either be acted upon or ignored. If they are not acted upon, it shows either a lack of IT Continuity management disciplines, or poorly performed IT Continuity management. The unmitigated accumulation of errors might be triggered by a seemingly insignificant event which could spiral the Company into crisis or disaster. Acting upon the list of corrective actions, would increase the credibility of the IT Continuity plans, and potentially lessen the impact of possible disasters.

Technological disasters are potentially predictable (Chapman, 2005), and following the line of thinking that, if companies adhere to addressing the HOT factors which cause errors and heed the corrective actions, technological disasters can often be mitigated. Disasters occur when hazards collide with vulnerabilities (Tekeli-Yesil et al., 2010), and when the vulnerabilities are made visible and a view exists as to what is wrong, disasters can potentially also be predicted. When this view is actively managed via the IT Continuity Management principles, as proposed in the Conceptual Model (Figure 10), disasters can not only be predicted, but can be mitigated and managed down to tolerable levels, thus averting disaster altogether or, at least, lessen the impact that a disaster might have on a company.

It is only with effective management of IT Continuity via the processes suggested in the Conceptual Model that the HOT factors could be managed down. The Business Impact Analysis (BIA) serves to gain a comprehensive understanding of the business, the technical requirements and their relationship with each other. This is a vital component in proving and justifying the return on investment within IT Continuity. A Continuity requirement assessment as part of the BIA solicits an understanding of the business operations, and yields the output necessary to address the difference between the current state of the RDC environment and that which is required. The risk assessment enables plans and mitigating strategies to be implemented to address the threats which exist. These threats are not only related to the tangible vulnerabilities, but also the intangible softer issues such

as apathy, low morale, etc. The findings were valuable in that they highlighted what resources were frustrated with, and thus gave Company X the ability to address those frustrations. The solutions strategy ensures that Enterprise Solutions are developed which will address the discrepancy between the technology deployed in the RDC environment and production. These steps, taken holistically, will ensure IT Continuity maturity.

Disaster remains a dilemma of sudden occurrence (which needs preparedness as the only way to reduce loss) versus infrequent occurrence (which means the priority of preparedness becomes lower compared with other hazards (Shaw et al., 2004). Consistent with this statement, the problem with IT Continuity is that, unlike production, the consequences of the triggering event will not be felt immediately. Unless the Company is spiraled into crisis where it needs to invoke the Remote Data Centre or call upon the Disaster Recovery plans, it will never feel the impact of unmitigated errors. The RDC tests revealed or highlighted the issues, but they are never felt tangibly by business.

Formal IT continuity and effective IT Continuity strategies, as suggested by the Conceptual Model, have the following recompense, namely: It aids in minimising the disastrous consequences of a disruption on an organisation; it reduces the hazard of financial loss; it retains the positive company brand and provides clients and suppliers with the assurance that the organisation's abilities and services are intact; it facilitates the recovery of a client's critical systems within the contracted timeframe; it allows companies to fulfil the legal, statutory and governance duties imposed; it allows companies to assess their levels of conformity to global IT continuity standards and further allows companies to implement IT continuity practices based on best practices (Holmes, 2010).

IT has become a vital part of conducting business in our technologically advanced world. Undeniably a business can practically not do without these components for extended periods of time. Employees, shareholders and customers have come to expect that information should be available around the clock. Even a minor disaster or disruption could cause irreversible damage to an organisation and its public image. To ensure that an organisation could recover after a disaster, a complete IT Continuity Plan should be in place. A complete Business Continuity Planning methodology should preferably be followed to ensure that such a plan is effective in protecting an organisation (Botha & Von Solms, 2003).

The recommendation from this study is to ensure that Company X and other companies pay credence to the recurring IT Continuity testing issues experienced within their companies, as these issues serve as warnings that an IT failure could be difficult to recover from. It takes one event or action to line these issues into a perfect constellation which could result in disaster. The research

further recommends that the Conceptual Model developed be used as a guide or methodology to manage the HOT factors.

If businesses are to remain competitive in our ever-changing economic and environmental climate, they must ensure the availability of their services, and be in a constant state of readiness with the flexibility to respond to any eventuality (Woodman & Kumar, 2009). Effective disaster planning is not optional, it is critical for the success of organisations. Should an organisation not make the appropriate plans and put the relevant mitigating factors into place, it risks losing vital computing resources which could bring the entire operation to a potential standstill and cause it to close its doors permanently (Al-Badi & Ashrafi, 2009).

Works Cited

Al-Badi, A. H., Ashrafi, R., Al-Majeeni, A. O., & Mayhew, P. J. (2009). IT disaster recovery: Oman and Cyclone Gonu lessons learned. *Information Management & Computer Security 17(2)*, 114-126.

Anderson, T. (2009). *Leadership Principles - Kill Blame Culture!* Retrieved December 16, 2010, from http://www.selfgrowth.com/articles/Leadership Principles - Kill Blame Culture.html

AT&T. (2008, June). *AT&T Business Continuity Study Results*. Retrieved June 23, 2012, from http://www.att.com/Common/merger/files/pdf/business continuity 08/Business Continuity Study Results.pdf

Avocent. (2005). *Avocent White Paper on Improving Business Continuity for the Remote Office*. Retrieved fromhttp://infotechnology.hoffmanmarcom.com/docs/Avocent-Business-Continuity-White-Paper.pdf

Baharein, K., & Noor, M. (2008). Case Study: A Strategic Research Methodology. *American Journal of Applied Sciences 5(2)*, 1602-1604.

Baur, E., Birkmaier, U., Rüstmann, M., & Re, S. (2001). *The economic importance of insurance in Central and Eastern Europe and the impact of globalisation and e-business*. UN.

Best Computer Practices. (2009). *DR Glossary of Terms.* Retrieved February 06, 2009, from http://www.best-computer-practices.com/best-computer-practices/index.php?option=com content&view=article&id=57&Itemid=64

Best Computer Practices. (2009). *Planning: IT Continuity.* Retrieved February 06, 2009, from http://www.best-computer-practices.com/best-computer-practices/index.php/index.php/planning-it-continuity

Bharadwaj, A. S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly 24(1)*, 169-196.

Bjelmrot, H. (2007). *The value of a business continuity management plan from a shareholders perspective.* Masters Thesis. Lund University. Retrieved September 28, 2010, from Lund Institute of Technology Digital Theses .

Blau, P. M., Falbe, C. M., McKinley , W., & Tracy, P. K. (1976). Technology and Organization in Manufacturing. *Administrative Science Quarterly 21(1)*, 20-40.

Booysen, T., & Nkomo, Y. (2009). Gearing SA businesses for tough economic and social challenges in 2009.[White Paper]. Retreived from http://www.cgfresearchinstitute.com/Portals/274/Gearing business tough economic times.pdf

Botha, J., & Von Solms, R. (2003). *A Cyclic Approach to Business Continuity Planning*. Thesis. Port Elizabeth Technikon. Retrieved June 21, 2010, from Port Elizabeth Technikon Digital Theses.

Brauchli, C. (2005). *Here They Come Again, How Insurance Companies Exploited 9/11.* Retrieved July 06, 2011, from http://www.counterpunch.org/brauchli05202005.html.

ContinuitySA (Pty) Ltd. (2010). *Measured continuity is good governance.* Retrieved May 07, 2010, from http://www.fanews.co.za/article.asp?Compliance Regulatory ;2,General;1082,Measured continuity is good governance;7381

Chapman, J. (2005). Predicting technological disasters: mission impossible? *Disaster Prevention and Management 14(3)*, 343-352.

Choo, C. W. (2005). *An Information Perspective of Organizational Disasters.* Thesis. University of Toronto. Retrieved June 21, 2010, from Department of Information Management Digital Theses.

ContinuityCentral. (2010). *Human error is a factor in the majority of IT downtime incidents.* Retrieved December 13, 2010, from http://www.continuitycentral.com/news05505.html.

ContinuityCentral. (2011). *2011 SMB Disaster Preparedness Survey .* Retrieved January 17, 2011, http://www.continuitycentral.com/news05548.html.

David, L. (2005). *Mars Polar Lander: Clues From the Crash Site.* Retrieved June 2012, from http://www.space.com/1153-mars-polar-lander-clues-crash-site.html.

Dekker, S., Hollnagel, E., Woods, D., & Cook, R. (2008). Resilience Engineering:New directions for measuring and maintaining safety in complex systems. PHD Thesis. Lund University School of Aviation. Retrieved June 21, 2010, from und University School of Aviation Digital Theses.

Department of Cooperative Governance and Traditional Affairs. (2011). *Declaration of a National State of Disaster* (Vol. 547, No. 33949). Pretoria, South Africa: Government Gazette Republic of South Africa.

Downer, J. (2010). *Anatomy of Disaster: Why Some Accidents Are Unavoidable.*

Earley, A., & Booz, R. (2007). *Catastrophic Events Will Continue to Test Insurers Through 2012*. Stamford, USA: Gartner Inc., ID Number: G00146929.

Firestone, W. (1987). Meaning in Method: The Rhetoric of Quantitative and Qualitative Research. *Educational Researcher 16(7),* 16-21.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative inquiry 12(2),* 219-245.

France 24 News. (2011). *Computer failure hits United Airlines operations .* Retrieved July 06, 2011, from http://www.france24.com/en/20110618-computer-failure-hits-united-airlines-operations

Funder, D. (1987). Errors and Mistakes: Evaluating the Accuracy of Social Judgment. *Psychological Bulletin 101(1)*, 75-90.

Gable, G. G. (1994). Integrating Case Study and Survey Research Methods: An Example in Information Systems. *European Journal of Information Systems, 3(2)*, 112-126.

Gartner. (2009). *Gartner for IT Leaders Toolkit: Presentation for the 2009 BCM Program Overview*. Stamford, USA: Gartner Inc.

Genserik, R. (2009). Man-made Domino Effect Disasters in the Chemical Industry: The Need for Integrating Safety and Security in Chemical Clusters. *Disaster Advances., 2(2)*, 1 - 5.

Gherardi, S., Pidgeona, T., & Ratzanb , S. (1999). Man-Made Disasters 20 years later: Critical commentary. *Health, Risk & Society 1(2)*, 233-239.

Gibb, A., St-Jacques, M. J. C., Nourry, G., & Johnson, M. T. A. (2002). Comparison of Deterministic vs Stochastic Simulation Models for Assessing Adaptive Information Management Techniques over Disadvantaged Tactical Communication Networks.

Ginige, K., Amaratunga, D., & Haigh, R. (2009). Mainstreaming gender in disaster reduction: why and how? *Disaster Prevention and Management 18(1)*, 23-34.

Glass, R. (2004). A Look at the Economics of Open Source. *Communications of the ACM 47(2)*, 25-27.

Gold, A. (2010, January). *Toyota recalls 2.3 million cars for sticking pedals; your thoughts wanted*. Retrieved June 2012, from http://cars.about.com/b/2010/01/22/toyota-recalls-2-3-million-cars-for-sticking-pedals-your-thoughts-wanted.htm

Gopalakrishnan, C., & Okada, N. (2007). Designing new institutions for implementing integrated disaster risk management: key elements and future directions. *Disasters 31(4)*, 353-372.

Gregory, P. (2008). *IT Disaster Recovery Planning for Dummies.* Indiana: Wiley Publishing Inc.

Guliani, G., & Woods, D. (2005). *Open Source for the Enterprise.* United States of America,Sebastopol: O'Reilly Media, Inc.

Hamilton, D. C. (2010). *In-Crisis Decision Making: 'Resolving The Dilemma'.* Retrieved August 13, 2010, http://www.continuitycentral.com/feature0748.html

Hammond, B. (2007). Planning for Business Resilience. *Business Continuity Today* 3(2), 1-15.

Helms, R. W., van Oorschot, S., Herweijer, J., & Plas, M. (2006). *An integral IT continuity framework for undisrupted business operations.* Paper prestented at the 2006 Proceedings of the First International Conference on Availability, Reliability and Security, Netherlands. Retrieved June 12, 2010, from IEEE database.

Heschl, J. (2006). *Cobit Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0.* United States of America: IT Governance Institute.

Hiles, A. (2011). *The Definitive Handbook of Business Continuity Management Third Edition.* West Sussex: John Wiley & Sons, Ltd.

Hill, D., & Haslag, K. (2010). *IT Continuity Management Roadmap: A Process for Identifying and Reducing IT Vulnerabilites*. Retrieved from http://www.secureitconf.com/OLD/2009/documents/Presentation-ITContinuityManagementRoadmap 000.pdf

Hiltz, S. R., & Johnson, K. (1990). User satisfaction with computer-mediated communications system. *Management Science, 36(6)*, 739-743.

Hinca, M. (2006). Business continuity and disaster recovery for IS. Thesis. Masarykova University. Retrieved August6, 2010, from Masarykova University ofTechnology Digital Theses.

Ho, P. (2010). *Accident Causation Model.* Retrieved August 10, 2011, from http://www.cpti.com.hk/Download/63531/CHAPTER3.pdf

Hollnagel, E. (2008). The Changing Nature Of Risks. *Ergonomics Australia Journal 22(1-2)*, 33-46.

Holmes, R. (2010). *Consulting Services Master Proposal: Specially prepared for Sanlam.* Cape Town: ContinuitySA (Pty) Ltd.

Honour, D. (2007). *Business Continuity Resolutions for 2007.* Retrieved May 17, 2010, from http://www.continuitycentral.com/feature0423.htm

Inelmen, K., Say, A. I., & Kabasakal, H. (2004). Participation Lethargy in Disaster Preparedness Organizations within the Framework of a Turkish CBO. *International Journal of Sociology and Social Policy 24(10)*, 130-158.

Insight Consulting. (2008). *Continuity Planning for Information Technology and Communications*. Surrey, UK: Siemens.

Irin. (2011). *South Africa: Floods highlight lack of disaster preparedness*. Retrieved May 04, 2011, from http://www.irinnews.org/Report.aspx?ReportID=91754

Kadlec, C., & Shropshire, J. (2009). *Establishing the IT Disaster Recovery Planning Construct*. Paper presented at the 2009 Proceedings of the Fifteenth Americas Conference on Information Systems AMCIS2009, San Francisco, California. Retrieved June 21, 2010, from AIS Electronic Library (AISeL).

Keeton, K., Santos, C., Beyer, D., Chase, J., & Wilkes, J. (2004, March). *Designing for disasters*. Paper presented at the 2004 Proceedings of the 3rd USENIX Conference on File and Storage Technologies, San Francisco, California. Retrieved June 21, 2010, from AIS Electronic Library (AISeL).

Kelly, C. (1999). Simplifying disasters: developing a model for complex non-linear events. *Australian Journal of Emergency Management*, 14(1), 25.

Kumar, S. (2009). Business Resiliency. Retrieved from http://www-07.ibm.com/my/smarterbusiness/meettheexperts/pdf/Surviving IT Disaster with IBM Business Continuity and Resiliency Services.pdf

Leavitt, H. J., & Whisler, T. L. (1958). Management in the 1980's. *Harvard Business Review, 36(6)*, 41-41.

Lloyd, R. (2009, September). *Metric mishap caused loss of NASA orbiter.* Retrieved June 2012, from http://edition.cnn.com/TECH/space/9909/30/mars.metric.02/

Louth, J. (2011). From Newton to Newtonianism: Reductionism and the Development of the Social Sciences. *Complexity and Organization, 13(4)*, 63-83.

Macintosh-Murray, A., & Choo, C. W. (2002). *Information failures and catastrophes: What can we learn by linking information studies and disaster research?*. Proceedings of the American Society for Information Science and Technology, 39(1), 239-249.

Maes, J. (1994). Blaming the victim: Belief in control or belief in justice? *Social Justice Research 7(1)*, 69-90.

Maiwald, E., & Sieglein, W. (2002). Developing Contingency Plans. In B. A. Nordin (Eds.), *Security Planning & Disaster Recovery* (pp.177 - 237). California: McGraw-Hill/Osborne.

Maruna, S., & Mann, R. (2006). A fundamental attribution error? Rethinking cognitive distortions. *Legal and Criminological Psychology 11(4)*, 155–177.

Marvell, S., & Watson, I. (2006, March 01). *Aligning Business Continuity and Information Security*.Paper presented at the 2006 Information Security Forum Limited (ISF), London, UK. Retrieved June 21, 2010, from Information Security Forum (ISF) database.

Masters, I. (2004). *Dealing with downtime*. Retrieved fromhttp://www.continuitycentral.com/feature0135.htm

Mawson, N., & McConnachie, K. (2011). *Vodacom meltdown.* Retrieved July 06, 2011, from http://www.itweb.co.za/index.php?option=com content&view=article&id=45031:vodacom-meltdown&catid=76

Mays, N., & Pope, C. (1995). Rigour And Qualitative Research. *British Medical Journal, 311(6997)*, 109-112.

Mills Consulting Group. (2005). *Stop. Start. Continue.Fostering effective team behaviors through communication*. Retrieved June 23, 2012, from MillsGroup.co.za: http://millsgroup.ca/Tips/MCG Stop Start Continue.pdf

Nakamura, T., & Kijima, K. (2008). *Failure or Foresight: Learning from System Failures Through Dynamic Model.* PhD Thesis. Tokyo Institute of Technology. Retrieved June 21, 2010, from Graduate School of Decision Science and Technology Digital Theses.

Nasreen, M. (2004). Disaster Research: Exploring Sociological Approach to Disaster in Bangladesh. *Bangladesh e-Journal of Sociology. 1(2)*, 1-8.

Nelson, K. (2000). A Contingency Model of IT Disaster Recovery Planning. Paper presented at the 2000 AMCIS (Americas Conference on Information Systems) Proceedings, Detroit. Retrieved June 21, 2010, from AISeL (AIS Electronic Library).

News24. (2011). *Eskom reassures on nuclear safety.* Retrieved April 04, 2011, from http://www.fin24.com/Companies/Industrial/Eskom-reassures-on-nuclear-safety-20110314.

Nielsen, J. (2008). *Business continuity in South African: the top ten challenges for 2008 .* Retrieved May 17, 2010, from http://www.continuitycentral.com/feature0540.htm.

Orlikowski, W. J. (1996). Improvising Organizational Transformation over Time: A Situated Change Perspective. *Information Systems Research 7(1)*, 63-92.

Paton, D. (2003). Disaster Preparedness: a social-cognitive perspective. *Disaster and Prevention Management 12(3)*, 210-216.

Perrow, C. (1967). A framework for the comparative analysis of organizations. *American Sociological Review 32(2)*, 194-208.

Perry, R. W., & Lindell, M. K. (2003). Preparedness for Emergency Response: Guidelines for the Emergency Planning Process. *Disasters 27(4)*, 336–350.

Rasmussen, J., Nixon, P., & Warner, F. (1990). Human Error and the Problem of Causality in Analysis of Accidents [and Discussion]. *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences* 327(1241), 449-462.

Reason, J. (1990). The Contribution of Latent Human Failures to the Breakdown of Complex Systems. *Philosophical Transactions of the Royal Society of London: Human Factors in Hazardous Situations 327(1241),* 475 - 478.

Reason, J. (2000). Human error: models and management. *Business Management Journal 320(1)*, 768–770.

Reason, J. T., Carthey, J., & de Leval, M. R. (2001). Diagnosing “vulnerable system syndrome”: an essential prerequisite to effective risk management. *Quality in Health Care 10(2)*, 21-25.

Regensberg, D. (2008). What is your practice’s financial health like? *Private Nursing Practioners 12(5)*, 8-10.

Richardson, B. (1994). Socio-Technical Disasters: Profile and Prevalence. *Disaster Prevention and Management 3(4)*, 41-69.

Ridley, G., Young, J., & Carroll, P. (2004). *COBIT and its Utilization: A framework from the literature*. Paper presented at the 2004 Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii. Retrieved June 12, 2000, from University of Tasmania Digital Database.

Roberts, K. H., Bea, R., & Bartles, D. L. (2001). Must Accidents Happen? Lessons from High-Reliability Organizations. *The Academy of Management Executive15(3)*, 70-79.

Sagan, S. D. (2004). Learning from Normal Accidents. *Organization & Environment 17(1)*, 15-19.

Saint-Germain, R. (2005). Information Security Management Best Practise based on ISO/IEC 17799. *The Information Management Journal July/August*, 60-66.

Sanna, L., Schwarz, N., & Small, E. (2002). Accessibility experiences and the hindsight bias: I knew it all along versus it could never have happened. *Memory and Cognition 30(8)*, 1288-1296.

Saunders, M., Lewis, P., & Thornhill, A. (2003). *Research Methods for Business Students.* England: Prentice Hall.

Schopp, A., Plant, J., Uzkalnis, A., Bengree, C., Murane, I., Van Boxtel, P., et al. (2006). *Aligning Business Continuity and Information Security.* London: Information Security Forum.

Seel, R. (2000). Culture and Complexity: New Insights on Organisational Change. *Culture & Complexity: Organisations and People 7(2)*, 2-9.

Shaluf, I. M. (2006). Disaster types in Malaysia:an overview. *Disaster Prevention and Management 15(2)*, 286-298.

Shaluf, I. M. (2007). An overview on disasters. *Disaster Prevention and Management 16(5)*, 687-703.

Shaluf, I. M. (2007). Disaster types. *Disaster Prevention and Management16(5)*, 704-717.

Shaluf, I. M. (2008). Technological disaster stages and management. *Disaster Prevention and Management 17(1)*, 114-126.

Shaluf, I. M., Ahmadun, F.-r., & Mustapha, S. (2003). Technological disaster's criteria and models. *Disaster Prevention and Management 12(4)*, 305-311.

Shaluf, I. M., Ahmadun, F.-r., & Said, A. M. (2003). Review of Disaster and Crisis. *Disaster Prevention and Management 12(1)*, 24-32.

Shaluf, I. M., Ahmadun, F.-R., & Shariff, A. R. (2003). Technological disaster factors. *Journal of Loss Prevention in the Process Industries 16*, 513–521.

Shaluf, I. M., Ahmadun, F.-r., Mustapha, S., Said, A. M., & Sharif, R. (2002). Bright Sparklers fire and explosion: the lessons learned. *Disaster Prevention and Management 11(3)*, 214 - 221.

Shaluf, I. M., Ahmadun, F.-R., Said, A. M., Sharif, R., & Mustapha, S. (2002). Technological man-made disaster precondition phase for major accidents. *Disaster Prevention and Management 11(5)*, 380-388.

Shaw, R., Shiwaku, K., Kobayashi, H., & Kobayashi, M. (2004). Linking experience, education, perception and earthquake preparedness. *Disaster Prevention and Management 13(1)*, 39-49.

Shields, G. (2009). Defining the Peril of Application Downtime. Retrieved from http://nexus.realtimepublishers.com/esbbraf.php?utm source=feedburner&utm medium=feed&utm campaign=Feed%3A+RealtimeNexusEbookAlerts+%28Realtime+Nexus%3A+Expert+Information+Technology+Book+alerts%29

Shrivastava, P., Mitroff, I. I., Miller, D., & Miclani, A. (1988). Understanding Industrial Crisis. *Journal of Management Studies 25(14)*, 285-303.

Smith, A. G. (2010). Top 10 Business Continuity issues South African companies will face in 2010. Retrieved from http://www.google.co.za/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CDQQFjAA&url=http%3A%2F%2Fwww.continuitysa.co.za%2F literature 33350%2FTop 10 business continuity issues South-African companies will face in 2010&ei=44-bUMGmFqjs0gXFnYGYBQ&usg=AFQjCNF1NFl GCL9FRwlVHKa9jzk8dHlpA

Speight, P. (2007). *Crisis & Contingency Planning is Part of the Risk Assessment Cycle*. Retrieved May 04, 2011, from http://www.asis.org.uk/documents/Crisis and Contingency.doc.

Srivantaneeyakul, Y. (2007). *Moving Towards Business Continuity and Disaster Recovery Trends*. Paper presented at the 2007 Symposium on Interactive Windows II Pro Forum '07, North America. Retrieved June 21, 2010, from Metro Systems Corporation PCL database.

Stride, R. (2007). *Disaster invocations in South Africa - what are the causes?* Retrieved July 01, 2011, from http://cbr.co.za/article.aspx?pklarticleid=4234

Strydom, A. (2009). *Don't cut back on Business Continuity.* Retrieved from http://www.brainstormmag.co.za/index.php?option=com content&view=article&id=2177:dont-cut-back-on-business-continuity

Sullivan, J., & Beach, R. (2003). *Understanding System Development and Operation in High Reliability Organizations: a conceptual model.*Paper presented at the 20031st Conference Proceedings of The Security Conference, Virginia. Retrieved June 21, 2010, fromUniversity of Bradford Database.

SunGard. (2009). *SunGard publishes 2009 business continuity invocations log.* Retrieved May 07, 2010, from http://www.continuitycentral.com/news05189.html

Swuste, P. (2007). Qualitative Methods for Occupational Risk Prevention Strategies in Safety, or Control Banding-Safety. *Safety Science Monitor 11(3)*, 1-7.

Tekeli-Yesil, S. (2006). Factors affecting peoples' mitigation activities and preparedness for an earthquake in Istanbul, a qualitative study. Thesis. University of Basel. Retrieved June 21, 2010, from Tropical Institute Department of Epidemiology and Public Health; Institute of Social and Preventive Medicine Digital Theses.

Tekeli-Yesil, S., Dedeoglu, N., Braun-Fahrlaender, C., & Tanner, M. (2010). Factors Motivating Individuals to Take Precautionary Action for an Expected Earthquake in Istanbul. *Risk Analysis 30(8)*, 1181-1195.

Tetzlaff, B. (2001, September 06). Normal Accidents: A Book Report. In C. Perrow (Eds.), *Normal Accidents* (pp. 1-38). New Jersey: Princeton University Press.

The Business Continuity Institute. (2010). *Insurance Sector Views on Business Continuity*. Retrieved from http://a/wp-content/uploads/2012/06/CII -Business-Continuity-Joint-Report-HiRes FINAL.pdf rtcosolution.com

The New York Times. (2011). *Earthquake, Tsunami and Nuclear Crisis.* Retrieved May 04, 2011, from http://topics.nytimes.com/top/news/international/countriesandterritories/japan/index.html

Toigi, J. W. (2003). *Disaster Recovery Planning: Preparing for the Unthinkable.* New Jersey: Prentice Hall.

Turner, B. A. (1976). The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly 21(3)*, 378-397.

Turner, B. A. (1994). Causes of Disaster: Sloppy Management. *British Journal of Management 5*, 215 - 219.

Ven, K., & Verelst, J. (2006). The Organisational Adoption of Open Source Server Software by Belgian Organisations. *IFIP (International Federation for Information Processing) 203*, 111 - 122.

Vision Solutions. (2009). Chapter 8: Recovery:Strategies for Resilience. In Business Continuity Today (pp. 1-24). Vision Solutions.

Vision Solutions; IBM. (2009). BCROI: Measuring Returns on Your Business Investment. Retrieved from http://cio.ittoolbox.com/research/bcroi-measuring-returns-on-your-business-investment-23592

Wallace, M., & Webber, L. (2011). *The Disaster Recovery Handbook.* New York: American Management Assoication.

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.

Wong, T. S. (2006). *A Framework for Evaluating the Components of a Disaster Recovery Plan (DRP) for Academic Institutions.* Masters Thesis. University of Houston. Retrieved June 21, 2010, from The University of Houston Faculty of the Department of Information & Logistics Technology Digital Theses.

Woodman, P., & Kumar, D. V. (2009). A Decade of Living Dangerously: The Business Continuity Management Report 2009. London: Chartered Management Institute.

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

Wunnava, S., & Ellis, S. (2009). *IT Capability: A Moderator Model of Competitive Advantage*. Paper presented at the 2009 Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco. Retrieved June 21, 2010, from Association for Information Systems database.

Yin, R. K. (1981). The Case Study Crisis: Some Answers. *Administrative Science Quarterly 26(1)*, 58-65.

Appendices

APPENDIX A: Overview of the Analysis Process

1. The RDC Tests and the HA tests yielded issues which were logged in the Problem Management Tool, and a sample of the report is reflected in the table below:

Ref number:	Issue	Logged by:	Assignee Group
2228425	On Demand: Server failed while accessing folder backup	Ilse Van Beulen	Application Team A
2228426	Content Manager : IMS Socket Time out	Ilse Van Beulen	Application Team B
2228427	LID: Failed to connect to IMS	Ilse Van Beulen	Service Provider B
2228428	NUB OMS: Jistel: Connection timed out	Ilse Van Beulen	Service Provider A
2228429	Unable to establish session : Req session failed. IMSP	Ilse Van Beulen	Service Provider B
2229110	SRV000548 - User says that server is not starting up. Deployment manager. Please investigate.	Ilse Van Beulen	Service Provider B

2. Each issue was assigned to a category and, on a more granular level, to a cause within a category. In the sample below, Ref number 2228428 is expanded on:

Ref number:	Issue	Logged by:	Assignee Group	Category	Cause
2228428	NUB OMS: Jistel: Connection timed out	Ilse Van Beulen	Service Provider A	Network	Slow Response

3. Each test contained in the study went through the same process. Once all 7 tests were assigned to categories and causes (incomplete sentence).
4. A year-on-year comparison was done, and this yielded a list of recurring issues between the successive tests over 2009 and 2010. These issues then served as the basis for the questionnaire, i.e. they served directly as the basis for some of the questions such as: “Why do recurring issues occur?”. The questions were adapted to suit the study, e.g. where I needed to understand why we experience recurring slow network responses, I had to postulate the question: “why do we experience slow network responses?”. However, to ensure that the question was generic enough so that all the service providers, service line managers and IT development could answer the question, I omitted the “slow network response” and posed the question as: “why do we experience recurring issues?” Where recurring issues yielded items such as Apathy, I needed to understand what the contributing factors were, i.e. did people not have enough experience of disasters, which came across as apathy, or could people just really not be bothered? I went to literature to elevate the HOT factor issues attributed to apathy to posing a question.
5. All questions in the questionnaire were developed in the light of a perceived recurring issue. A full list of the questions can be found in Appendix C.

APPENDIX B: Linking Propositions to the Literature Review

Nr	Question	Propositions	HOT Factor	Literature Review
1	Why do we experience recurring issues during DCN and HA tests and how do we prevent these from occurring in future?	Research Question 1	-	• "holes" or vulnerabilities are present all the time, (Roberts, et al., 2001). Pg.34. • A result of this phenomenon is that companies may ignore the warning signs and alarms because people associate them with testing or malfunction rather than with genuine emergencies (Chapman, 2005). Pg. 35.
2	Which factors contribute to resources not taking corrective actions which stem from previous DCN / HA tests?	Research Question 1	-	• Even when information is available, it is not always made use of, either because recipients do not attend to it, or because they fail to see its significance thereof (Nakamura & Kijima, 2008). Pg. 33. • Man-made disasters, also known as technological or socio-technical disasters, are those disastrous events which arise from human decisions. (Shaluf et al., 2002; 2003b; 2003c; Shaluf, 2006; 2007a; 2007b). Pg. 19. • A multiplicity of minor causes, misperceptions, misunderstandings and miscommunications accumulate unnoticed during the incubation period (Figure 3, stage II) (Turner, 1994) Pg. 27.
3	IT Continuity is viewed as an overhead, protecting against something that may never happen and not contributing directly to 'the bottom-line'. In your view, why is this statement justified / not justified?	Proposition 3.1.2.3: Cost Justification	Organisational	• IT Continuity faces various challenges, the most conspicuous being that "like life insurance, IT Continuity is a 'grudge' insurance", and since IT continuity is regarded as an expense which safeguards the company against an event which may never happen, it is problematic to demonstrate a Return on Investment (ROI) in IT continuity (Vision Solutions, 2009; Strydom, 2009).Pg. 13

4	Remote Data Centre: End of Life (EOL) Technology is used in DCN and thus the infrastructure is quite old. Thus testing is not always like on like technology (servers of a later generation in production). Wat is your opinion of the statement and how does it impact on you?	Proposition 3.1.3.1: Compatibility and Complexity	Technological	• The increasing complexity, rapid change and growing size of technical systems affects the capability of the designers to predict and supply the means to control, the relevant disturbances to an acceptable degree of completeness and consequently the ability of the operating staff to cope with unforeseen and rare disturbances (Rasmussen, et al., 1990). Pg. 29. • Technological problems which include defective equipment and faulty design play a part in the creation and amplification of crisis (Richardson, 1994). Pg. 34.
5	In your experience / view, what are the frustrations with IT Continuity?	Proposition 3.1.2.1: Available Resources	Organisational	• Root causes of catastrophes are inadvertently embedded in operational systems, latent until an undesirable combination of events occurs. This means that small problems can cascade into disasters if they aren't stopped by pre-planned organisational, technical, or procedural defences (Swuste, 2007; Reason, 1990). Pg. 35.
6	What must be done to alleviate the frustrations? i.e. How can we improve your experience with Continuity? How do we increase the focus and commitment to Continuity efforts?	Proposition 3.1.2.1: Available Resources	Organisational	• Failures and near misses can be seen as occasions for shame or as incidents to be covered up, but they can also be understood as learning opportunities (Turner, 1994). Pg. 30.
7	What is your managers' view of IT Continuity efforts? How does this impact on / influence your outlook toward continuity efforts?	Proposition 3.1.1.1: Credibility	Human	• In a survey done by AT&T (2008), one third of IT executives were unaware of what their continuity or recovery plans comprised of and many admitted that their respective companies had no plans in place pg. 12
8	Have you ever experienced a disaster?	Proposition 3.1.1.2: Terms of Reference	Human	• human factors which can cause recurring issues e.g. experience (Reason, et al., 2001). Pg. 29. • The 'it won't happen to us' syndrome prevalent in large companies is an example of 'rigidities in institutional beliefs' posited by Turner (1976; 1994). Pg. 31

9	Is IT Continuity justified?	Proposition 3.1.1.2: Terms of Reference	Human	• Organisations continue to be complacent on the subject of continuity (Srivantaneeyakul, 2007) pg. 13
10	The DCN tests are bi-annual and because the Mainframe is unavailable outside of these slots, testing between these phases is not possible. What impact does this have on you?	Proposition 3.1.3.2: Trialability / Testability	Technological	• Therefore "fallible decisions" are part of the design and management processes, and the focus should be on ensuring that any adverse consequences are detectable and recoverable (Dekker, et al., 2008). Pg. 28
11	Do you receive the necessary support during tests from vendors, managers etc. If not, please substantiate your answer	Proposition 3.1.2.1: Available Resources	Organisational	• Organisational inadequacies (Organisational factors, Figure 6) are comprised of policy failures, insufficient resources allocations, strategic business pressure leading to a neglect of safety issues, communication breakdowns etc. Pg. 27
12	What must we stop doing? What must we continue doing? What must we start doing?	Research Question 2	-	• Organisations fall into the incompetence trap and learn to do the wrong thing better. This period is characterised by sufficient time for all the minor events to interact and accumulate to produce major system failure (Shaluf et al., 2002b; Shaluf et al., 2003b; Shaluf, 2008). Pg. 40.
13	"IT Continuity is mandatory and the company can be fined if we do not adhere"…are you aware of policies, SLA's etc? If not, what must be done to ensure that such awareness is raised?	Proposition 3.1.2.2: Legislation and Standards	Organisational	• Patterns of responsibility and awareness of statutory obligations and communications between top management, middle management, and operational resources are often lacking (Turner, 1976). Pg. 32.

APPENDIX C: Questionnaire

	Question
1	Why do we experience recurring issues during the DRN tests and how do we prevent these from occurring in future?
2	Which factors contribute to resources not taking corrective actions which stem from previous DRN / HA tests?
3	IT Continuity is viewed as an overhead, protecting against something that may never happen and not contributing directly to 'the bottom-line'. In your view, why is this statement justified / not justified?
4	Remote Data Centre: End of Life (EOL) Technology is used in DRN and thus the infrastructure is quite old. Thus testing is not always like on like technology (servers of a later generation in production). What is your opinion of the statement and how does it impact on you?
5	In your experience / view, what are the frustrations with IT Continuity?
6	What must be done to alleviate the frustrations? i.e. How can we improve your experience with Continuity? How do we increase the focus and commitment to Continuity efforts?
7	What is your manager'sview of IT Continuity efforts? How does this impact on / influence your outlook toward continuity efforts?
8	Have you ever experienced a disaster?
9	Is IT Continuity justified?
10	The DRN tests are bi-annual and because the Mainframe is unavailable outside of these slots, testing between these phases is not possible. What impact does this have on you?
11	Do you receive the necessary support during tests from service provides, managers etc. If not, please substantiate your answer
12	What must we stop doing? What must we continue doing? What must we start doing?
13	"IT Continuity is mandatory and the company can be fined if we do not adhere"…are you aware of policies, SLA's etc? If not, what must be done to ensure that such awareness is raised?

APPENDIX D: Ethics Form

Ethics in Research

It is the responsibility of the student/staff to complete an ethics form that involves the human subjects, or research the may hold ethical consequences for the University of Cape Town. A completed ethics form should be submitted to the Ethics Committee by the student/staff to the faculty they belong to, in this instance Faculty of Commerce. The following documents should be accompanying the ethics form:

- A full copy of the research design
- The signed consent form by the participants
- The interviewer should provide schedules, forms, instructions, planned question and any relevant material planned to be used in the study

---

A. PROJECT TITLE: *Investigating Recurring Impediments to Effective IT Continuity Management in a South African Insurance Firm*

A.1 Name of Principal Investigators: *Van Beulen Ilse*

A.2 Primary research methodology (outline the main research tool being use i.e. interviews, experiments, secondary data use etc.):

Case study research utilising semi-structured interviews, studying and analysis of existing company documents.

B. CHARACTERISTICS OF STUDY PARTICIPANTS:

In this section, please describe the characteristics of the individuals who will be participating in the study. (This includes interview respondents, experimental subjects etc).

B.1 Gender, race or ethnic group, age range, location etc.

There is no gender, race, ethnic group nor age discrimination. The interviewees will be taken from employees from the company used as a case study.

B.2 Affiliation of subjects, e.g., institutions, hospitals, general public, etc.

Employees and management of Company X.

B.3 If human subjects are either children (aged 15 and below), mentally incompetent, or legally restricted people/groups please explain why it is necessary to use these particular groups

There are neither minors, mentally incompetent, nor legally restricted people or groups participating in this study.

APPENDIX E: TYPE OF CONSENT

C.1 What type of consent will be obtained from study participants?

It will be a written consent form and with all the relevant details the person needs to know before the participation in the study. However, if participant is not willing to sign the consent form, the planned interaction will be terminated.

C.2 If participants are required to sign a written consent form, please submit a copy of the consent from with your application. If there is no written consent, please provide a motivation as to why this is not the case.

The consent form has been attached; it is called the "Interview Consent Form".

C.3 How and where will consent/permission be recorded?

By interviewee reading the consent form, being explained and prompted questions concerning the consent form details by interviewer to ensure mutual understanding of the consent form.

APPENDIX F: CONFIDENTIALITY OF DATA

D.1. What precautions will be taken to safeguard identifiable records of individuals? These questions also apply if you are using secondary sources of data. Please describe specific procedures to be used to provide confidentiality of data by you and others, in both the short and long run.

Information that can be used against the organisationand people representing organisation will be masked during analysis. The data collected will be disposed of as soon as the analysis is completed.

APPENDIX G: RISKS TO SUBJECTS

E.1. Describe in detail the extent of any physical, psychological, social, legal, economic, or other risks to study participants you can foresee, both immediate and long range, and provide the rationale for the necessity of such risks.

The employee's privacy might be at risk due to employees perceiving certain things personal and private. Company have certain routines, operations and communication private and/or perceive private. Thus they might not want to expose certain aspects of their business due to privacy infringement.

E.2. Where possible, outline any alternative approaches that were or will be considered and why alternatives may not be feasible in the study. Also outline whether and why you feel that the value of information to be gained outweighs the risks?

N/A

E.3. ADDITIONAL COMMENTS:

N/A

Van Beulen Ilse's SIGNATURE: **DATE:**