A framework to enhance Information and Communication Technology (ICT) readiness for business continuity at the South African Revenue Services (SARS)

By

Euphodia Mathase

Submitted in fulfilment of the requirements for the degree of Master of Philosophy in IT Governance to be awarded at the Nelson Mandela University

December 2020

Supervisor: Prof Houdini Fourie

Co-Supervisor: Mr T. Jagwanth

Research is subject to a confidentiality agreement

DECLARATION

I, Euphodia Mathase, Student number S219713790, hereby declare that the treatise for Master of Philosophy in IT Governance qualification to be awarded is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

……………………………

Euphodia Mathase

18 November 2020

LIST OF ACRONYMS AND ABBREVIATIONS

ADRC	Asian Disaster Reduction Centre
APP	annual performance plan
BC	business continuity
BC/DRP	business continuity and disaster recovery plan
BCM	business continuity management
BCMS	business continuity management system
BCP	business continuity plan/planning
BIA	business impact analysis
CAPEX	capital expenditure
CBM	continuous business management
CSF	critical success factors
DOIS	design-oriented IS
DRP	disaster recovery planning
DS	design science
DSR	design science research
ICT	information and communication technology
IRBC	ICT readiness for business continuity
IS	information systems
IT	information technology
ODSR	ontology-based design science
OECD	Organisation for Economic Co-operation and Development
RBV	resource-based view
SARS	South African Revenue Services

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Many organisations, especially public sector organisations, are required to ensure that they are able to continue with their operation in cases of major disasters that affect the organisations. In the same light, the South African Revenue Services (SARS), being a quasi-government organisation, faces a similar phenomenon. The main purpose of conducting this research was to explore a problem in depth that was identified at the SARS. SARS does not have a comprehensive business continuity plan. The study therefore examined possible techniques or actions for ensuring information and communication technology (ICT) readiness and business continuity, explored various frameworks and policy documents which will assist public entities with readiness for business continuity, and identified frameworks that will assist SARS in implementing an effective ICT readiness for business continuity. The study adopted the design science research approach and aspects of design science research in information systems. Data gathered through the questionnaire instrument was used to design a framework that can be adopted at SARS to enhance ICT readiness for business continuity. The research findings show the importance of effective business continuity management (BCM) and a framework that can be used to implement an effective BCM.

Keywords:
Business continuity management, Disaster Recovery Planning (DRP), ICT Readiness for business continuity, Information Technology, IT continuity,

CHAPTER 1
INTRODUCTION

1.1. INTRODUCTION

The main purpose of this research was to explore, in depth, a problem that was identified at the South Africa Revenue Services (SARS). The subsections that follow discuss the background to the study, problem statement, research process/research design and ethical considerations to gain deeper knowledge of the research area.

1.2. BACKGROUND TO THE STUDY

In recent times, organisations are dependent on information and information technology (IT) in their daily operations. “Even though technology has made daily operations more effective and efficient for organisations, they still face the risk of business disruptions, which may hamper business operations significantly.” Royds, 2010). Such being the case, “business continuity management (BCM) becomes imperative for organisations to create, sustain, and improve organisation resilience, and information and communication technology (ICT) plays a key role in BCM (Hinson, 2012)”. According to Nicholas (2008), “Business continuity is a management process that identifies potential factors that threaten an organisation and provides a framework for building resilience and the capability for an effective response”. ICT readiness for business continuity (IRBC) is also key for organisations and it ensures that an organisation has the capability to support business operations by prevention and detection of and responding to disruption and recovery of ICT services. ISO/IEC 27031 (2011) states that “IRBC refers to a management system which complements and supports an organisation’s BCM or ISMS program, to improve the readiness of the organisation in responding and recovering”. There are various events or potential disasters that trigger organisations to implement business continuity and a disaster recovery plan (BC/DRP). Some of these could be natural disasters, inadvertent disasters (such as software problems, power failure), and deliberate actions (such as hackers, terrorists, bomb scares, labour unrest) which can all disrupt operations (Cook, 2015). These potential disasters or events ultimately have a negative impact on organisations such as loss of revenues, of reputation, of information, of access to facilities, and of personnel. It therefore becomes imperative for organisations to plan for continued critical operations of workflow functions, despite adversity and loss of support systems, by implementing good BC/DRPs.

1.3. PROBLEM STATEMENT

Public entities in South Africa, such as the South African Revenue Service, have tried to implement IRBC under their BCM programmes. However, there have been challenges in defining critical business activities that need to be recovered in the event of business disruptions. In addition, various departments have different perceptions of what is termed “critical”, when it comes to ICT operations. In an event where SARS faces disruptions in its business operation, it may not be able to resume operation timeously and efficiently. This results in loss of productivity, loss of critical data and loss of revenue, among other negative consequences and negative reputation. Based on these challenges, the questions that arise are:

- Does SARS management have a solid understanding of IRBC to resume operation timeously?
- How well are they prepared for business affecting emergencies?
- What steps can be put in place to restore business and IT systems in the event of a disaster?

1.3.1. Treatise statement

A suitable IRBC framework can assist SARS to have ICT readiness for business continuity in the event of business or IT incidents or related disruptions that could affect critical business functions.

1.3.2. Research objectives

The primary research objective was to develop a framework which SARS can use to ensure that their IRBC is effective and reduces the impact of information incidents on the organisation. The primary objectives were further divided into secondary objectives. The following secondary objectives were derived from the primary objective:

- To investigate the board members’ responsibilities in IRBC and BCM, and their awareness of these responsibilities.

- To investigate possible techniques or actions for ensuring ICT readiness and business continuity in SARS.
- To investigate typical frameworks and policy documents which will assist SARS with ICT readiness for business continuity.
- To develop and recommend a suitable framework that will assist SARS in implementing an effective IRBC.

1.3.3. Research questions

1. What are the board members' responsibilities in IRBC and BCM, and are they aware of these responsibilities?
2. What actions need to be taken to ensure that there is ICT readiness and business continuity in public entities?
3. What typical frameworks exist, and which elements can be extracted from these frameworks to come up with a possible framework for ICT readiness for business continuity?
4. What framework will be suitable to assist public entities in implementing an effective IRBC?

1.3.4. Delineation

The scope of this study was restricted to South African Revenue Service.

1.4. RESEARCH PROCESS/RESEARCH DESIGN

The design science (DS) paradigm was used in the development of the IRBC framework because it assists in guiding researchers in developing an artefact through their research. Its objective is to develop knowledge that can be used by other professionals. Armstrong and Armstrong (2010) stated that "design science is not just a methodology for devising solutions utilising technology. It is an approach that offers the researcher the ability to investigate problem spaces and devise theories and designs that could address such problem spaces".

Wieringa (2014) stated that design science iterates in two activities which are designing an artefact that improves something and investigating the performance of an artefact. According to Peffers, Tuunanen, Rothenberger and Chatterjee (2007), the design science research methodology incorporates principles, practices and procedures that are consistent with prior literature; it provides a process model and a mental model for presenting and evaluating DS research in IS.

Peffers et al. (2007) set out the DS process as follows:

- problem identification and motivation;
- definition of the objectives for a solution;
- design and development;
- demonstration;
- evaluation; and
- communication.

The design science research paradigm in the information systems field encourages the creation and evaluation of artefacts/outcomes as a means for research. The research is aimed at providing a solution to how an organisation can recover its IT operations after a disruption. As mentioned by Peffers et al. (2007), the design science approach is intended for a design type of study. Therefore, the design science research approach was deemed appropriate for this research. De Leoz and Petter (2018) suggested that “design science researchers often create and evaluate artefacts that tend to be techno-centric. By also considering the social impacts of a design science artefact throughout the creation and evaluation process, the researcher develops an artefact with a greater potential to thrive when the artefact is instantiated and implemented”.

This study was conducted at SARS as the sample organisation. A literature review was conducted to gain an understanding of the environment and to help define the objective of the IRBC framework. Interviews were conducted on the readiness of the ICT department to respond to business disruptions. This included information on their recent and previous ICT readiness for business continuity. The ICT department personnel comprised the population from which a sample was selected to be interviewed.

1.5. ETHICAL CONSIDERATIONS

The research has conformed to the Research Ethics Policy of the Nelson Mandela University.

1.6. STRUCTURE OF THE TREATISE

Chapter 1: Introduction – This chapter outlines the research topic, objectives of the study; presents the problem statement and the key research questions.

Chapter 2: Literature Review – This chapter critically discusses the relevant literature relating to frameworks to enhance ICT readiness for business continuity within organisations.

Chapter 3: Research Methodology – This chapter explains the methods used in this research and comprises sections of design science research, population and sampling and the proposed conceptualisation of artefacts.

Chapter 4: Data Analysis and Presentation – This chapter comprises the presentation and analysis of results in order to answer the stipulated research questions.

Chapter 5: Summary Findings and Conclusions– This chapter explores the findings from the research and provides conclusions thereof.

Chapter 6: Validation of Framework and Recommendations for Further Study – This chapter validated the framework, discusses the limitations of the research, and provides recommendations for further studies.

CHAPTER 2
LITERATURE REVIEW

2.1. INTRODUCTION

A review of the literature, which is discussed in this chapter, was undertaken to examine literature related to business continuity management highlighting the importance of IRBC. The researcher also examined the literature for possible techniques or actions for ensuring ICT readiness and business continuity, explored various frameworks and policy documents which can assist SARS with ICT readiness for business continuity, and identified frameworks that will assist SARS in implementing an effective IRBC. In this presentation of the literature reviewed, the researcher will define SARS as a public entity, the entity's mandate, and state the rationale why it should have a comprehensive and effective BCM and DRP.

SARS has a disaster recovery plan that was solely developed by its ICT business unit. The organisation does not have a comprehensive BCM and DRP plan in place. This review will seek to investigate the importance of disaster recovery plan and business continuity management at SARS.

2.2. BUSINESS CONTINUITY MANAGEMENT DEFINITIONS

Business continuity is about developing and maintaining a capability around the non-IT elements of the business continuity management programme or system. It focuses on the core advisory services for the wider programme, such as policy, people and processes, including implemented strategies, response plans, training and exercise needs, whilst ensuring they are successfully embedded and maintained within the organisation (Nicholas, 2008). 'Resilience' is all about designing and implementing a robust IT infrastructure, with technical recovery strategies and solutions, effectively providing IT service continuity.

The term business continuity plan (BCP) refers to the identification and protection of critical business processes and resources required to maintain an acceptable level of business, protecting such resources and preparing procedures to ensure the survival of the organisation in times of business disruptions (Lou, Liu & Sio, 2010:220). Thus, the existence of the BCP enables the company to resume operations at the earliest opportunity without any further implication on the company in the event of an encounter with such contingencies.

Business continuity management (BCM) is based on the principle that it is the key responsibility of an organisation’s directors to ensure the continuation of its business operations at all times. It may be defined as: “a holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realized, 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” (Speight, 2011:2.4).

Royds (2010:6) defined BCM as “the means by which organisations design, develop, implement and maintain response and recovery measures in order to identify threats and vulnerabilities, while mitigating and managing the risks to services and operations, and the effects or consequences of disruption”. According to Nicholas (2008), “Business continuity is a management process that identifies potential factors that threaten an organisation and provides a framework for building resilience and the capability for an effective response”.

2.3. THE IMPORTANCE OF BUSINESS CONTINUITY MANAGEMENT

Business continuity management (BCM) has evolved into a process that identifies an organisation’s exposure to internal and external threats, providing effective prevention and recovery. It emerged out of the need for a mechanism to demonstrate the maturity of an organization’s business continuity management. Any incident that impairs a business's ability to function can negatively impact the organisation long after they resume normal operations. Integrating a business continuity management system into the organisation, demonstrates to business partners and customers that the organisation is dedicated to providing the best possible service at all times, regardless of interruption. (Lou et al., 2010, Nicholas, 2008; Speight, 2011).

Information technology (IT) and information system (IS) incidents affect business operations and, as many examples show, may also have severe business impacts. Organisations recognise IS continuity as a key information management issue (Luftman & Zadeh 2011). The reliability of the technology and the systems is the primary objective of information management, although extremely complex systems do not always deliver perfectly (Butler & Gray, 2006; Mithas, Ramasubbu & Sambamurthy, 2011).

One traditional approach to ensuring IT and IS continuity is through disaster recovery planning (DRP). Businesses have become convinced that they should make contingency plans for coping with IT and IS incidents, and ensure that backup copies are stored in a safe location (Chow & Ha, 2009). Are these measures sufficient? Is it possible to avoid incidents? The adoption of a strategic mindset for business continuity, is crucial as BCM is important in delivering value preservation to the organization in the forms of increased resistance to crises and higher reliability configurations. This implies that an organization must nevertheless, demonstrate the best possible service even if it cannot survive.

2.4. THE LACK OF BUSINESS CONTINUITY MANAGEMENT FRAMEWORKS

However, despite findings in commercial and academic studies suggesting their crucial importance for chief information officers, no frameworks for business or IS continuity management have been validated academically (Ernst & Young, 2011; Luftman & Zadeh, 2011). According to Ernst & Young's Global Information Security Survey (Ernst & Young 2011), organisations have perceived business continuity management, or DRP, as the most probable information security investment area. The International Organisation for Standardization and other bodies have developed several risk-management, business-continuity and information security standards, but they have been criticised as too general for companies with specific business needs (Siponen &Willison, 2009). In the case of SARS, there is no BCM but only a DRP. Very little investment has been made towards developing a BCM for the entire organisation.

In order to weaken the negative impact of IS incidents, organisations should prepare for them. In many countries, finance and healthcare sectors are required to ensure continuity in IS operations according to governmental regulations (Elliott, Swartz & Herbane, 2010). However, customers nowadays do not expect the delivery of products and services to be interrupted for any reason. The embeddedness of continuity practices facilitates the effective implementation of IS continuity management and requires stability and a clear organisational structure (Elliott et al., 2010). One way of embedding continuity in an organisation is to follow an international standard or framework that comprehensively integrates it into the processes.

BCM is the management processes that ensure the resilience of an organisation in the face of a range of business disruptions which evolved from DRP (A'Nasiren, Abdullah & Asmoni, 2016:105–122). Business continuity emerged in response to the increased corporate realisation that any disruption in the continuity of the business for an extended period of time will seriously affect the overall practicality of the company (Duncan, Yeager, Rucks, & Ginter, 2011:135–142). The authors explained the purpose of having BCM in organisations is to identify and protect the critical business processes, to maintain an acceptable level of business, and to ensure the survivability of the organisation in the times of business disruption caused by disasters or extreme events (ENISA, 2010). The readiness of an organisation in reacting to such disruption is very much dependent on how actively involved its management is in embracing the BCM (Pheng Low, Liu & Sio, 2010). SARS can benefit from implementing an effective BCM.

2.5. LACK OF GROWTH IN SOUTH AFRICAN ICT SECTOR

Techterms, (2017) state that ICT refers to "technologies that provide access to information through telecommunications." South Africa's economic struggles over the last five years have seen it lose its 'Africa's largest market' status to Nigeria. South Africa now competes with Egypt for second place, with a weak rand also reducing its purchasing power in the global market. As a result, the country's ICT sector has struggled to grow as impressively as in other countries, and contributed only 3% to GDP, according to the 2014 ICT Satellite Account (Stats SA, 2017).

While several smaller players in the market have welcomed its potential to increase both competition and equitable access to spectrum (TechCentral, 2018), larger operators and various industry interests have condemned this approach and cautioned against unintended outcomes, especially the negative impact on significant investment currently being made in mobile networks (ITWeb, 2018).

2.6. THE ROLE OF CRITICAL SUCCESS FACTORS (CSF) IN BUSINESS CONTINUITY MANAGEMENT

Critical success factors (CSF) first have to be identified and tailored to an organisation’s specific objectives, businesses, managers, environment in which the organisation operates and the strategies it has adopted (Asian Disaster Reduction Centre [ADRC] 2012). Thus, in terms of the BCM implementation, the CSFs are those conditions that must be met in order for its implementation to occur successfully.

According to the ISO 22301 (2012) standard, appropriate workforce planning in an organisation is an important facet of organisational resource mobilisation and that is a critical success factor of business continuity management, which then lead to positive outcomes of organisational performance. Effective organisational performance is as a result of sustained competitive advantage (Priem & Butler, 2001:22–40). Such a performance emanates from unique, valuable and non-substitutable resources which positively affect business continuity practices.

According to the ACI World Secretariat (2012), in order to develop or implement BCM, there needs to be a dedicated effort, driven by the top management team to define the BCM structure and oversee its implementation. Gallagher (2005:66–68), stressed that for BCM to work it must be driven and obtain clear and unequivocal support from the top. The author added that the single greatest influence that determines the state or condition of the plan, or the whole BCM process, is the degree of commitment to it by top management. Table 1 indicates the strategic and tactical critical success factors that are important in the successful implementation of BCM. The table indicates the strategic CSFs linking them with the relevant tactical CSFs.

Table 1: Strategic and tactical Critical Success Factors for business continuity management implementation

Strategic critical success factors	Tactical critical success factors
Top management commitment and support	Financial & budget utilisation
Industry-focused	Effective communication
Key stakeholders	Education & training of BCM
Human resources	Legislation
Cultural changes	Participation of facilities and staff
Ownerships	BCP committees
BCM organisation	Awareness campaign
	Leadership
	Input of BCM programme

Source: Researcher’s own construct from literature

By identifying CSF first when implementing BCM, SARS can ensure that their BCM is tailor-made for their environment and it meets their specific objectives.

2.7. REQUIREMENTS FOR AN EFFECTIVE IMPLEMENTATION OF BUSINESS CONTINUITY MANAGEMENT

2.7.1. Education and training for Business Continuity Management

The purpose and importance of education and training is due to the assurance of the benefits and objectives of the BCM strategy being communicated to the workforce and consequently achieving its objectives (Gibb & Buchanan 2006:128–141). Furthermore, Tammineedi (2010:36–50), training should be carried out as the content of training requirements vary depending upon the roles and different categories of employees. Momani (2010:272–279) insisted that training is needed in order to implement the BCM effectively, as each employee who has the responsibility in BCM implementation should receive proper training. SARS should train and educate employees and relevant stakeholder on BCM to ensure that they are able to respond and execute their responsibility effectively.

2.7.2. Effective communication

In ensuring the effectiveness of BCM implementation, BC professionals need widespread communication of the BCP to all necessary parties, starting from the board down to the most junior employees (Carley, 1993:75–126). Gallagher (2005:66–68) also highlighted that effective communication arrangements are essential to keep the staff informed of all developments, in case of emergency. The framework to be used to enhance BCM at SARS must incorporate how BCM should be communicated to all employees.

2.7.3. Cultural changes

The study made by Tammineedi (2010:36–50) found that to embed BCM in the organisation’s culture the BCM policy should be appropriate to the nature, scale, complexity, geography, and criticality of the business and must reflect the organisational culture, mission, vision and operating environment. Consequently, it offers the following: developing a BCM programme more efficiently; instilling confidence in the stakeholders in its ability to handle business disruptions; increasing its resilience over time by ensuring BCM implications are considered in decisions at all levels; and lastly, minimising the likelihood and impact of disruptions. Therefore, organisational culture will predict how BCM and any changes are handled (Garrett 2012). SARS, in the journey of enhancing their BCM should ensure that BCM is embedded in the organisation’s culture and apply necessary culture changes if there is a need to do so.

2.7.4. Key stakeholders

As highlighted by Woodman (2007), external drivers, such as key stakeholders, have been driving organisations in changing their approach to BCM, and the top driver for change remains existing customers, followed by the insurers of the organisations – thus representing an increasingly prominent force for the promotion of BCM. Finney and Corbett (2007:329–347) contended that an intimate understanding of the CSFs of various stakeholder groups would determine if the concerns of these relevant groups are being addressed as effectively as possible. Rasi, Raja, Abdekhodaee and Nagarajah (2014:132–149) also highlighted that as in any organisation, stakeholders in small and medium enterprises may have significant power to influence the efficiency and effectiveness of corporate activities. In light of SARS, as a tax collecting agency may require to have an effective BCM to reduce or even prevent business disruptions in order to be able to continue with its operations.

2.7.5. Organisational resources

Resources are broadly defined as the set of assets, capabilities, organisational processes, firm characteristics, information, and knowledge under the firm's control, allowing the firm to conceive of and realise strategies intended to increase its effectiveness (Barney 2002). Since the mid-1980s, the resource-based view of the firm has been widely viewed as an important strategic management theory. Further, the theory suggests that, as resources become redundant, companies must continually reinvent themselves through growth and investments, taking advantage of early adoption and deploying resources in sequence as they develop (Barney 2002).

Organisations have at least four types of resources (human, capital, physical and time) that can be used to achieve desired results. Verman (2011:11–36) reiterated that BCM development and implementation has the following levels of involvement of key personnel or teams. They include general management (25%), dedicated BCM department/person (16%), information technology (20%), risk management (12%) and finance and accounting personnel (5%). Johnson, Onwuegbuzie and Turner (2007:112–133) noted that resource allocation is a central management activity that allows for strategy execution. The authors further highlighted that resources should be allocated according to priorities established by annual objectives. Shuja and Abbasi (2015:2551–2558) highlighted that factors such as overprotection of resources, too great emphasis on short-run financial criteria, organisational politics, vague strategy targets, a reluctance to take risks and lack of sufficient knowledge prohibit effective resource allocation. Based on the previous argument, it is my opinion that SARS also needs to invest in technology to ensure that they have the required capacity and capabilities.

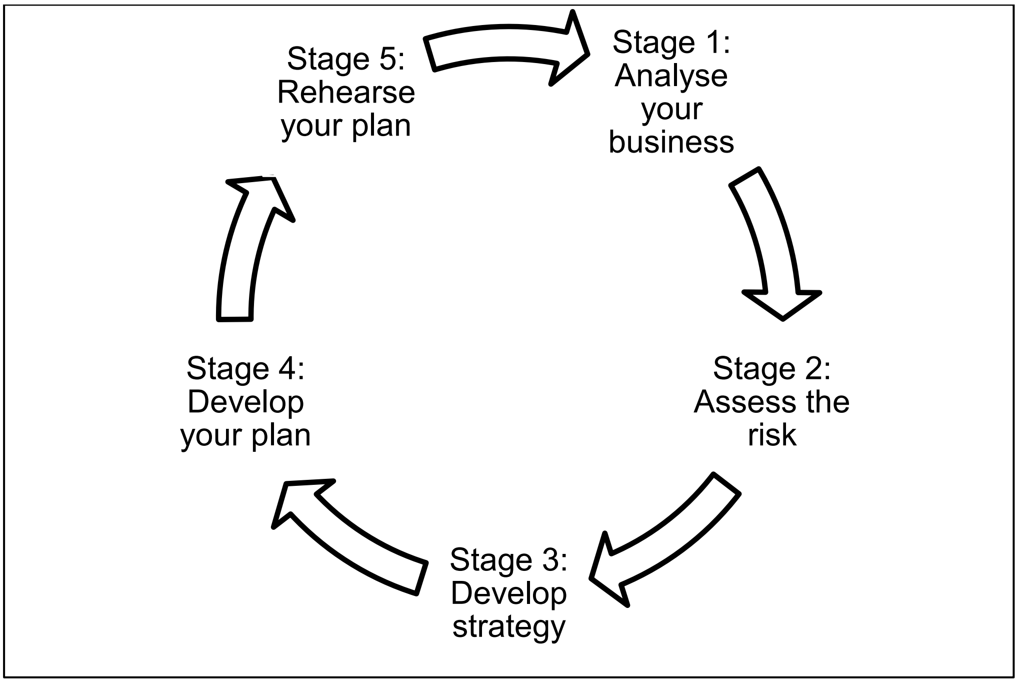
2.7.6. Human resources

Human resources can be evaluated from two points; key position is the one that incorporates the most important activities necessary to ensure key processes in an organisation, and the second is key individuals who have such competences, knowledge, skills and abilities, which are essential to achieve the required level of performance. Furthermore, BCM processes consist of sets of activities which are dependent upon human resources to initiate, enact, and control specific activities and on infrastructure, material, financial and information resources to provide the context and inputs (Gneist, Kiersz & Osman 2009). SARS should identify employees who will be involve in the implementation and the execution of the BCM. Furthermore, in my opinion, SARS should also ensure that knowledge transfer do take place as some knowledge might leave the organisation when employees resigns.

2.8. DISASTER RECOVERY PLANNING

An organization can implement business continuity and a disaster recovery plan as a result of a number of events or potential disasters that trigger crises. This is known as Business Crisis/Disaster Recovery Plan (BC/DRP). Some of these events which can disrupt all operations could be natural disasters, inadvertent disasters such as software problems or power failure. Others could be deliberate actions like hackers, terrorists, bomb scares, and labour unrests (Cook, 2015). These potential disasters or events ultimately have a negative impact on organisations such as loss of revenues, of reputation, of information, of access to facilities, and of personnel. Management should be concerned about the impact of these disasters in order to satisfy their customers' needs under these circumstances. It therefore becomes imperative for organisations to plan for continued critical operations of workflow functions, despite adversity and loss of support systems, by implementing good BC/DRPs. In the case of SARS, the organisation has a DRP in place to recover IT systems in an event or disruptions. However, there is no BCM that ensures continuity of other business activities. Hence the need for a framework to enhance the organisation's BCM. This has been documented as one of SARS' enterprise-wide risk in the SARS annual performance plan document. SARS (2019)

Figure 1: The BCM lifecycle



Source: Manchester Business Community Forum (2018)

Business continuity management requires a well-structured system as well as the following of the critical lifecycle stages depicted in the diagram above. The following are the basic stages of the BCM lifecycle

2.8.1. Stage 1 – Analyse your business

Understand what is critical to the business operations by undertaking a business impact analysis (BIA) to ensure the following:

- Key processes and interactions are identified.
- Critical activities are understood.
- Key resources are identified – people, IT systems, data/documentation, telecoms, essential stationary such as cheques and specialised equipment like a debit card machine.
- Define what is critical and what would be deemed to be a serious incident.

2.8.2. Stage 2 – Assess the risk

Maintain a list known as a risk register assessing the threats to the organisation. The threats are potentially very wide and varied, such as fire, power cuts, flooding, data loss, chemical leak, public transport strike, flu pandemic, terrorist threat, gas leak, severe weather, vandalism, postal strike or a telecommunications loss. The register should record both the likelihood and impact of the threats identified, as this will help prioritise actions, for example by focusing on the events identified as high likelihood to occur and high impact if they did occur.

2.8.3. Stage 3 – Develop strategy

Develop a business continuity strategy to cover what would do if an event (risk) occurred such as the following scenarios which may be the result of one of the above risks occurring:

- Inability to access or utilise building.
- Loss of IT or communications.
- Loss of key individuals or high absenteeism.
- External disruptive incident.
- Supply chain failure in developing the strategy.
- Service disruption is tolerable to the business.

2.8.4. Stage 4 – Develop plan

For larger, complex organisations made up of several teams, it is usually beneficial to have an overarching plan to manage a serious disruptive incident that sits above departmental plans. This overarching plan would cover, for example, management of the incident across the organisation including media and communications liaison. It is recommended by Departmental Business Continuity Management Team (2009) that each department must have a standard BCP owned by the departmental manager. This individual and their deputy should be familiar with the plan and understand how it will be deployed and how it links to the overarching plan.

2.9. RISE OF DIGITAL DISRUPTION

According to Christensen (1997); Gans (2016) the major technological disruption of today is digitalisation. Digitalisation is creating a virtual mirror image of reality, and a data layer has emerged on top of reality, which virtually recreates it.

Algorithms are making possible the full exploitation of Big Data (Domingos 2015). Sophisticated algorithms are necessary to put order in the massive amounts of data created by sensors, to make it relevant. Furthermore, algorithms are now incorporating machine learning tools, or "artificial intelligence" (Organisation for Economic Co-operation and Development [OECD] 2017). They are no longer a set of fixed commands rigidly linking a fact to a consequence. On the contrary, algorithms peruse through the available data in order to learn from previous experience and dynamically link facts to consequences. Algorithms improve themselves with each interaction, and they are growing to become predictive (Agrawal, Gans & Goldfarb, 2018).

Digitalisation, algorithms and automation can significantly improve the efficiency of the infrastructure manager, reducing the investment necessary for the construction and maintenance of infrastructure, and improving efficiency in the provision of infrastructure-based services. However, technology can also disrupt existing business models and erode the position of the infrastructure managers and the funding available for the construction and maintenance of infrastructure. Technology can reduce the cost of infrastructure.

2.9.1. Technology is transforming maintenance

The Internet of Things (IoT) allows the installing of sensors in all the elements of any infrastructure. In this way, the infrastructure manager can monitor the status of such elements, and maintenance can be tailored to the real condition of the infrastructure, making possible "conditions-based maintenance" for infrastructure (Jardine, Lin & Banjevic, 2006:1483–1510). Even more, intelligent algorithms can make use of existing data to predict the need of maintenance, enabling the so-called "predictive maintenance" (Daneshkhah, Stocks & Jeffrey, 2017:33–45).

2.9.2. Reduced maintenance costs

Maintenance costs can be reduced, as interventions take place when they are really necessary, and not based on a conservative theoretical analysis or even worse, when costly and unfortunate faults take place. As an example, for railways rolling stock, it has been estimated that “condition-based maintenance” can reduce costs from 10 to 15%, while predictive maintenance can reduce cost a further 10% (McKinsey & Company, 2016).

2.9.3. Reduced costs for the infrastructure manager

Implementing new technical solutions is a costly exercise on its own, but an investment that has demonstrated to pay off in many different contexts. Technology can reduce the cost of design, construction, maintenance and charging for traffic (Kearney, 2017). As an example, it has been estimated that as an average, a 30% reduction in capital expenditure (CAPEX) can be expected from the implementation of the leading technologies in the road industry (Cruz & Sarmento, 2018).

2.9.4. Technology can transform the use of infrastructure

Infrastructure managers have new tools to manage demand and increase efficiency. Adapting capacity to demand is the key strategy in infrastructure management. Infrastructure presents obvious network effects: the larger the number of users, the larger the pool to distribute the high fixed sunk costs of operating the infrastructure. It is not by chance that infrastructures are considered network industries. However, as network industries, they may also face negative network externalities, for instance in the form of congestion (Costa, Montero & Roson, 2018).

Business users are increasingly demanding telecommunications services that adapt to the capacity they need at any given time. If they need more bandwidth because their servers are getting more traffic, the telecommunications infrastructure manager can increase in real time the available bandwidth (and the price charged for it). When demand returns to normal, bandwidth and price will be reduced. The “bandwidth on demand” services are already a reality (Kreutz, Ramos, Verissimo, Rothenberg, Azodolmolky & Uhlig, 2015).

A similar effect is emerging in the electricity industry. Alternative distributed networks, for example consumers installing their own power generating technologies, are challenging traditional centralised networks, often with exclusive rights in their territory. New players have entered the market, including equipment manufacturers, digital companies, telecoms, and start-ups (McKinsey & Company 2018), but it is difficult to quantify the impact at this stage.

Overall, technology is introducing more uncertainty in the management of infrastructures. Costa et al., (2018:15), opine that while technology is providing new instruments to predict and manage traffic flows, it is also empowering users to make more effective use of the existing infrastructures.

2.10. DISRUPTION BY NEW PLAYERS IN THE DATA LAYER: ONLINE PLATFORMS

Online platforms are transforming the traditional industrial organisation paradigm of large vertically integrated corporations that sells goods and services to consumers, into a new model in which online platforms create a multisided market facilitating the interactions between goods and service providers and users (Rochet & Tirole 2003:990–1029; Evans & Schmalensee 2016; OECD 2009).

Online platforms are the leaders in the new data layer. Once an industry is digitalised and a data layer is created on top of it, transaction costs can be drastically reduced. The internet reduces communications costs to nil. Algorithms reduce search costs, information costs and bargaining costs.

Platforms can introduce mechanisms to increase trust and reputation (OECD 2017). Moreover, online platforms are disrupting an increasing the number of industries. Search platforms, such as Google, and social network platforms, such as Facebook which has disrupted media and content industries, have facilitated new and innovative interactions between content providers, advertisers and audiences. These platforms have generated indirect network effects at a previously unknown scale, displacing traditional players in the media industry. Platforms such as Amazon and eBay are creating new marketplaces, again connecting sellers and buyers at a previously unknown scale and creating massive indirect network effects. Subsequently, traditional retailers are being displaced (Costa et al., 2018:17).

2.11. CONDITIONS NECESSARY FOR BUSINESS CONTINUITY MANAGEMENT PROGRAMME IMPLEMENTATION

2.11.1. Legislation/Legal requirement

Momani (2010:272–279) highlighted that it is important to consider legal requirements to which the organisation subscribes, such as safety code of practices, because by considering such requirements the organisation will both follow existing requirements and improve its business continuity capability.

2.11.2. Awareness campaign

Implementing a BCM programmes involves managing a number of related projects such as awareness raising that involves events which maintain the enthusiasm for undertaking a BCM programme (Business Continuity Institute, 2010). Moreover, an awareness programme must be started after the appointment of a BCM manager and the manager and staff should be aware of the significance of BCM to the organisation and of the commitment to it. BCM must be sold positively and everyone should be convinced that it is essential (Gallagher, 2005:66–68).

2.11.3. Industry focused

BCM must be tailored to the company's specific objectives, business, managers, and the industry in which the company operates and the strategies it has adopted (Asian Disaster Reduction Centre, 2012).

2.11.4. Financial support

Availability of financial support to fund business continuity management initiatives is ensured by the chief financial officer. All the role players are assigned to specific groups and committees created within the organisation. The manager in charge of BCM is responsible for assembling a team to execute the decisions made by the business continuity management steering committee (Verman, 2011:11–36). The BCM manager presents vital decisions to business owners and should lead them during the recovery processes if a disruption has occurred. From the aforementioned, it is clear that the organisation's executives should drive business continuity management. It is important to incorporate at all levels of the organisation so that employees can become involved in the BCM processes.

2.12. BUSINESS CONTINUITY ORGANISATIONS

BCM should be business-owned and business-driven. A dedicated BCM team is required to facilitate the continuation of business operations efficiently in the event of business disruption (Tammineedi, 2010:36–50). Additionally, the team should consist of people who understand the organisation, its business, technology, processes, and business risks, in which the team will collectively provide the expertise within the organisation. Roles, responsibilities and authorities should be defined, documented and communicated in order to facilitate effective business continuity planning (Momani, 2010:272–279). The authors further accentuated the importance of having objectives and targets that could be achieved given the resources and preparations, for instance, if a company provides internet services by depending on cables without having a microwave data transferring system, it cannot claim zero downtime for their internet services due to cable failure.

2.13. ORGANISATIONAL STRUCTURE AND BUSINESS CONTINUITY MANAGEMENT

The findings of Johnson et al. (2007:112–133) were that structure dictates how policies and objectives are established and how resources are allocated. There is no one optimal organisational design or structure for a given strategy. They argued that when an organisation changes its strategy, the existing organisational structure may become ineffective. They further highlighted that symptoms of an ineffective organisational structure include too many people, too much attention being directed towards solving conflicts, too large a span of control and too many unachieved objectives. Changes in structure should not be expected to make a bad strategy good or to make a bad manager good.

2.14. ICT READINESS FOR BUSINESS CONTINUITY (IRBC)

Information technology (IT) and information system (IS) incidents affect business operations and, as many examples show, may also have severe business impacts. Organisations recognise IS continuity as a key information management issue (Luftman & Zadeh, 2011:193–204). Crises such as oil spills interrupt business operations, affect reputations and reduce the firm’s market value (Coombs, 2007:163–176; Smith, Smith & Wang, 2010:201–221). Similarly, when an IS incident occurs and continuity is disrupted, the operational work in part of the organisation stalls and the impact on the business is negative. If the incident affects customer service, for instance, it may also cause reputational damage. It has been found that service disruptions have significant negative effects on customer loyalty: one Nordic bank lost 30,000 customers because of a long-drawn-out incident during an IS merger (Luoma-aho & Paloviita 2010:49–67; Wang, Wu, Lin & Wang 2010: 350–359).

The reliable delivery of data and information is indicative of the information management capability of an organisation (Mithas et al., 2011:137–A15). Availability incidents were common in the early days of business computing, and disaster recovery planning (DRP) was developed to address that (Herbane, 2010:978–1002). According to Ernst & Young's Global Information Security Survey (Ernst & Young 2011), organisations perceived business continuity management, or DRP, as the most probable information security investment area. The International Organisation for Standardization and other bodies have developed several risk-management, business-continuity and information-security standards, but they have been criticised as too general for companies with specific business needs (Siponen & Willison, 2009:267–270).

2.15. EXTERNAL REQUIREMENTS

External requirements have a positive effect on the embeddedness of continuity practices. According to Herbane, Elliott and Swartz (2004), recovery speed after an incident depends on how quickly the organisation identifies the incident and how well it is prepared. The authors further asserted that organisational alertness and preparedness are easily improved if managers allocate resources and decide to implement back-up plans and form crisis teams. It is also essential that top management takes responsibility for and requires regular reports on continuity issues (Ivancevich, Hermanson & Smith, 1998; Seow, 2009; Wong, Monaco & Sellaro, 1994). However, if top management assigns responsibility to the IT department, chief information officers may not sufficiently emphasise organisational alertness or preparedness.

2.16. MANAGEMENT SUPPORT

Management support has a positive effect on organisational alertness and preparedness. Another technique is to embed IS continuity in organisational practices, and to make sure that employees and management in other departments understand its importance (Alesi 2008; Morwood 1998). Instead of giving the sales director responsibility for every information system in the IT department, it might be more beneficial to make them responsible for the customer relationship management system and its continuity. In this way, awareness of and responsibility for IS continuity would therefore extend beyond the IT department (Herbane et al., 2004:435–457). If top management supports the embedding of IS continuity practices throughout a company, heightened awareness and commitment would become part of the organisational culture for everyone (Alesi, 2008:214–220).

2.17. ORGANISATIONAL ALERTNESS AND PREPAREDNESS

Organisational alertness and preparedness have a positive effect on the embeddedness of continuity practices. As Herbane et al. (2004:435–457) suggested, organisational alertness and preparedness have business impacts (see Figure 1). Herbane et al. (2004:435–457) contended that when an organisation is prepared and practices are included in processes – and employees, business units as well as managers are fully committed – continuity practices are said to be embedded.

BCM aims to identify potential risks and avoid, minimise or prepare for them so as to continue business processes and services without interruption (Gibb & Buchanan, 2006). It is a socio-technical approach, in which the emphasis is on preparation for possible continuity problems. Therefore, it has strategic implications for preserving the value of the organisation (Herbane et al., 2004:435–457). Service disruptions have been discovered to have significantly negative effects on customer loyalty (Wang et al., 2010).

2.18. THE CORPORATE RISK MANAGEMENT FRAMEWORKS

Agencies should have some form of risk management structure in order to meet their risk management obligations. As ICT disaster recovery is primarily a risk management activity, it should be linked to organisational risk management arrangements and governance. An agency’s risk management arrangements are a natural starting point for assigning roles and responsibilities relating to the management of ICT disaster recovery risks. This will also assist in creating a proper link to an agency’s business continuity planning arrangements (Government of Western Australia, 2017).

Moreover, proper governance can provide accountable authorities, business service owners and ICT practitioners with confidence that an appropriate ICT disaster recovery capability exists, and that this capability is aligned with the requirements of core business service delivery. It can also assist agencies in identifying and minimising the likelihood of disruptions impacting business functions, and ensure integrated responses from both the business and ICT areas in the event of disruptions occurring.

2.19. ISO 22301 – THE INTERNATIONAL BUSINESS CONTINUITY STANDARD

The international standard, ISO 22301:2012, provides a best-practice framework for implementing an optimised BCMS (business continuity management system), enabling the organisation to minimise business disruption and continue operating in the event of an incident. An ISO 22301-aligned BCMS also includes disaster recovery and business continuity plans to help the organisation recover critical operations as quickly as possible.

The most significant contribution by the private sector for disaster risk reduction is denoted by the business continuity plan/planning (BCP) or business continuity management system (BCMS) of each enterprise that can reduce damages and help quick restoration from business interruption. The BCP or BCMS is standardised as ISO22301 (ISO 2012) and disseminated in many business enterprises around the world.

2.20. ELEMENTS OF A BUSINESS CONTINUITY MANAGEMENT PROGRAMME

A well-thought-out BCM programme allows an organisation to continue functioning during a disaster and, ultimately, to fully recover normal business operations in a timely manner afterward. Through the process of business continuity planning, an organisation identifies its main risks, processes and IT systems, and it then creates plans for remediation should a disaster occur. (Crowe, 2019). Though they may intersect with emergency management plans, which are concerned with keeping patients and staff safe from harm during a disaster, BCPs are focused on continuing operations when main systems are down. The central elements of a BCM programme are discussed next.

2.20.1. Business impact analysis

A business impact analysis (BIA) is a process to predict the impact on business processes and systems in the event of a disaster in order to develop strategies to recover. Conducting a BIA helps an organisation prioritise recovery of each business process and define what those processes need from the following three perspectives:

- People: What are the minimum personnel requirements needed to conduct the business process?
- Technology: What IT resources (for example, software applications or systems) are required and considered critical to execute that business process?
- Process: What non-IT tools, such as patient care instruments and paper charting, are needed to support the process?

2.20.2. Business continuity planning

Using the framework created during the BIA, organisational leadership then can move into creating a BCP. A BCP is a strategic plan that positions an organisation's high-risk business processes to be able to function should a disaster occur and major systems shut down.

2.20.3. Disaster recovery

As a result of conducting a BIA and developing a BCP, the organisation should now have a comprehensive list of applications and systems needed to continue operations and a prioritisation plan for how quickly the IT department needs to be able to recover those applications and systems. This is known as a disaster recovery plan. While business continuity plans focus primarily on operations, disaster recovery plans largely are an IT endeavour to support operations (Crowe, 2019).

2.20.4. Testing

Another crucial component of a BCM programme is testing of both business continuity and disaster recovery plans. Teams should conduct tests at least annually using either a table top simulation or a full-scale drill. Periodic testing of the plans helps expose incomplete and ineffective procedures that need to be revised or updated to strengthen and refine recovery plans (Crowe, 2019).

2.21. LIMITATIONS AND CHALLENGES TO EFFECTIVE BUSINESS CONTINUITY MANAGEMENT

A BCM programme incorporates organisational capabilities to prevent accidents from occurring and spreading its impacts, and to recover to a normal operational state, after an accident has happened. This programme requires active efforts in business continuity and disaster recovery activities to fulfil the proper resilience level of critical operations and IT infrastructure throughout the organisation (Giacchero, Giordano & Schiraldi, 2013:3544–3553).

The BCM adaptation based on the holistic management process and program involving training, exercises and reviews to ensure business continuity stays relevant and up-to-date. BCM adaptation began with the identification of possible threatening events in organisational activities which transformed into a workable framework (Bird & Higgins 2013; Bras & Ribeiro 2016). This framework provides resilient, effective response and recovery. The framework safeguards the interests of key stakeholders, reputation, brand and value-creating activities. The framework also improves an organisation’s ability to successfully and appropriately react to disruptive events. An efficient and resilient BCM programme incorporates organisational capabilities to prevent accidents from occurring and spreading its impacts, and to recover to normal operational state, after an accident has happened. This programme requires active efforts in business continuity and disaster recovery activities to fulfil the proper resilience level of critical operations and IT infrastructure throughout the organisation (Giacchero et al., 2013:3544–3553).

Table 2: Good practice guidelines between disaster recovery plan, risk management, including BC planning and management

Activities	Key method	Key parameters	Type of incident
Disaster Recovery Plan	Technical components of BCP	Addresses the recovery of core systems, data and communication technologies that support the business	Disaster recovery that is subset of business continuity
Risk Management	Risk analysis	Impact and probability	All types of events, usually segmented
BC Planning	Recovery planning of processes and business functions	Covering emergency response, business continuity, disaster recovery and also managing crises	Events causing significant business interruption
BC Management	Business impact analysis	Impact and time	Events causing significant business interruption

Source: BCI (2017, 12-17)

BCM and BCP are subsets of enterprise risk management, while DRP is a subset of business continuity (Bras & Ribeiro 2016; Krell, 2006). Table 2 shows a good practice guideline that integrates BC functional activities required for the success and effectiveness of a BCM resilience programme as discussed earlier.

2.22. SOUTH AFRICAN REVENUE SERVICES AS A PUBLIC ENTITY

SARS is the revenue collection service (tax collection agency) of the South African government. SARS mandate to collect all revenues due is to ensure optimal compliance with tax, customs and excise legislation and provide a customs and excise service that will facilitate legitimate trade as well as protect our economy and society.

SARS is a public entity under the National Treasury; SARS is a schedule 3A of The Public Finance Management Act, 1999 (PFMA). According to the SARS Act, SARS is established as an organ of state within the South African public administration, but as an institution outside the public service (SARS, 2019).

According to (SARS, 2019) SARS reports to the Minister of Finance. The organisation is required to report actual performance against the approved annual performance plans. It is very important that SARS meets its performance targets as the impact of not meeting targets affects the entire country in that the state would not be able to finance the running and maintenance of the country as the tax money is required to pay state grants, fix and maintain roads, education, health and defence, amongst other state expenses.

According to The South African Revenue Service Act, 1997 ("SARS Act"), the function of SARS is that to achieve its objective SARS must—

> *(a)* Secure the efficient and effective, and widest possible, enforcement of—
>
> > (i) the national legislation listed in Schedule 1; and
> >
> > (ii) any other legislation concerning the collection of revenue that may be assigned to SARS in terms of either legislation or an agreement between SARS and the organ of state or institution entitled to the revenue; and
>
> *(b)* advise the Minister, at the Minister's request, on—
>
> > (i) all matters concerning revenue; and
> >
> > (ii) the exercise of any power or the performance of any function assigned to the Minister or any other functionary in the national executive in terms of legislation referred to in paragraph *(a).*

Additionally, the Public Finance Management Act,1999 (Act 1 of 1999) ensures the management of public funds are managed, emphasising prudent use of state resources, improved reporting requirements and use of management information to enhance accountability.

SARS must perform its functions in the most cost-efficient and effective manner and in accordance with the values and principles mentioned in section 195 of the Constitution.

SARS performs its functions—

> *(a)* under the policy control of the Minister; and
>
> *(b)* subject to any directives and guidelines on policy matters issued by the Minister”.

SARS's mission is to optimise revenue yield, facilitate trade and enlist new tax contributors by promoting awareness of the obligation to comply with South African Tax and Customs Laws, and to provide quality and responsive service to the public.

SARS has strategic outcomes which are linked to and support its mandate, which comprises:

- increased customs and excise compliance;
- increased tax compliance;
- increased ease and fairness of doing business with SARS;
- increased cost effectiveness and internal efficiencies; and
- increased public trust and credibility.

Section 12 of the Policy Finance Management Act states that SARS must deposit into a Revenue Fund all taxes, levies, duties, fees and other moneys collected by it for that Revenue Fund. SARS may withdraw money from the National Revenue Fund to refund any tax, levy or duty credits or any other charges in connection with taxes, levies or duties; or to make other refunds as approved by the National Treasury; or to transfer money that was collected on behalf of other agencies.

2.23. STATE OF BUSINESS CONTINUITY MANAGEMENT AT SOUTH AFRICAN REVENUE SERVICES

SARS does not have BCM in place and has listed the “Business interruption” as one of their enterprise-wide risks in the SARS Annual Performance Plan (APP) document 2019/2020 and SARS Strategic Plan 2020/21 – 2024/25.

The risk has been described as “Business interruption – The lack of an approved enterprise-wide Business Continuity Management Framework leads to an inability to plan a response to unplanned business interruptions. Therefore, in the event of an incident it may result in a prolonged business interruption, operational failures, and potential business failure.” SARS (2019)

SARS proposed that it will mitigate the risk by establishing a Business Continuity Management Committee, which will oversee the development and implementation of an enterprise-wide Business Continuity Management Framework (including a Disaster

Recovery Plan) as their mitigation actions for the risk of business disruptions. SARS (2020)

Therefore, the main objective of the study which is to propose a framework to enhance ICT readiness for business continuity would assist SARS in mitigating the risk of business disruption.

2.24. CONCLUSION

This literature review has analysed the importance of business continuity management, organisational resilience through BCM, the role of CSF in BCM, and requirements for an effective implementation of BCM strategy and how it affects SARS in their journey towards enhancing their BCM. SARS does not have a comprehensive BCM and in this chapter the importance of BCM at SARS was discussed. The review further analysed the theoretical framework underpinning the study that is the resource-based view. DRP, the BCM Lifecycle and related concepts, the rise of digital disruption as well as frameworks for information systems continuity management were also examined. The next chapter presents the research methodology adopted for the study.

CHAPTER 3
RESEARCH METHODOLOGY

3.1. INTRODUCTION

In this chapter, the research methodology employed in the study is analysed and explained. The design research approach was adopted and aspects of design science research in information systems, philosophical grounding for IS research, action design research, (ontology-based design science) ODSR framework, and ODSR roadmap are discussed in relation to the study.

3.2. DESIGN SCIENCE RESEARCH DEFINED

"Design science creates and evaluates IT artefacts intended to solve identified organizational problems (Hevner, March & Park, 2004:77)". It involves a rigorous process to design artefacts to solve observed problems, to make research contributions, to evaluate the designs, and to communicate the results to appropriate audiences. Such artefacts may include constructs, models, methods, and instantiations (Hevner et al., 2004:75–105). They might also include social innovations (Van Aken 2004:219–246) or new properties of technical, social, and/or informational resources (Järvinen, 2007:37–54).

3.2.1. Overview of design science research

Two main genres of research paradigms in the information systems discipline have been recognised as behavioural science and design science. Behavioural science research aims for theoretical development and verification whereas design science research focuses on delivering innovative artefacts in the context of extending the body of knowledge (Hevner & March, 2003:111–113; Hevner, March, Park & Ram, 2004:75–105). Design science research originated from the field of engineering (Hevner et al., 2004) and was introduced to the IS research community in 1990 (Nunamaker, Chen & Purdin, 1991). The mechanism involves diagnosing observed practical problems to establish research questions, solving the problems, developing artefacts to demonstrate the comprehensive solution, and evaluating the presented result. The designed artefacts are matched into the body of knowledge to offer additional understandings on the application or relevant area.

All research is established with underlying assumptions on the philosophical grounding around the research validity and the appropriateness of research methodology (Vaishnavi & Kuechler, 2005). In order to conduct and evaluate research, it is important to acknowledge the existence of these philosophical assumptions, especially those related to reality, knowledge and value constructivism.

3.3. THE ONTOLOGY-BASED DESIGN SCIENCE ROADMAP

The ODSR roadmap consists of eight key steps and four activities connecting the research tasks with the use of ontologies that were employed as follows:

Step 1: The first step was to observe and analyse the problem at SARS. This step is described as observation activities in Nunamaker et al.'s (1991) multi-methodological design research framework (Nunamaker et al., 1991), the identification of business needs to prevent disruption of IT and other business activities, and the applicable theory/framework and methods in Hevner et al.'s (2004) DSR framework. In this step, the researcher assessed the existing ontologies of relevant technologies and/or theories for identifying the business needs or gaps in the literature (De Almeida Biolchini, Mian, Natali, Conte & Travassos, 2007).

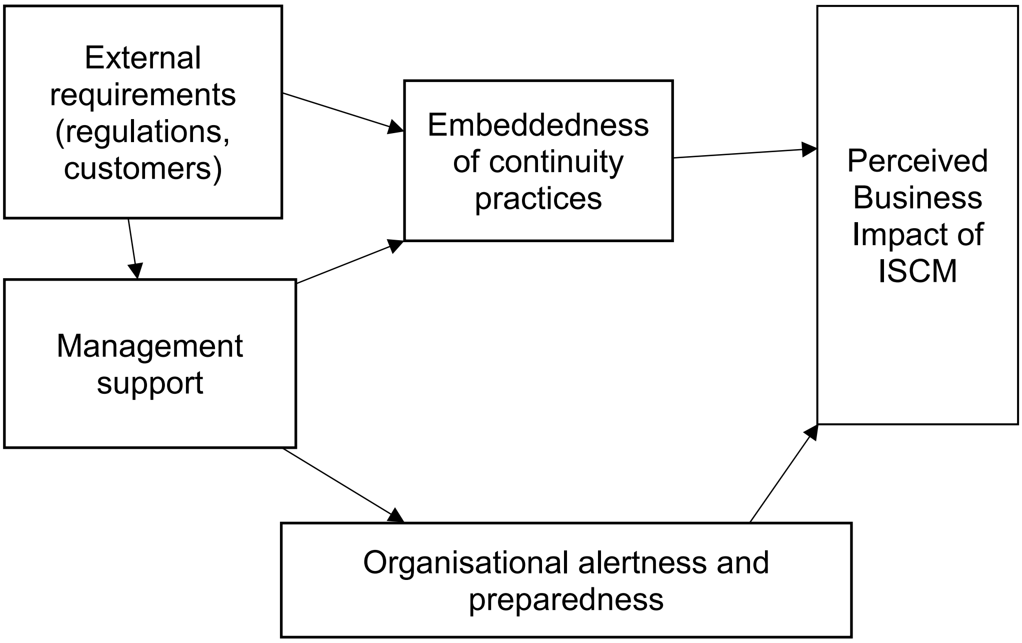
Step 2: The second step was to formally define the research scope and objectives. For this study, the research objective was to ensure that business and systems disruptions are addressed in a way that minimises business activity failure. The primary research objective was to develop a framework that SARS can use to ensure that their IRBC is effective and reduces the impact of information incidents on the organisation. The following were the secondary objectives of the study:

- To investigate the board members' responsibilities in IRBC and BCM, and their awareness of these responsibilities.
- To investigate possible techniques or actions for ensuring ICT readiness and business continuity in public entities.
- To investigate typical frameworks and policy documents which will assist public entities with ICT readiness for business continuity
- To develop and recommend a suitable framework that will assist public entities in implementing an effective IRBC.

While defining the research scope and objectives for the design project, the ontological scope and existing ontologies were also selected for supporting the research and evaluation process. The selected ontologies needed to include not only those related to the to-be-built artefacts, but also the semantic representation of publications in the domain of interest.

Step 3: The existing ontologies aid the identification of design requirements. The requirements may be adopted from previous studies and practices or constructed for a new context that has not been reported in the literature. In this study the requirements were adopted from the International Standard ISO/IEC 27031 of which the framework is illustrated in Figure 2 below.

Figure 2: A framework for information systems continuity management


External requirements (regulations, customers)
Embeddedness of continuity practices
Perceived Business Impact of ISCM
Management support
Organisational alertness and preparedness

Source: Järveläinen (2013)

Step 4: Design is “a search process to discover an effective solution to a problem” Hevner et al. (2004). It is important to recognise and evaluate the existing solutions before developing a new one. The study appraised the relevance and effectiveness of the model in Figure 4 and developed a questionnaire developed to test the effectiveness of the CBM within the parameters indicated.

Step 5: In this step, the artefact was designed to address the identified problem/opportunity within the framework for CBM. As the development of an artefact is a time-consuming process (Nelson & Stolterman, 2012; Peffers et al., 2007), the feasibility of the design had to be evaluated before conducting the development.

Step 6: In this step, the researcher started constructing the artefact based on the proposed design. The design requirements, alternative solutions, relevant technologies and theories identified from previous steps were reflected through the development of the new artefact (Gazem, Rahman, Saeed & Iahad, 2018; Alturki, Gable & Bandara, 2013).

Step 7: Evaluation is essential in DSR to demonstrate both the relevance to the environment and research significance to the field. In fact, this step helps to distinguish DSR artefacts from practice-based IT applications. There are various evaluation approaches such as experiments, simulations, case studies or field studies (Hevner et al., 2004).

Step 8: Lastly, the researcher will communicate findings of the research communities. In particular, this step involves writing, publishing, and/or presenting research outputs to appropriate academic conferences and journals. Furthermore, the ODSR researcher will refine, update and/or create the relevant ontologies which act as a shared conceptualisation of the constructs and the relations among them within the research field.

3.4. THE POPULATION AND SAMPLE

The survey was conducted as a cross-sectional study at SARS, participants are classified in Table 3.

Table 3: Population and sample

Department	**Population**	**Sample**
ICT Department	15	15
Top management	9	9
Middle management/supervisors	26	26
Operatives	50	50
Total	100	100

Source: Researcher’s elaboration

The survey was a complete cross-sectional survey. Given the small size of the target population, the study was conducted as a cross-section of the target population and a total of 100 participants were invited to participate in the survey. Hence the study was a complete once-off survey and the participants were reachable via email and located in one place (the organisation).

Data was collected using an email inquiry which was decided on after taking into account accuracy, practicability and cost factors from among the alternative methods.

Web-based enquiry

This study employed a web-based survey. In web-based enquiry, data are collected by obtaining questionnaires filled in by the respondents, with the questionnaires being posted on the net. One important advantage of using computer technology in data collection is that it helps to minimise the loss of data (owing to incomplete or incorrectly completed data sets) by using client-side validation. In an era of information superhighway, this method is one of the fastest means of data collection.

3.5. DESIGN: DEVELOPMENT OF THE METHODOLOGY

3.5.1. Activity 1. Problem identification and motivation

Define the specific research problem and justify the value of a solution. Since the problem definition of this study was used to develop an artefact that can effectively provide a solution, it was considered useful to split the problem conceptually so that the solution could capture its complexity. Justifying the value of a solution accomplishes two things: it motivates the researcher and the audience of the research to pursue the solution and to accept the results and it helps to understand the reasoning associated with the researcher’s understanding of the problem. Resources required for this activity include knowledge of the state of the problem and the importance of its solution (Peffers et al., 2007).

3.5.2. Activity 2. Define the objectives for a solution

Infer the objectives of a solution from the problem definition and knowledge of what is possible and feasible. The objectives can be quantitative, such as terms in which a desirable solution would be better than current ones, or qualitative, for example a description of how a new artefact is expected to support solutions to problems not hitherto addressed. The objectives should be inferred rationally from the problem specification. Resources required for this include knowledge of the state of problems and current solutions, if any, and their efficacy (Peffers et al., 2007 and De Leoz and Petter 2018).

In some of the research by Eekels & Roozenburg, (1991); Nunamaker et al., (1991:89–106), the design and development activities are further subdivided into more discrete activities whereas other researchers focus more on the nature of the iterative search process (Hevner et al., 2004:75–105).

3.5.3. Activity 3. Design and development

This involves creating the artefact. Artefacts are broadly defined potential constructs, models, methods, or instantiations (Hevner et al., 2004:75–105). According to Järvinen, (2007:37–54) artefacts are new properties of technical, social, and/or informational resources and can be any designed object in which a research contribution is embedded in the design. Research and development involves determining the artefact's desired functionality and its architecture and then creating the actual artefact. It also covers resources allocation related to moving from objectives to design and development including knowledge of theory that can be brought to bear in a solution.

According to Eekels & Roozenburg, (1991), Vaishnavi & Kuechler, (2005), and Rossi & Sein, (2003) the next stage involves demonstrations to prove that the idea works, and to attain a more formal evaluation.

3.5.4. Activity 4. Demonstration

Demonstrate the use of the artefact to solve one or more instances of the problem. This could involve its use in experimentation, simulation, case study, proof, or other appropriate activity. Resources required for the demonstration include effective knowledge of how to use the artefact to solve the problem (De Leoz, Petter, 2018).

3.5.5. Activity 5. Evaluation

Observe and measure how well the artefact supports a solution to the problem. According to Peffers, & Tuunanen, Rothenberger, Chatterjee, & Samir. (2008), this activity involves comparing the objectives of a solution to actual observed results from use of the artefact in the demonstration. It requires knowledge of relevant metrics and analysis techniques. Depending on the nature of the problem, venue and the artefact, evaluation could take many forms. It could include such items as a comparison of the artefact's functionality with the solution objectives from activity two above, objective quantitative performance measures, such as budgets or items produced, the results of satisfaction surveys, client feedback, or simulations. It could include quantifiable measures of system performance, such as response time or availability.

Conceptually, such evaluation could include any appropriate empirical evidence or logical proof. At the end of this activity the researcher can decide whether to iterate back to step three to try to improve the effectiveness of the artefact or to continue on to communication and leave further improvement to subsequent projects (Peffers, et al. 2008).

3.5.6. Activity 6. Communication

Communicate the problem and its importance, the artefact, its utility and novelty, the rigour of its design, and its effectiveness to researchers and other relevant audiences, such as practising professionals, when appropriate (Peffers, et al. 2008). In scholarly research publications, researchers might use the structure of this process to structure the paper, just as the nominal structure of an empirical research process (problem definition, literature review, hypothesis development, data collection, analysis, results, discussion, and conclusion) is a common structure for empirical research papers. Communication requires knowledge of the disciplinary culture.

3.6. CONCLUSION

This chapter has presented the research methodology adopted in this study, ontology-based design science (ODSR) framework for IS research, and ODSR roadmap and the activities to develop a methodology that were employed in the study were discussed. The population and sampling techniques utilised in the study were also provided and the researcher stated that a complete cross-sectional survey was undertaken for the study. Furthermore, a framework for information systems continuity management.

The model was modified in light of the findings from the study so that it may be presented and communicated as the solution to the problem of minimising business disruptions at SARS.

CHAPTER 4
DATA ANALYSIS AND PRESENTATION

4.1. INTRODUCTION

Towards the design of a framework to enhance ICT readiness for business continuity at the South African Revenue Services, this chapter presents the data on the findings gathered from the study. Data gathered through the questionnaire instrument are presented and analysed in 5 sections. Section 1 is the demographic information of the participants; Section 2 has the benefits of BCM; Section 3 includes the critical incidents covered in the BCM plan; Section 4 comprises the key characteristics of BCM framework; and Section 5 the development plan.

4.2. SECTION 1: DEMOGRAPHICS OF THE STUDY

The demographic information that the researcher gathered from the respondents included their gender, level of employment within SARS, period within employment as well as educational qualifications. Demographic data enables the researcher to determine the calibre of the participants in the study, hence the validity and reliability of the information gathered. The demographic profile of research participants also enables the researcher to justify objectivity and balance in the sample selection to enable users of the research information to be assured of its reliability and representation of the population.

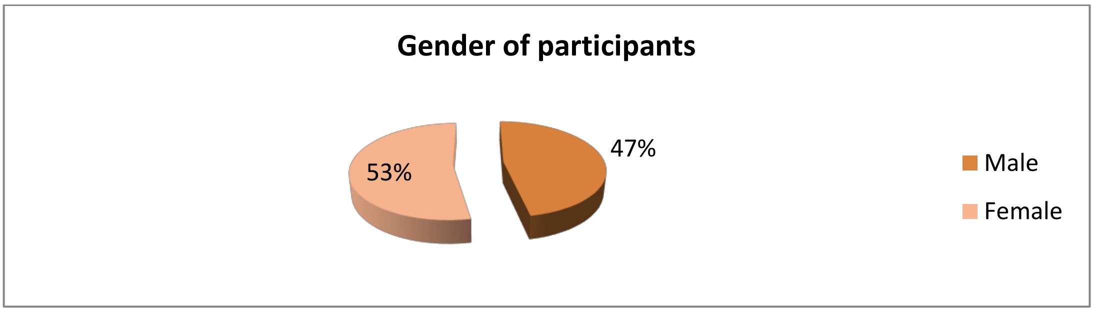
The whole population of 100 participants comprised of 15 from the ICT Department, nine senior level managers, 26 middle management, and 50 operatives. A 49% response rate was achieved from the population. The 49 respondents did not respond to all questions on the survey. The number of respondents for each set of questions has been provided in tables below. This study was qualitative in nature and scholars highlight the lack of concrete guidelines on the sample size or response rate for qualitative research as a barrier for justifying sample size or response rate for most researchers (Domegan and Fleming, 2007). However, they highlight the consideration of practical reasons for justifying the adequacy of a sample or response rate. To justify the response rate of 49% as adequate, the researcher considered the homogenous nature of the participants which provided a platform for validation of responses. Morse

(2000) opined that stakeholder demographics and diversity is the strongest defence for sample and response rate adequacy.

4.2.1. Gender of participants

Out of the 49 participants, 26 (53%) were female and 23 (47%) male. These statistics reflect a gender balance in the sample selection which is critical for the avoidance of bias and adds to the appearance of credibility of the participants.

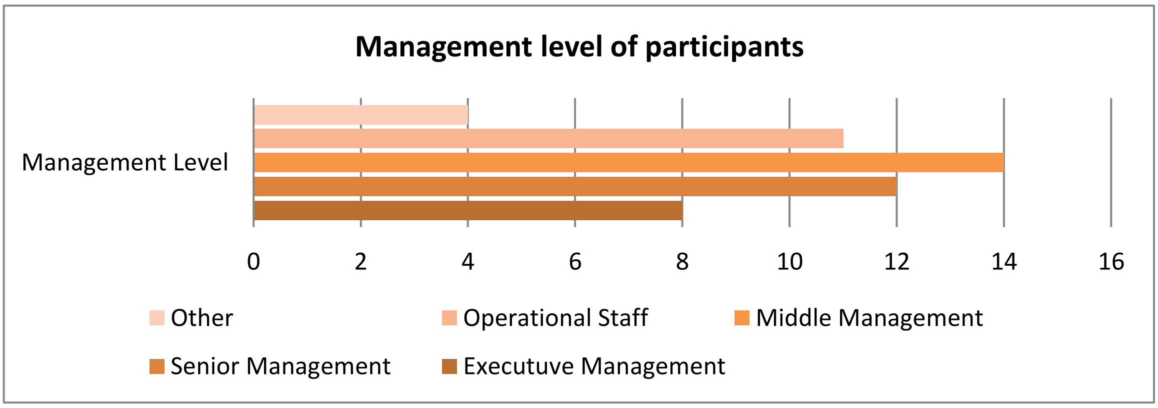
Figure 3: Gender



4.2.2. Level of employment with South African Revenue Services

The sample included, among others, participants from the ICT department as well executive management. As indicated in Figure 4 below, eight (16.3%) participants were at executive management level; 2 (4.1%) were senior management; 14 (28.6%) were middle level management; 11 (22.4%) were operational staff; and four (8.2%) were other. This reflects the validity and relevance of the participants for the purpose of the study.

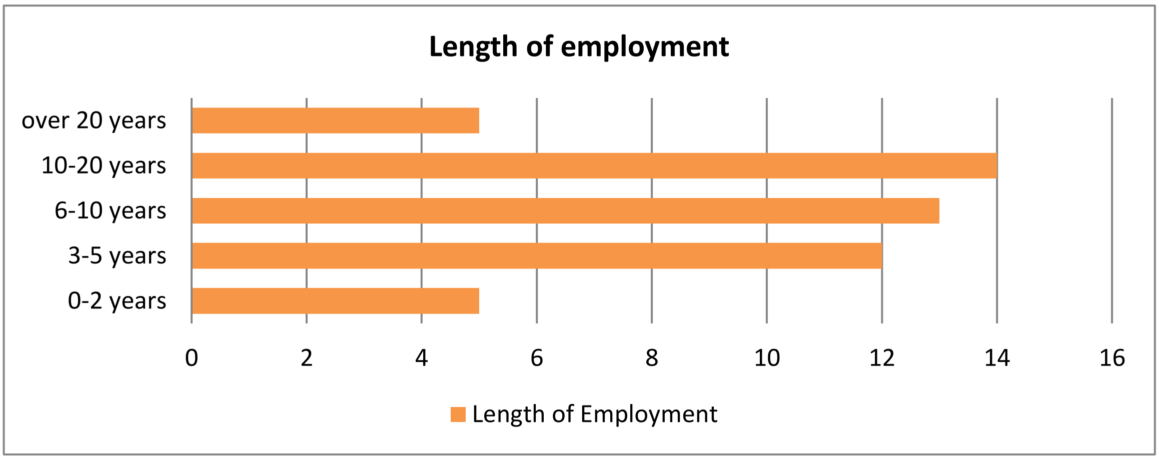
Figure 4: Level of employment



4.2.3. Length of employment

Most of the participants (19) had been in employment for over 10 years; 14 (28%) for 10 to 20 years; and five (10.2%) over 20 years. Of the 49 participants, those who had been in employment for 0-2 years only made up 10.2% (5) of the sample, 2 (24.5%) had been employed for 3 to 5 years and 13 (26.5%) had been employed for 6 to 10 years. Since most participants had been employed for 3 years, they were well versed with the study area and the policies in place in the organisation. However, of concern is the reflection of the highest representation being of the older generation (10–20 years).

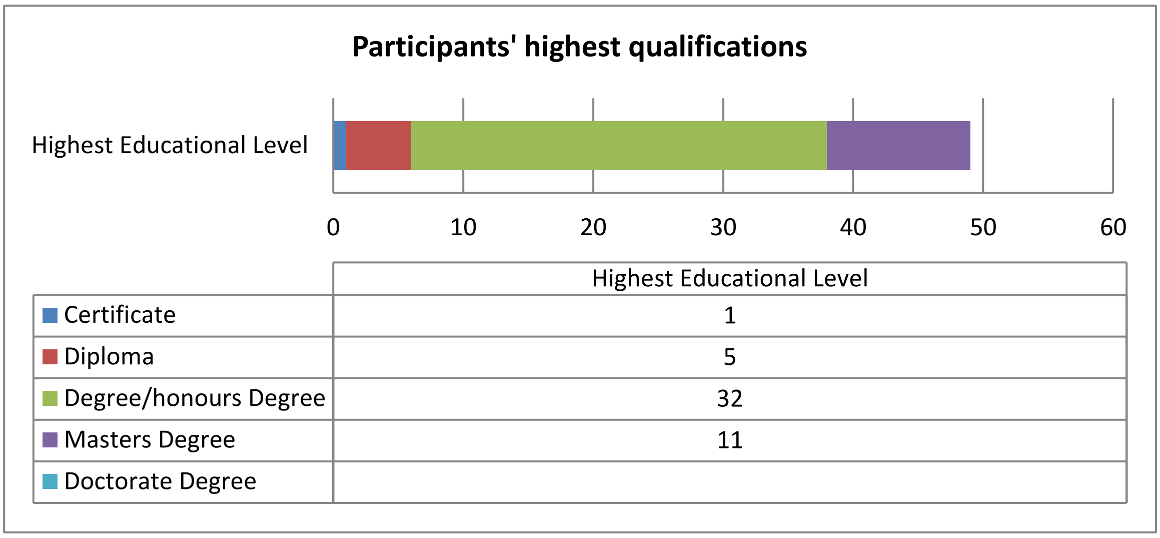
Figure 5: Length of employment



4.2.4. Highest educational qualifications

Most prominent within the sample were participants holding a degree or honours degree as a highest qualification – 32 (65.3%), while 11 (22.4%) were at master's degree level and none held a doctorate degree. One participant was at certificate level and five at diploma level. The prevalent qualification was the degree/honours degree level followed by the master's degree level, which is a good reflection of the sample on strategic decision making, knowledge and policy management.

Figure 6: Participants' qualifications



	Highest Educational Level
🟦 Certificate	1
🟥 Diploma	5
🟩 Degree/honours Degree	32
🟪 Masters Degree	11
🟦 Doctorate Degree	

4.3. SECTION 2: THE BENEFITS OF BUSINESS CONTINUITY MANAGEMENT

Downes (2018) highlighted that business continuity had been identified as a critical issue, developed as a result of the need for a best practice framework to guide business and the need for a mechanism to demonstrate business continuity management maturity. He opined that integrating a business continuity management system into the organisation demonstrates to business partners and customers that the organisation is dedicated to providing the best possible service at all times, regardless of interruption.

4.3.1. The Board's / EXCO's understanding of Business Continuity Management

The researcher sought to establish the Board/ top management understanding of BCM and hence their awareness of its benefits. The factors listed below were analysed and the results gathered summarised in Table 5 are demonstrated in Figure 7.

A. BCM offers the ability to identify risks to operations and put in place a capability to mitigate and manage those risks.

B. BCM provides the ability to manage uninsurable risk, such as risk to reputation.

C. BCM avails an effective response to major disruptions.

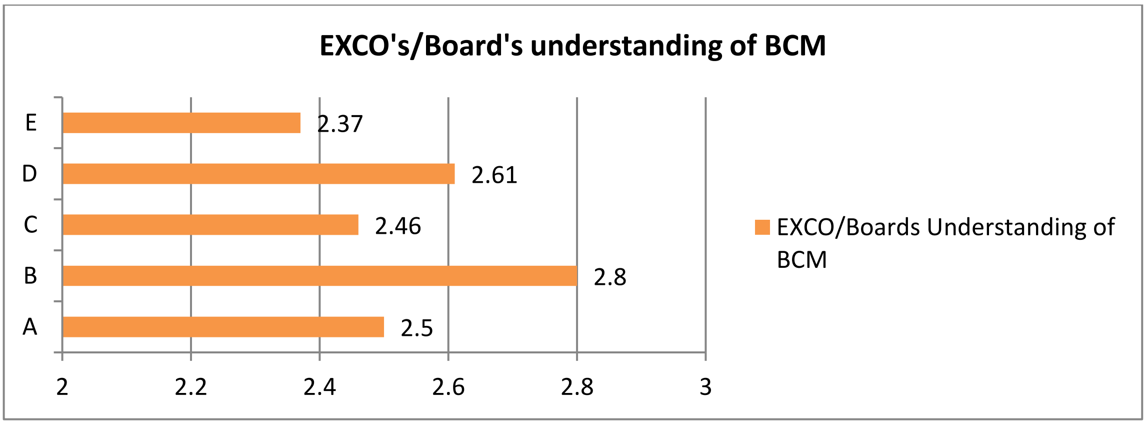
D. BCM is important because it provides the ability to demonstrate that the process is credible and consistent via exercising and auditing.

E. There are competitive advantages conferred in BCM by the ability to maintain customer service, staff employment and stakeholder confidence.

Table 4: Board's input: Benefits of Business Continuity Management

Number of Respondents 46	Strongly Disagree (1)	Disagree (2)	Not Sure (3)	Agree (4)	Strongly Agree (5)	Not Applicable (0)	Arithmetic Average (∅)	Standard Deviation (±)
A	15x32.61	10x21.74	9x19.57	7x15.22	5x10.87	-	2.50	1.38
B	14x30.43	8x17.39	6x13.04	9x19.57	9x19.57	-	2.80	1.54
C	13x28.26	13x26.26	9x19.57	8x17.39	3x6.52	-	2.46	1.26
D	11x23.91	14x30.43	5x10.87	14x30.43	2x4.35	-	2.61	1.27
E	12x26.09	16x34.78	9x19.57	7x15.22	2x4.35	-	2.37	1.16

Figure 7: Board's level of understanding Business Continuity Management



The main benefit of BCM was understood as (B) – to provide the ability to manage uninsurable risk, such as risk to reputation. And the second was (D) – BCM is important because it provides the ability to demonstrate that the process is credible and consistent via exercising and auditing. (A) – BCM offers the ability to identify risks to operations and put in place a capability to mitigate and manage those risks, ranked third. Of concern is that the finding for (C) which actually is the main objective of BCM

'BCM avails an effective response to major disruptions' was ranked second last according to the participants' understanding of the purpose of BCM.

4.4. SECTION 3: CRITICAL INCIDENTS ARE COVERED IN THE BUSINESS CONTINUITY MANAGEMENT PLAN

The study established that the international standard ISO 22301:2012 provides a best practice framework for implementing an optimised BCMS (business continuity management system), enabling the organisation to minimise business disruption and continue operating in the event of an incident. An ISO 22301-aligned BCMS also includes reduction of damage, disaster recovery and business continuity plans to help the organisation recover critical operations as quickly as possible. The key outcome for this requirement is that agencies will ensure that there is a process for identifying incidents which may, or already have, become a disruption, warranting the triggering of the ICT disaster recovery response (Government of Western Australia, 2017).

4.4.1.1. Participants' awareness of the critical incidents plan in the Business Continuity Management framework

A. Loss, damage or denial of access to key IT services.

B. Failure or non-performance of critical service providers, distributors, or commercial third parties like trading partners.

C. Loss or corruption of information.

D. Sabotage or commercial espionage.

E. Deliberate infiltration or attack on IT Systems.

F. The key requirements of managing effective business continuity can be achieved by suppliers in the "cloud".

Table 5: Participants' input: Critical incidents plan in the Business Continuity Management framework

Number of Respondents 46	Strongly Disagree (1)	Disagree (2)	Not Sure (3)	Agree (4)	Strongly Agree (5)	Not Applicable (0)	Arithmetic Average (∅)	Standard Deviation (±)
A	6x13.04	13x28.26	7x15.22	14x30.43	6x13.04	-	3.02	1.29
B	8x17.39	16.34.78	11x23.91	8x17.39	3x6.52	-	2.61	1.16
C	8x17.39	13x28.26	8x17.39	15x32.61	2x4.35	-	2.78	1.21
D	7x15.22	18x39.13	10x21.74	10x21.74	1x2.17	-	2.57	1.07
E	5x10.82	9x19.57	11x23.91	17x36.96	4x8.70	-	3.13	1.17
F	6x13.04	18x39.13	11x23.91	7x15.22	2x4.35	2x4.33	2.57	1.07

The table above demonstrates the identification by some participants of the irrelevance of (F). The key requirements of managing effective business continuity can be achieved by suppliers in the "cloud" as a critical incident for BCM. (D), Deliberate infiltration or attack on IT systems; followed by (A), Loss, damage or denial of access to key IT services; then (C), Loss or corruption of information; and B and D with arithmetic averages of 2.61 and 2.57 respectively.

4.5. SECTION 4: KEY CHARACTERISTICS OF THE FRAMEWORK

The study established that a well-thought-out BCM programme allows an organisation to continue functioning during a disaster and, ultimately, to fully recover normal business operations in a timely manner afterward. Through the process of business continuity planning, an organisation identifies its main risks, processes and IT systems, and it then creates plans for remediation should a disaster occur (Crowe, 2019). Though they may intersect with emergency management plans, which are concerned with keeping patients and staff safe from harm during a disaster, business continuity plans are focused on continuing operations when main systems are down. The study sought to establish the participants' understanding of the key characteristics of BCM among the following characteristics for which the resultant rankings are embedded in Table 6 and further demonstrated in Figure 11.

The key characteristics of BCM are:

A. A planning process driven by risk and threat assessment is an important component of BCM (1).

B. BCM at my organisation takes on a focus on consequences not causes (6).

C. BCM at my organisation adopts a focus on critical capabilities and information (3).

D. There is teamwork and mutual support within the members involved in BCM (4).

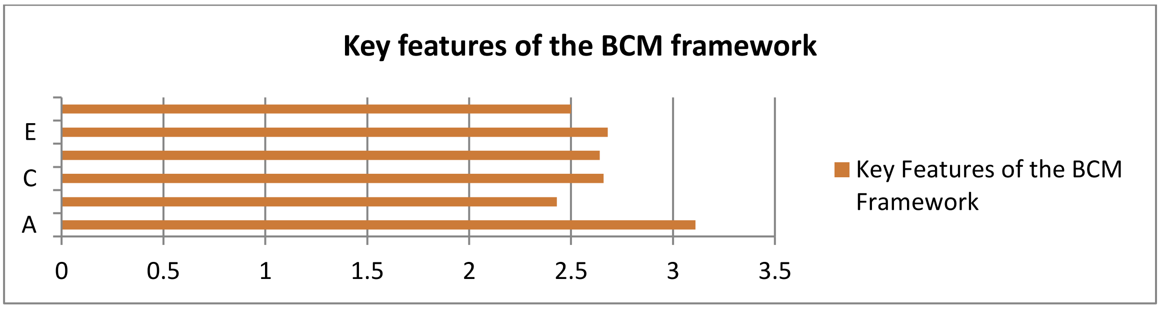
E. Training, regular exercises and rehearsals are provided under BCM (2).

F. BCM in my organisation has in place flexible and coordinated response measures (5).

Table 6: Participants' input: Key characteristics of Business Continuity Management

Number of Respondents 44	Strongly Disagree (1)	Disagree (2)	Not Sure (3)	Agree (4)	Strongly Agree (5)	Not Applicable (0)	Arithmetic Average (∅)	Standard Deviation (±)
A	9x20.45	11x25	1x2.27	12x27.27	11x25.00	-	3.11	1.54
B	8x18.18	18x40.91	10x22.73	7x15.91	1x2.27	-	2.43	1.04
C	6x13.64	18x14.91	8x18.18	9x20.45	3x6.82	-	2.66	1.16
D	8x18.18	16x36.36	8x18.18	8x18.18	4x9.09	-	2.64	1.24
E	9x20.45	16x36.36	4x9.09	10x22.73	5x11.36	-	2.68	1.34
F	12x27.27	12x27.27	7x15.91	12x27.27	1x2.27	-	2.50	1.23

Figure 8: Participants' understanding of Business Continuity Management framework features



4.6. SECTION 5: DEVELOPING A PLAN

Business continuity has been identified as a critical issue, developed as a result of the need for a best practice framework to guide business, and the need for a mechanism to demonstrate business continuity management maturity. Any incident that impairs a business's ability to function can negatively impact the organisation long after they resume normal operations. Integrating a business continuity management system into the organisation, demonstrates to business partners and customers that the organisation is dedicated to providing the best possible service at all times, regardless of interruption (Downes, 2018).

Asked on their sentiments concerning the availability of a development plan to mitigate loss of critical assets, data from 44 participants brought the following results

A. The business impact analysis (BIA) that quantifies and qualifies the impacts of loss or disruption is in place (5).

B. There are alternative strategies that are available to mitigate loss of critical assets such as personnel, premises and ICT (1).

C. There is a plan that identifies actions that are necessary and resources that may be required to enable business to manage the consequences of disruption (2).

D. There is a clear procedure for escalation and control of an incident (4).

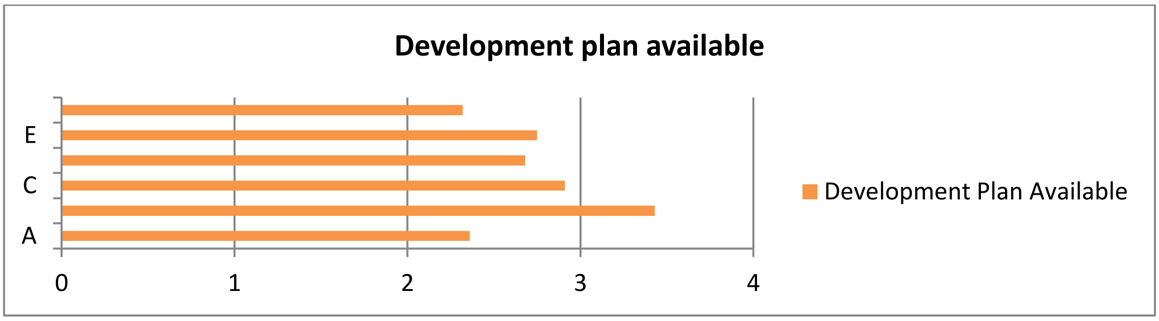
E. There are plans in place to resume after disruptions to activities, such as cross training of staff, alternative premises and off-site data, rerouting of telecoms (3).

F. A continuity culture is embedded in the business (6).

Table 7: Participants' input: A development plan

Number of Respondents 44	Strongly Disagree (1)	Disagree (2)	Not Sure (3)	Agree (4)	Strongly Agree (5)	Not Applicable (0)	Arithmetic Average (∅)	Standard Deviation (±)
A	11x25.00	17x38.64	6x13.64	9x20.45	1x2.27	-	2.36	1.14
B	2x 4.55	8x18.18	4x9.09	29x65.91	1x2.27	-	3.43	0.97
C	6x13.64	14x31.82	4x9.09	18x40.91	2x4.55	-	2.91	1.22
D	5x11.36	20x45.45	6x13.64	10x22.73	3x6.82	-	2.68	1.16
E	7x15.91	16x36.36	5x11.36	13x29.55	3x6.82	-	2.75	1.24
F	10x22.73	21x47.73	4x9.09	7x15.91	2x4.55	-	2.32	1.14

Figure 9: Participants' understanding of availability of development plan



Ranking first, (B) showed that there were alternative strategies that were available to mitigate loss of critical assets such as personnel, premises and ICT. Secondly, there was a plan that identified actions that were necessary and resources that could be required to enable business to manage the consequences of disruption (2). Thirdly, there were plans in place to resume after disruptions to activities – cross training of staff, alternative premises and off-site data, rerouting of telecoms (3). However, the findings show that the availability of There is a clear procedure for escalation and control of an incident (4), The Business Impact Analysis (BIA) that quantifies and qualifies the impacts of loss or disruption is in place (5) and A continuity culture is embedded in the business (6) were not prevalent.

CHAPTER 5
SUMMARY FINDINGS AND CONCLUSIONS

5.1. INTRODUCTION

This chapter summarises the research findings as per research objectives and highlights the conclusions reached from the study through the presentation of the proposed BCM framework, the artefact. The primary research objective was to develop a framework that SARS can use to ensure that their IRBC is effective and reduces the impact of information incidents on the organisation. The following were the secondary objectives:

- To investigate the board members’ responsibilities in IRBC and BCM, and their awareness of these responsibilities.
- To investigate possible techniques or actions for ensuring ICT readiness and business continuity in public entities.
- To investigate typical frameworks and policy documents which will assist public entities with ICT readiness for business continuity
- To develop and recommend a suitable framework that will assist public entities in implementing an effective IRBC.

The design science paradigm was used to develop a BCM for effective IRBC (ICT Readiness for Business Continuity Framework) through the stages: 1. problem identification and motivation, and 2. definition of the objectives for a solution, covered by Chapter 1; 3. design and development, Chapters 2–4; and 4. demonstration, 5. evaluation, and 6. communication, covered by Chapters 5 and 6.

Following the ontology-based design science roadmap chosen for this study, this step, the artefact, was designed to address the identified problem/opportunity within the framework for BCM. In this step, the researcher started constructing the artefact based on the proposed design. The design requirements, alternative solutions, relevant technologies and theories identified from previous steps were reflected through the development of the new artefact.

5.2. FINDINGS

5.2.1. The board members’ responsibilities in IRBC and Business Continuity Management and their awareness of these responsibilities

The research findings show that IRBC and BCM are the responsibility of Board members as they constitute a policy issue that should be placed at strategic level for strategic positioning and prioritisation. Any set framework has to be robust thus needing implementation from strategic level that is the Board. Business continuity management (BCM) is based on the principle that it is the key responsibility of an organisation’s directors to ensure the continuation of its business operations at all times. The term “business continuity plan (BCP)” refers to the identification and protection of critical business processes and resources required to maintain an acceptable level of business, protecting such resources and preparing procedures to ensure the survival of the organisation in times of business disruptions – the business continuity management programme or system. It focuses on the core advisory services for the wider programme, such as policy, people and processes, including implemented strategies, response plans, training and exercise needs, whilst ensuring they are successfully embedded and maintained within the organisation, hence its positioning at Board level (Lou et al., 2010, Nicholas, 2008; Speight, 2011).

From the study findings it is evident that the main benefits of BCM were understood as (B) provision of the ability to manage uninsurable risk, such as risk to reputation. And the second was (D), its provision of ability to demonstrate that the process is credible and consistent via exercising and auditing. (A) offering the ability to identify risks to operations and put in place a capability to mitigate and manage those risks, ranked 3rd. Of concern is that the finding for (C) which actually is the main objective of BCM ‘BCM avails an effective response to major disruptions’ was ranked second from the last according to the participants’ understanding of the purpose of BCM, thus demonstrating dedication to providing the best possible service at all times, regardless of interruption.

Regarding the participants’ awareness of the critical incidents plan in the BCM framework, most identified the irrelevance of (F) The key requirements of managing effective business continuity can be achieved by suppliers in the “cloud” as a critical incident for BCM. (D), Deliberate infiltration or attack on IT systems; followed by (A), Loss, damage or denial of access to key IT services; then (C) Loss or corruption of information; and B and D with arithmetic averages of 2.61 and 2.57 respectively.

5.2.2. Actions to be taken to ensure that there is ICT readiness and business continuity

The study sought to establish the participants' understanding of the key characteristics of BCM. The key characteristics of BCM identified from the findings were:

1. A planning process driven by risk and threat assessment is an important component of BCM.
2. Training, regular exercises and rehearsals are provided under BCM.
3. BCM at my organisation adopts a focus on critical capabilities and information.
4. There is teamwork and mutual support within the members involved in BCM.
5. BCM in my organisation has in place flexible and coordinated response measures.
6. BCM at my organisation takes on a focus on consequences not causes (6).

The nature of the available development plan to mitigate loss of critical assets and data was identified as follows:

1. There were alternative strategies available to mitigate loss of critical assets such as personnel, premises and ICT.
2. There is a plan that identifies actions that are necessary and resources that may be required to enable business to manage the consequences of disruption.
3. There are plans in place to resume after disruptions to activities: cross training of staff, alternative premises and off-site data, rerouting of telecoms.
4. There is a clear procedure for escalation and control of an incident.
5. The business impact analysis (BIA) that quantifies and qualifies the impacts of loss or disruption is in place.
6. A continuity culture is embedded in the business.

Ranking first, (B) showed that there were alternative strategies available to mitigate loss of critical assets, such as personnel, premises and ICT. Secondly, there was a plan that identified actions that were necessary and resources that could be required to enable business to manage the consequences of disruption (2). Thirdly, there were plans in place to resume after disruptions to activities – cross training of staff, alternative premises and off-site data, rerouting of telecoms (3). However, the findings show that the availability, of a clear procedure for escalation and control of an incident (4), The Business Impact Analysis (BIA) that quantifies and qualifies the impacts of loss or disruption is in place (5), and A Continuity culture is embedded in the business (6) were not prevalent.

5.2.3. Typical frameworks that exist, and elements that can be extracted from these frameworks to determine a possible framework for ICT readiness for Business Continuity

The existing ontologies that aid the identification of design requirements were identified for adoption from previous studies and practices or constructed for a new context that has not been reported in the literature. The study established a set of five elements extracted from various frameworks that can be useful in designing the artefact for ICT readiness for business continuity.

Table 8: Elements for designing artefact for ICT readiness for business continuity

1. Requirements for implementation of an effective of BCM Strategy ➢ Educational training of BCM ➢ Effective Communication ➢ Cultural changes ➢ Identification of Key Stakeholders ➢ Organisational resources allocation (Its assets, capabilities. Organisational processes, firm characteristics, information, knowledge, time, personnel) ➢ Human Resources- carriers of knowledge (key personnel role irreplaceable competencies, knowledge, skills and abilities essential to achieve the required level of performance	
2. A Theoretical framework (resource based view)- ➢ Four attributes should be available – resources, capabilities, competitive advantage and strategy	
3. Disaster recovery planning ➢ Stage 1- Analyse your business ➢ Stage 2- Assess risk ➢ Stage 3- Develop your strategy ➢ Stage 4- Develop your plan	4. Elements of BCM program ➢ Business impact analysis (BIA) - (of People. Technology. Processes) ➢ Business continuity planning (BCP) ➢ Disaster Recovery ➢ Testing
5. Conditions necessary for BCM program implementation ➢ Legislation or legal requirement ➢ Awareness campaign ➢ Industry focus/ industry specific ➢ Financial support	

5.3. OUTCOME

5.3.1. The framework that will assist SARS in implementing an effective ICT Readiness for Business Continuity

The objective of this study was to develop a framework to enhance ICT readiness for business continuity at the South African Revenue Services (SARS). The primary research objective was to develop a framework that public entities can use to ensure that their IRBC is effective and reduces the impact of information incidents on the organisation, with the last secondary objective being to recommend a suitable framework that will assist public entities in implementing an effective IRBC. In this step, the artefact was designed to address the identified problem/opportunity within the framework for CBM. The researcher constructed the artefact based on the proposed design requirements, and alternative solutions, relevant technologies and theories identified from previous steps are reflected through the development of the new artefact.

5.3.1.1. The artefact elements

The factors to make up the artefact derived from the research are as follows:

- Business analysis and business impact analysis - This involves analysis of the business to single out incidents that may have significant impact on the business continuity. There has to be initially an appreciation of what is critical r business operations by undertaking a Business Impact Analysis (BIA) to; identify key process and interactions; understand critical activities, identify key resources (people, IT systems, data / documentation, telecoms, essential stationary and specialized equipment) and to define what is critical and what would be deemed a serious incident.
- Development of strategy for appropriate response to analysis findings – develop a business continuity strategy to cover what you would do if an event (risk) occurred such as the following scenarios which may be the result of one of the above risks identified above occurring that has potential to disrupt business.
- Provision of required resources - Identification and protection of critical resources required to maintain an acceptable level of business, protecting such resources and preparing procedures to ensure the survival of the organization in times of business disruptions, valuable and non-substitutable resources which positively affect business continuity practices.
- Develop business continuity plan for disaster recovery - The organizations to plan for continued critical operations of workflow functions for disaster recovery.
- BCM policy drafting and legalising - The lack of a legal backing for implementation of BCM as well as policy guidelines greatly affects the successful implementation hence the need for such policy to be drafted as well as legalising the disaster recovery processes and responsibilities for accountability.

- Awareness campaign and education and training of BCM for key stakeholders – Awareness of BCM is critical for successful policy implementation as well as training on the action plan and steps in handling different disasters.

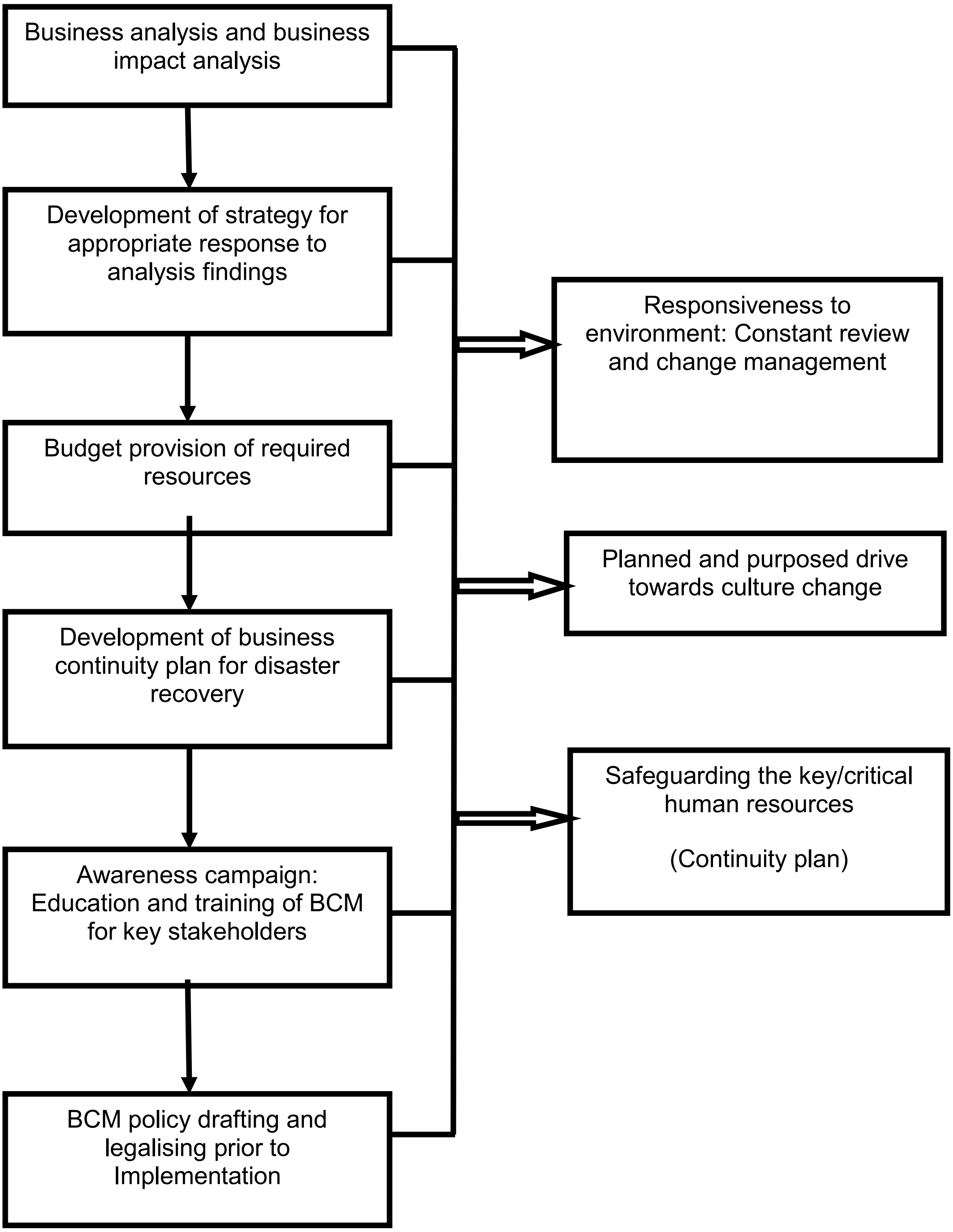
Mediating Factors

- Driving culture change - If top management supports the embedding of IS continuity practices throughout a company, heightened awareness and commitment would become part of the organisational culture for everyone. Also BCM policy should be appropriate and criticality of the business and must reflective of the organizational culture, if not, management has to drive culture change to fit effective implementation of the BCM policy.
- Safeguarding key critical human resources - An extension on the provision of the required resources for the implementation of the policy, critical human resources have to be preserved and safeguarded to ensure competitive advantage as well as the desired continuity in operations. Human resources are important as carriers of knowledge and therefore the protection of knowledge as the production resources and the employees as the carriers of the knowledge is vital to take account the value of key employees which play an irreplaceable role in the process of BCM application.
- Constant review and change management - Reviews are critical to ensure business continuity stays relevant and up-to-date followed by the implementation of the appropriate changes through formulation of proper change management structures and processes

This framework emphasises continuity through education and continuous training of the key stakeholders to narrow the knowledge gap to facilitate the effectiveness of the proposed change management structures. Critical human resources have to be preserved and safeguarded to ensure competitive advantage as well as the desired continuity in operations. This can be done through incentives as well as training of new personnel whilst the seasoned personnel are still available – thus managing loss of key personnel through separation. Points to note are the need to make the framework a statutory requirement through legalising it as well as the implementation of the BCM in the organisation.

5.3.1.2. The framework for ICT readiness for business continuity at the South African Revenue Services

Figure 10: Framework for ICT readiness for Business Continuity


Business analysis and business impact analysis
Development of strategy for appropriate response to analysis findings
Budget provision of required resources
Development of business continuity plan for disaster recovery
Awareness campaign: Education and training of BCM for key stakeholders
BCM policy drafting and legalising prior to Implementation
Responsiveness to environment: Constant review and change management
Planned and purposed drive towards culture change
Safeguarding the key/critical human resources
(Continuity plan)

Source: Researcher's own construct adopted from Larsen (2016) and ISO/IEC 37021 and ISO/IEC 37022

The proposed framework above was customised from other frameworks to suit the SARS enviroment. SARS may also need to form a committee to ensure accountability and performance tracking to successfully achieve the goal of implementing effective BCM. “The success of embedding BCM lies in organisational structure and creation of organtional conditions for effective implementation.” Larsen (2016)

5.4. CONCLUSION

This chapter discussed the research findings and provided the conclusion through the meeting of the main research objective to design a framework for effective implementation of IRBC-BCM. The next chapter constitutes an evaluation, which seeks to validate the proposed framework phase as well as the recommendations for further studies.

CHAPTER 6
VALIDATION OF FRAMEWORK AND RECOMMENDATIONS FOR FURTHER STUDY

6.1. INTRODUCTION

In evaluating the framework, the researcher analysed the availability of essential elements in DSR, demonstration of relevance to the environment, and research significance to the field. This is critical to help distinguishing DSR artefacts from practice-based IT applications.

6.2. VALIDATION OF THE DESIGNED FRAMEWORK

Evaluation of research conclusions is usually dependent on the nature of the problem and/or solution (purely technical or at least partially social or organisational). This paper adopted a naturalistic evaluation that enables a researcher to explore how well or poorly the solution technology works in terms of promoting CBM in its real environment – the organisation.

6.2.1. Relevance to the environment

People’s opinions or perceptions rather than the phenomenon itself were derived from the research responses of the selected sample and the conclusions thereof. Hence, in this study, successfully solving a problem was about whether the framework addresses the gaps witnessed from the research findings.

The artefact is considered relevant to the environment, firstly because it incorporates ideas from international standards and best practice frameworks. Relevance of this IRRBC-BCM framework was also derived after considering the results from the study which give a reflection of gaps within SARS as an organisation which informed the research conclusions. There is certainty that the framework addresses the gaps, for example in the nature of the environment, the lack of knowledge, the lack of a legal backing for implementation of BCM and the lack of resources which is affected by having the Board not being part of the BCM drive. All these are issues incorporated within the proposed framework.

The research followed the design science research approach which offers proper direction in the implementation or design of IT-based frameworks, hence the following of appropriate processes and stages to arrive at the final recommendation. The study participants in terms of demography consisted of highly qualified personnel. Seasoned employees with great knowledge of the organisation's systems and dynamics, top level management as well as a fair number of IT personnel at operational level were represented and the response rate was 49/100, a response rate of 49%, which offers high representation of the population in terms of the results and findings arrived at which informed the main research objective.

6.2.2. Limitations of the Study

It has to be noted that a limitation to the study is the possibility that respondents may not have answered truthfully and could have just painted a perfect picture. The study was mainly based on the sample size which was rather small and compounded by the low response rate of 49%. However, the homogeneity of the sample aided on the adequacy of the responses range.

6.2.3. Research significance to the field

The current business and operational environment is highly influenced and affected by developments in the IT environment, which is highly volatile and dynamic as well as being costly to organisations in terms of implementation, maintenance, upgrading, monitoring and control. Because of the IT influence which has resulted in the phasing out of manual data storage to digital data storage of all operational and critical data, the risks that come with any malfunction, error or disruptions in the systems are highly detrimental to organisations, and more so SARS which handles data for the whole South African economy in terms of fiscal data and taxation data (De Jongh, 2013). It is therefore critical and relevant that concentrated attention be placed on the field in terms of business continuity planning, of which a framework to guide the design or implementation of a business continuity management system is highly significant.

This research contributes to an understanding of the importance and significance as well as strategies for business continuity and the effects of the risks involved in the lack of the same. The researcher discovered some areas in the field that could need further study to fill the knowledge gap as well as offer solutions to societal problems in the field and they are listed in the next section.

6.3. RECOMMENDATIONS FOR FURTHER STUDY

1. Strategies and challenges in being responsive to the dynamic digital age while maintaining the continuity management requirement.
2. An examination of the extent of BCM implementation in public sector organisations in South Africa.

REFERENCE LIST

A'Nasiren, M.D., Abdullah, M.N. & Asmoni, M. 2016. Critical success factors on the BCM implementation in SMEs. *Journal of Advanced Research in Business and Management Studies*, 3(1):105–122.

ACI World Secretariat. 2012. *Best practice paper: BCM framework and case studies for health related disruptions at airports*. Cape Town: ACI.

Agrawal, A., Gans, J.S. & Goldfarb, A. 2019. Artificial intelligence: The ambiguous labour market impact of automating prediction. *Journal of Economic Perspectives*, 33(2):31–50.

Alesi, P. 2008. Building enterprise-wide resilience by integrating business continuity capability into day-to-day business culture and technology. *Journal of Business Continuity & Emergency Planning*, 2(3):214–220.

Alturki, A., Gable, G.G. & Bandara, W. 2013. *The design science research roadmap: In progress evaluation*. PACIS 2013 Proceedings. Available: http://eprints.qut.edu.au/61626/ [Accessed: 24 May 2019].

Armstrong, C. & Armstrong, H. 2010. Modeling forensic evidence systems using design science. *Information Systems Design Science Research*, 5(17):282–300.

Asian Disaster Reduction Centre (ADRC). 2012. *BCP status of the SMEs in the Asia-Pacific region.* Japan: Asian Disaster Reduction Center.

Barney, J.B. 2002. *Gaining and sustaining competitive advantage*. Upper Saddle River, NJ: Prentice Hall.

Bird, L. & Higgins, D. 2013. *Good practice guidelines 2013*. United Kingdom: Business Continuity Institute (BCI).

Bras, J. & Ribeiro, R. 2016. *Business continuity and disaster recovery: An overview, trends and challenges*. 13th International Conference of Information Systems and Technology Management (CONTECSI), Brazil.

Business Continuity Institute (BCI). 2010. *Good practice guidelines 2010*. Available: http://www.efectus.cl/upload_files/documentos/20042010092531-112191411.pdf [Accessed: 24 March 2019].

Butler, B.S. & Gray, P.H. 2006. Reliability, mindfulness, and information systems. *MIS Quarterly*, 30(2):211–224.

Carley, K. 1993. Coding choices for textual analysis: A comparison of content analysis and map analysis. *Sociological Methodology*, 23:75–126.

Chow, W.S. & Ha, W.O. 2009. Determinants of the critical success factor of disaster recovery planning for information systems*. Information Management & Computer Security*, 17(3):248–275. Available: https://doi.org/10.1108/09685220910978103 [Accessed 3 May 2019].

Christensen, C.M. 1997. *The innovator's dilemma: When new technologies cause great firms to fail.* Boston, MA: Harvard Business School Press.

Cook, J. 2015. A six-stage business continuity and disaster recovery planning cycle. *Advanced Management Journal*, 80(3):23–68.

Coombs, W.T. 2007. Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, 10(3), 163–176. Available: http://dx.doi.org/10.1057/palgrave.crr.1550049 [Accessed: 24 March 2019].

Costa, P., Montero, P.J.J. & Roson, R. 2018. *The impact of disruptive technologies on infrastructure networks*. Organisation for Economic Co-operation and Development (OECD). Available: https://www.sipotra.it/old/wp-content/uploads/2018/11/The-impact-of-disruptive-technologies-on-infrastructure-networks.pdf [Accessed: 4 March 2019].

Crowe. 2019. *Healthcare business continuity management and disaster recovery—No longer an afterthought in today's world*. Association of Healthcare Internal Auditors. Available: https://ahia.org/getattachment/news/White-Papers/AHIA-Crowe-Whitepaper.pdf/?lang=en-US [Accessed: 15 May 2019].

Cruz, C.O. & Sarmento, J.M. 2018. Maximizing the value for money of road projects through digitalization. *Research in Transportation Economics*, 70:161–172.

Daneshkhah, A., Stocks, N.G. & Jeffrey, P. 2017. Probabilistic sensitivity analysis of optimised preventive maintenance strategies for deteriorating infrastructure assets. *Reliability Engineering & System Safety*, 163:33–45.

De Almeida Biolchini, J.C., Mian, P.G., Natali, A.C.C., Conte, T.U. & Travassos, G.H. 2007. Scientific research ontology to support systematic review in software engineering. *Advanced Engineering Informatics*, 21(2):133–151.

De Jongh, E. (2013). *A review of operational risk in banks and its role in the financial crisis. South African Journal of Economic and Management Sciences*, 16(4): 364-382.

De Leoz, G. & Petter, S. 2018. Considering the social impacts of artefacts in information systems design science research. *European Journal of Information Systems*, 27(2):154–170.

Departmental Business Continuity Management Team (2009). Departmental Business Continuity Framework Part 1 – Policy and Standards. Department for Work and Pensions; available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61083/dwp-bc-framework-part1.pdf accessed 15.03.2020

Domegan, C. & Fleming, D. (2007) Marketing Research in Ireland: Theory and Practice, 3rd Edition

Domingos, P. 2015. *The master algorithm: How the quest for the ultimate learning machine will remake our world*. New York: Basic Books.

Downes, L. 2018. Why is business continuity management so important? *IT Governance*, 30 October. Available: https://www.itgovernance.eu/blog/en/why-is-business-continuity-management-so-important [Accessed: 24 August 2019].

Duncan, W.J., Yeager, V.A., Rucks, A.C. & Ginter, P.M. 2011. Surviving organizational disasters. *Business Horizons*, 54(2):135–142.

Elliott, D., Swartz, E. & Herbane, B. 2010. *Business continuity management: A crisis management approach*. 2nd Edition. London: Routledge.

ENISA. 2010. IT business continuity management: An approach for small medium sized organization. *ENISA: BCM: An Approach for SMEs*, p.127.

Ernst & Young. 2011. *Into the cloud, out of the fog*. Ernst & Young's 2011 Global Information Security Survey. Available: https://www.shinnihon.or.jp/shinnihonlibrary/publications/research/2012/pdf/2011-GlobalInformationSecuritysurvey-E.pdf [Accessed: 24 April 2019].

Evans, D.S. & Schmalensee, R. 2016. *Matchmakers. The new economics of multisided platforms*. Boston: Harvard Business Review Press.

Finney, S. & Corbett, M. 2007. ERP implementation: A compilation and analysis of critical success factors. *Business Process Management Journal*, 13(3):329–347.

Gallagher, M. 2005. The road to effective business continuity management. *Accountancy Ireland*, 37(2):66–68.

Gans, J.S. 2016. Keep calm and manage disruption. *Sloan Management Review*, 57(3):83–95.

Garrett, D.N. 2012. *The evolution of business continuity management in large Irish enterprises between 2004 and 2009*. Unpublished PhD dissertation. Dublin: City University.

Gazem, N., Rahman, A.A., Saeed, F. & Iahad, N.A. 2018. Design science research roadmap model for information systems projects. *International Journal of Information Technology Project Management*, 9(3):1–19.

Giacchero A, Giordano, F. & Schiraldi, M. 2013. From business continuity to design of critical infrastructures: Ensuring the proper resilience level to datacenters. *International Journal of Engineering and Technologies (IJET)*, 5(4):3544–3553.

Gibb, F. & Buchanan, S. 2006. A framework for business continuity management. *International Journal of Information Management*, 26(2):128–141.

Gneist, P., Kiersz, R. & Osman, O. 2009. *The need for a developed business continuity plan*. Jönköping International Business School. Available: http://www.diva-portal.org/smash/get/diva2:222109/FULLTEXT01.pdf [Accessed: 4 June 2019].

Government of Western Australia. 2017. *Whole of Government: ICT disaster recovery for Business Continuity Policy –A supplementary guide*, Version 1, April. Available: https://www.wa.gov.au/sites/default/files/2018-06/ICT%20Disaster%20Recovery%20for%20Business%20Continuity%20Policy%20Supporting%20Guide.pdf [Accessed: 1 February 2019].

Gregor, S. & Jones, D. 2007. The anatomy of a design theory. *Journal of Association for Information Systems*, 8(5):312–335.

Herbane, B. 2010. The evolution of business continuity management: A historical review of practices and drivers. *Business History*, 52(6), 978–1002. Available: http://dx.doi.org/10.1080/00076791.2010.511185 [Accessed: 21 March 2019].

Herbane, B., Elliott, D. & Swartz, E. 2004. Business continuity management: Time for a strategic role? *Long Range Planning*, 37(5):435–457.

Hevner, A.R. & March, S.T. 2003. The Information Systems Research Cycle. *IT Systems Perspective*, 36(11):111–113.

Hevner, A.R., March, S.T. & Park, J. 2004. Design research in information systems research. *MIS Quarterly*, 28(1):75–105.

Hevner, A.R., March, S.T., Park, J. & Ram, S. 2004. Design science in information systems research. *MIS Quarterly*, 28(1):75–105.

Hinson, G. 2012. *Technical briefing: Business continuity management*. Available: https://www.tandfonline.com/doi/full/10.1080/07366981.2012.678125?scroll=top&needAccess=true [Accessed: 16 May 2019].

Holmström, J.B., Ketokivi, M. & Hameri, A.P. 2009. Bridging practice and theory: A design science approach. *Decision Science*, 40(1):65–87.

International Organization for Standardization (ISO). 2012. *Societal security – Business continuity management systems – Requirements*. International Organization for Standardization (ISO). Available: http://www.iso.org/iso/catalogue_detail?csnumber=50038 [Accessed: 24 May 2019].

ISO/IEC 27031. 2011. Information technology - Security techniques. *Guidelines for Information Technology Readiness for Business Continuity*, 1(1):1–36.

ITWeb. 2018. *Regulatory pressure could hurt African telecoms market*. Available: https://www.itweb.co.za/content/WnxpEv4aGWB7V8XL [Accessed: 24 April 2019].

Ivancevich, D.M., Hermanson, D.R. & Smith, L.M. 1998. The association of perceived disaster recovery plan strength with organizational characteristics. *Journal of Information Systems*, 12(1):31–40.

Jardine, A.K., Lin, D. & Banjevic, D. 2006. A review on machinery diagnostics and prognostics implementing condition-based maintenance. Mechanical Systems and Signal Processing, 20(7):1483–1510.

Järveläinen, J. 2013. IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, 33(3):583–590.

Johnson, R.B., Onwuegbuzie A.J. & Turner, L.A. 2007. Toward a definition of mixed methods research. *Journal of Mixed Methods Research*, 1(2): 112–133. Available: http://mmr.sagepub.com [Accessed: 14 June 2019].

Kearney, A.T. 2017. Technology and Innovation for the Future of Production: Accelerating Value Creation   Available: http://www3.weforum.org/docs/WEF_White_Paper_Technology_Innovation_Future_of_Production_2017.pdf [Accessed: 16 November 2020].

Königová, M. & Fejfar, J. 2013. Role of personnel planning in business continuity management. In *Proceedings of World Academy of Science, Engineering and Technology*, 76: 213. World Academy of Science, Engineering and Technology (WASET).

Krell, E. 2006. *Management accounting guideline: Business continuity management*. Canada: The Society of Management Accountants of Canada and the American Institute of Certified Public Accountants.

Kreutz, D., Ramos, F.M., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S. & Uhlig, S. 2015. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76.

Larsen, A. (2016). *Business Continuity Management*. https://www.slideshare.net/AlexanderLarsen/business-continuity-management-bcm-bcp-smaple-animations-dont-work-in-slideshare. Date of access 1 November 2019.

Lou, P., Liu, S.J. & Sio, S. 2010. Business continuity management in large construction companies in Singapore. *Disaster Prevention and Management: An International Journal,* 19(2):219–232.

Luftman, J. & Zadeh, H.S. 2011. Key information technology and management issues 2010–2011: an international study. *Journal of Information Technology*, 26(3):193–204. Available: http://dx.doi.org/10.1057/jit.2011.3 [Accessed: 23 April 2019].

Luoma-aho, V. & Paloviita, A. 2010. Actor-networking stakeholder theory for today’s corporate communications. *Corporate Communications: An International Journal*, 15(1):49–67. Available: http://dx.doi.org/10.1108/13563281011016831 [Accessed: 24 March 2019].

Manchester Business Community Forum. 2018. *Business continuity, whatever, the disruption*. Available: www.what_is_Business_Continuity.pdf [Accessed: 12 May 2019].

Markus, M.L., Majchrzak, A. & Gasser, L. 2002. A design theory for systems that support emergent knowledge processes. *MIS Quarterly*, 26(3):179–212.

McKinsey & Company. 2016. *Huge value pool shifts ahead – How rolling stock manufacturers can lay track for profitable growth*. Available: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/How%20rolling%20stock%20manufacturers%20can%20lay%20track%20for%20profitable%20growth/How-rolling-stock-manufacturers-can-lay-track-for-profitable-growth.ashx [Accessed: 24 March 2019].

Mithas, S., Ramasubbu, N. & Sambamurthy, V. 2011. How information management capability influences firm performance. *MIS Quarterly*, 35(1):137–A15.

Momani, N.M. 2010. Business continuity planning: are we prepared for future disasters. *American Journal of Economics and Business Administration*, 2(3):272–279.

Morse, J. M. 2000. Determining sample size. Qual Health Res, 10(1):3–5.

Morwood, G. 1998. Business continuity: Awareness and training programmes. *Information Management & Computer Security,* 6(1):28-32. Available: http://dx.doi.org/10.1108/09685229810207425 [Accessed: 4 June 2019].

Nelson, H.G. & Stolterman, E. 2012. *The design way: Intentional change in an unpredictable world.* Cambridge, MA: The MIT Press.

Nicholas, M. 2008. *Business continuity & resilience capability and solutions*. Available:

http://www.back2business.com/pdf/back2business%20briefing%20pack.pdf [Accessed: 16 May 2019].

Nunamaker, J.F., Chen, M. & Purdin, T.D.M. 1991. Systems development in information systems research. *Journal of Management Information Systems*, 7(3):89–106.

Organisation for Economic Co-operation and Development (OECD) 2009. *Two-sided markets, policy roundtables*. Paris: OECD Publishing. Available: https://www.oecd.org/daf/competition/44445730.pdf [Accessed: 1 May 2019].

Organisation for Economic Co-operation and Development (OECD). 2017. *Trust in peer platform markets: Consumer survey findings*. OECD Digital Economy Papers No. 263. Paris: OECD Publishing. Available: https://doi.org/10.1787/1a893b58-en [Accessed: 2 April 2019].

Orlikowski, W.J. & Iacono, C.S. 2001. Research commentary: Desperately seeking the 'IT' in IT Research – A call to theorizing the IT artifact*. Information Systems Research*, 12(2):121–134.

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. 2007. A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3):45–48.

Penrose, E. T. (1959). *The Theory of the Growth of the Firm*. New York: John Wiley.
Google Scholar

Pheng Low, S., Liu, J. & Sio, S. 2010. Business continuity management in large construction companies in Singapore. *Disaster Prevention and Management: An International Journal*, 19(2):219–232.

Priem, R.L. & Butler, J.E. 2001. Is the resource based view a useful perspective for strategic management research? *Academy of Management Review*, 26(1):22–40.

Rasi, R.Z.R.M., Raja, Abdekhodaee, A. & Nagarajah, R. 2014. Stakeholders' involvements in the implementation of proactive environmental practices: Linking environmental practices and environmental performances in SMEs. *Management of Environmental Quality: An International Journal*, 25(2):132–149.

Rochet, J.C. & Tirole, J. 2003. Platform competition in two-sided markets. *Journal of the European Economic Association*, 1(4):990–1029.

Rossi, M. & Sein, M.K. 2003. *Design research workshop: A proactive research approach.* 26th Information Systems Research Seminar in Scandinavia, Haikko Finland, The IRIS Association.

Royds, J. 2010. Business continuity management: An introductory guide. *Faculty of Information Technology*, 1(1):1–36.

SARS 2019 Annual Performance plan. https://www.sars.gov.za/AllDocs/SARSEntDoclib/Ent/SARS-Strat-22%20-%20SARS%20Annual%20Performance%20Plan%202019-2020%20-%2017%20September%202019.pdf

SARS 2020 Strategic plan 2020/21 – 2024/25 https://www.sars.gov.za/AllDocs/SARSEntDoclib/Ent/SARS-Strat-23%20-%20SARS%20Annual%20Performance%20Plan%202020-2021%20-%2011%20May%202020.pdf, page 29

SARS. 2019. What SARS does. https://www.sars.gov.za/About/Pages/default.aspx.

Seow, K. 2009. Gaining senior executive commitment to business continuity: Motivators and reinforcers. *Journal of Business Continuity & Emergency Planning*, 3(3):201–208.

Sheffi, Y. & Rice, J.B. 2005. A supply chain view of the resilient enterprise. *MIT Sloan Management Review*, 47(1):41–48.

Shuja, A. & Abbasi, A.S. 2015. An investigation of the impact of resource mobilization on business continuity management: a study on banking sector of Pakistan. *Science International (Lahore)*, 27(3): 2551–2558. Available: www.sci-int.com/.../2142185562551- 2558%20Aleena%20Shuja%202++ [Accessed: 24 February 2016].

Siponen, M. & Willison, R. 2009. Information security management standards: Problems and solutions. *Information & Management*, 46(5):267–270. doi:16/j.im.2008.12.007

Smith, K.T., Smith, M. & Wang, K. 2010. Does brand management of corporate reputation translate into higher market value? *Journal of Strategic Marketing*, 18(3):201–221. Available: http://dx.doi.org/10.1080/09652540903537030 [Accessed: 16 June 2019].

South Africanmi. 2019. SA vs World. Available: https://www.southafricanmi.com/sa-vs-the-world.html

Speight, P. 2011. Business continuity. *Journal of Applied Security Research*. Available: https://www.tandfonline.com/doi/abs/10.1080/19361610.2011.604021 [Accessed: 16 May 2019].

Starr, R., Newfrock, J. & Delurey, M. 2003. Enterprise resilience: Managing risk in the networked economy. *Strategy and Business*, 30(Spring):1–10.

Statistics South Africa (Stats SA). 2017. *Quarterly employment*. Available: http://www.statssa.gov.za/?m=2017 [Accessed: 24 July 2019].

Tammineedi, R.L. 2010. Business continuity management: A standards-based approach. *Information Security Journal: A Global Perspective*, 19(1):36–50.

TechCentral. 2018. *The Woan could succeed, but only if done right*. Available: https://techcentral.co.za/woan-succeed-done-right/79712/ [Accessed: 24 June 2019].

Vaishnavi, V. & Kuechler, B. 2005. *Design research in information systems*. Association for Information Systems. Available: http://www.isworld.org [Accessed:24 June 2019].

Van Aken, J.E. (2004). Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules. *Journal of Management Studies*, 41(2):219–246.

Verman, A.G. 2011. Business continuity planning in the IT age: A railway sector case study. *Journal of Business Management*, 3(5):11–36.

Wang, Y.S., Wu, S.C., Lin, H.H. & Wang, Y.Y. 2010. The relationship of service failure severity, service recovery justice and perceived switching costs with customer loyalty in the context of e-tailing. *International Journal of Information Management*, 31(4):350–359.

Wieringa, R.J. 2014. *Design science methodology for information systems and software engineering*. 1st Edition. New York: Springer.

Wong, B.K., Monaco, J.A. & Sellaro, C.L. 1994. Disaster recovery planning: Suggestions to top management and information systems managers. *Journal of Systems Management*, 45(5):28–33.

Woodman, P. 2007. *Business continuity management*. Chartered Management Institute. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60842/bcm_report2007.pdf [Accessed: 3 June 2019].

APPENDIX A:
STUDY QUESTIONNAIRE

Section A: Demographic Information

Please tick the most appropriate box in this section that fits your background.

1. Gender of interviewee

Gender	Please choose/tick your age range with an X
Male	
Female	

2. Level of Employment with SARS

Position or Level of Employment	Please choose/tick your position/level of employment an X
Executive Management	
Senior Management	
Middle management	
Operational staff	
Other (explain)	

3. Length of Employment

Length of employment	Please choose/tick your appropriate years of employment an X
1 to 5 years	
6 to 10 years	
10 – 20 years	
Over 20 years	

4. Highest Educational Qualifications

Highest educational qualifications	Please select most appropriate highest level of educational qualifications with an X
Diploma	
Degree/Honors degree	

Master’s degree	
PhD/Doctorate	

Section 2: The benefits of BCM

5. BCM offers the ability to identify risks to operations and put in place a capability to mitigate and manage those risks

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

6. BCM provides the ability to manage uninsurable risk, such as risk to reputation

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

7. BCM avails an effective response to major disruptions

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

8. BCM is important because it provides the ability to demonstrate that the process is credible and consistent via exercising and auditing

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

9. There are competitive advantages conferred in BCM by the ability to maintain customer service, staff employment and stakeholder confidence

Strongly Disagree 😫	**Disagree** ☹	**Not sure** 😐	**Agree** ☺	**Strongly Agree** 😍

Section 3: Critical incidents covered

The following critical incidents are covered in the BCM plan:

10 Loss, damage or denial of access to key IT services

Strongly Disagree 😫	**Disagree** ☹	**Not sure** 😐	**Agree** ☺	**Strongly Agree** 😍

11 Failure or non-performance of critical service providers, distributors, or commercial third parties like trading partners.

Strongly Disagree 😫	**Disagree** ☹	**Not sure** 😐	**Agree** ☺	**Strongly Agree** 😍

12 Loss or corruption of information

Strongly Disagree 😫	**Disagree** ☹	**Not sure** 😐	**Agree** ☺	**Strongly Agree** 😍

13 Sabotage or commercial espionage

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

14 Deliberate infiltration or attack on IT Systems

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

15 The key requirements of managing effective business continuity can be achieved by suppliers in the "cloud".

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

Section 4: Key characteristics of the framework

The key characteristics of BCM are:

16 A planning process driven by risk and threat assessment is an important component of BCM

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

17 BCM at my organization takes on a focus on consequences not causes

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

18 BCM at my organization adopts a focus on critical capabilities and information

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

19 There is teamwork and mutual support within the members involved in BCM

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

20. Training, regular exercises and rehearsals are provided under BCM

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

21 BCM in my organization has in place flexible and coordinated response measures

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

Section 5: Developing a plan

22 The Business Impact Analysis (BIA) that quantifies and qualifies the impacts of loss or disruption is in place

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

23 There are alternative strategies that are available to mitigate loss of critical assets such as personnel, premises and ICT

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

24 There is a plan that identifies actions that are necessary and resources that may be required to enable business to manage the consequences of disruption

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

25 There is a clear procedure for escalation and control of an incident

Strongly Disagree 😫	Disagree ☹	Not sure 😐	Agree ☺	Strongly Agree 😍

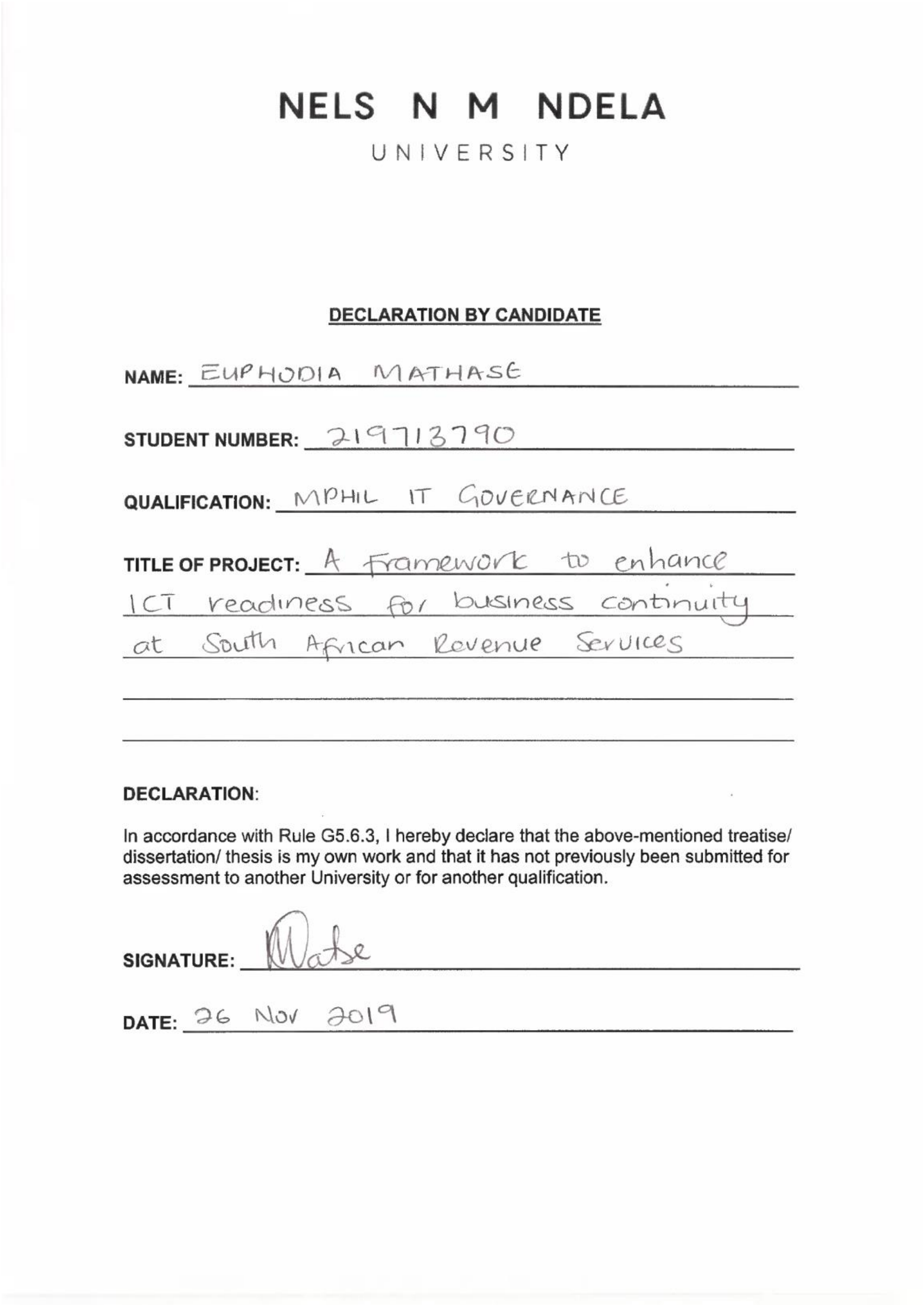
26 There are plans in place to resume after disruptions to activities – cross training of staff, alternative premises and off-site data, rerouting of telecoms.

Strongly Disagree 😫	**Disagree** ☹	**Not sure** 😐	**Agree** ☺	**Strongly Agree** 😍

27 A continuity culture is embedded in the business

Strongly Disagree 😫	**Disagree** ☹	**Not sure** 😐	**Agree** ☺	**Strongly Agree** 😍

APPENDIX B:
DECLARATION BY CANDIDATE



NELS N M NDELA
UNIVERSITY

DECLARATION BY CANDIDATE

NAME: EUPHODIA MATHASE

STUDENT NUMBER: 219713790

QUALIFICATION: MPHIL IT GOVERNANCE

TITLE OF PROJECT: A Framework to enhance ICT readiness for business continuity at South African Revenue Services

DECLARATION:

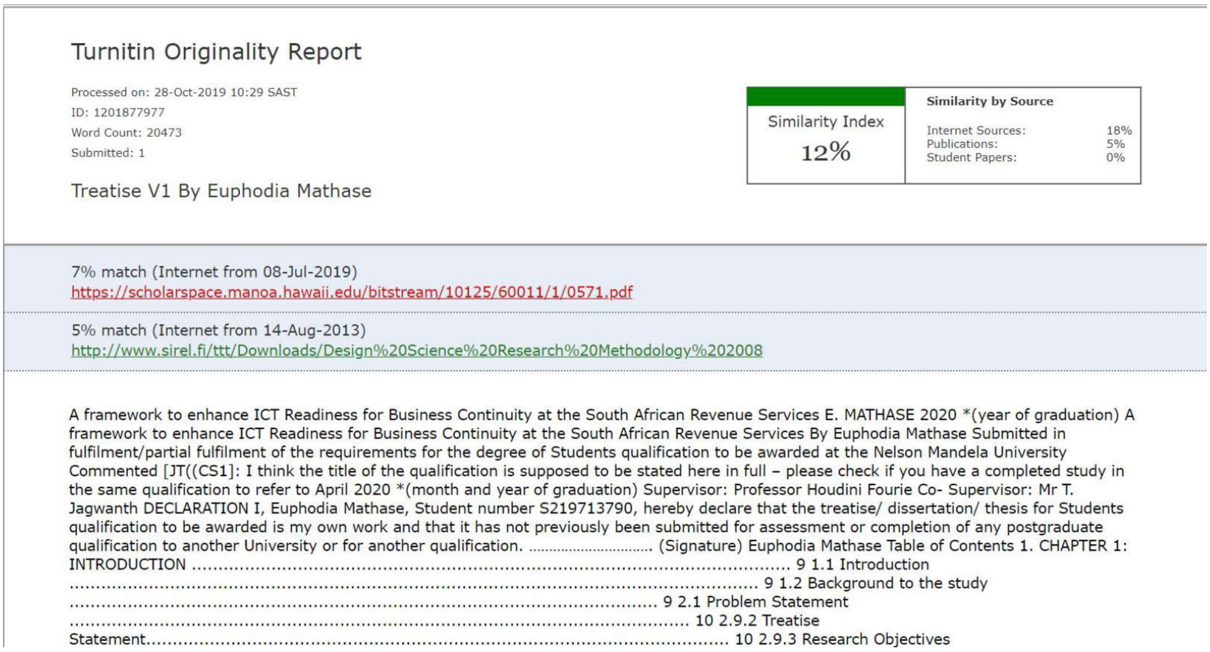
In accordance with Rule G5.6.3, I hereby declare that the above-mentioned treatise/ dissertation/ thesis is my own work and that it has not previously been submitted for assessment to another University or for another qualification.

SIGNATURE:

DATE: 26 Nov 2019

APPENDIX C:

TURNITIN REPORT



Turnitin Originality Report

Processed on: 28-Oct-2019 10:29 SAST
ID: 1201877977
Word Count: 20473
Submitted: 1

Treatise V1 By Euphodia Mathase

Similarity Index
12%

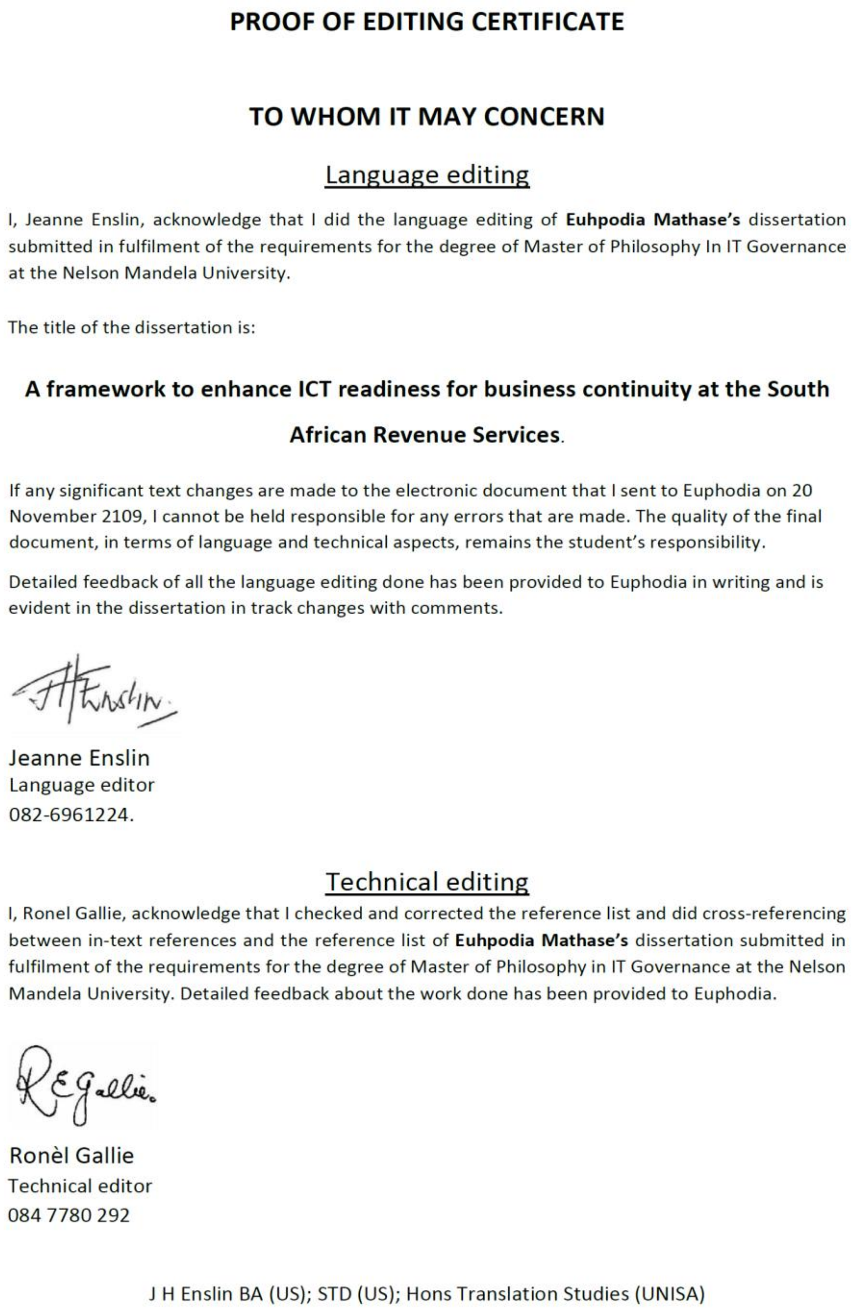
Similarity by Source	
Internet Sources:	18%
Publications:	5%
Student Papers:	0%

7% match (Internet from 08-Jul-2019)
https://scholarspace.manoa.hawaii.edu/bitstream/10125/60011/1/0571.pdf

5% match (Internet from 14-Aug-2013)
http://www.sirel.fi/ttt/Downloads/Design%20Science%20Research%20Methodology%202008

A framework to enhance ICT Readiness for Business Continuity at the South African Revenue Services E. MATHASE 2020 *(year of graduation) A framework to enhance ICT Readiness for Business Continuity at the South African Revenue Services By Euphodia Mathase Submitted in fulfilment/partial fulfilment of the requirements for the degree of Students qualification to be awarded at the Nelson Mandela University Commented [JT((CS1]: I think the title of the qualification is supposed to be stated here in full – please check if you have a completed study in the same qualification to refer to April 2020 *(month and year of graduation) Supervisor: Professor Houdini Fourie Co- Supervisor: Mr T. Jagwanth DECLARATION I, Euphodia Mathase, Student number S219713790, hereby declare that the treatise/ dissertation/ thesis for Students qualification to be awarded is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification. .... (Signature) Euphodia Mathase Table of Contents 1. CHAPTER 1: INTRODUCTION .... 9 1.1 Introduction .... 9 1.2 Background to the study .... 9 2.1 Problem Statement .... 10 2.9.2 Treatise Statement.. 10 2.9.3 Research Objectives

APPENDIX D:
EDITING CERTIFICATE



PROOF OF EDITING CERTIFICATE

TO WHOM IT MAY CONCERN

Language editing

I, Jeanne Enslin, acknowledge that I did the language editing of **Euhpodia Mathase's** dissertation submitted in fulfilment of the requirements for the degree of Master of Philosophy In IT Governance at the Nelson Mandela University.

The title of the dissertation is:

A framework to enhance ICT readiness for business continuity at the South African Revenue Services.

If any significant text changes are made to the electronic document that I sent to Euphodia on 20 November 2109, I cannot be held responsible for any errors that are made. The quality of the final document, in terms of language and technical aspects, remains the student's responsibility.

Detailed feedback of all the language editing done has been provided to Euphodia in writing and is evident in the dissertation in track changes with comments.

JHEnslin.

Jeanne Enslin
Language editor
082-6961224.

Technical editing

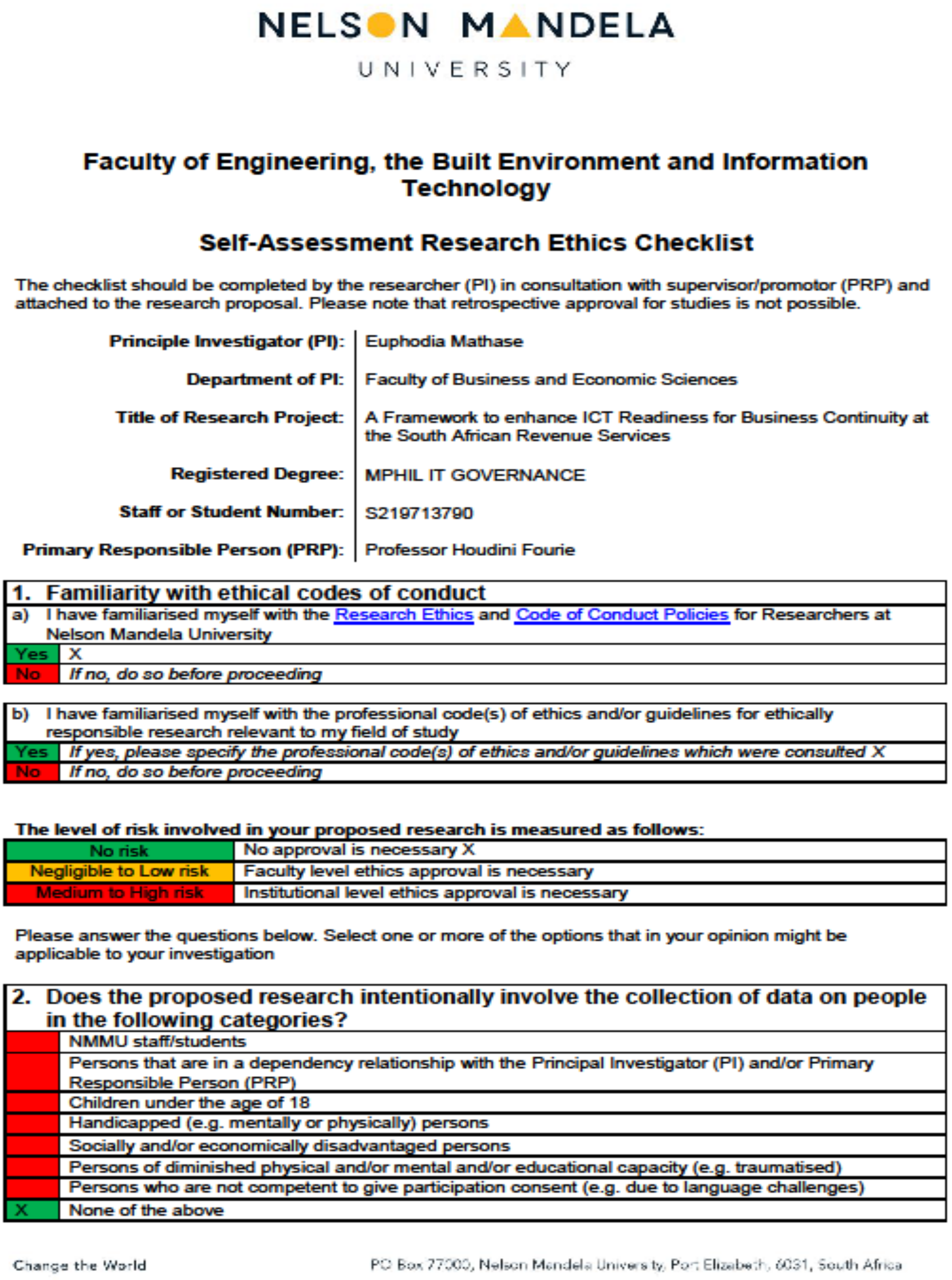
I, Ronel Gallie, acknowledge that I checked and corrected the reference list and did cross-referencing between in-text references and the reference list of **Euhpodia Mathase's** dissertation submitted in fulfilment of the requirements for the degree of Master of Philosophy in IT Governance at the Nelson Mandela University. Detailed feedback about the work done has been provided to Euphodia.

REGallie.

Ronèl Gallie
Technical editor
084 7780 292

J H Enslin BA (US); STD (US); Hons Translation Studies (UNISA)

APPENDIX E:
ETHICAL CHECKLIST



NELSON MANDELA
UNIVERSITY

Faculty of Engineering, the Built Environment and Information Technology

Self-Assessment Research Ethics Checklist

The checklist should be completed by the researcher (PI) in consultation with supervisor/promotor (PRP) and attached to the research proposal. Please note that retrospective approval for studies is not possible.

Principle Investigator (PI):	Euphodia Mathase
Department of PI:	Faculty of Business and Economic Sciences
Title of Research Project:	A Framework to enhance ICT Readiness for Business Continuity at the South African Revenue Services
Registered Degree:	MPHIL IT GOVERNANCE
Staff or Student Number:	S219713790
Primary Responsible Person (PRP):	Professor Houdini Fourie

1. Familiarity with ethical codes of conduct	
a)	I have familiarised myself with the Research Ethics and Code of Conduct Policies for Researchers at Nelson Mandela University
Yes	X
No	*If no, do so before proceeding*

b)	I have familiarised myself with the professional code(s) of ethics and/or guidelines for ethically responsible research relevant to my field of study
Yes	*If yes, please specify the professional code(s) of ethics and/or guidelines which were consulted* X
No	*If no, do so before proceeding*

The level of risk involved in your proposed research is measured as follows:

No risk	No approval is necessary X
Negligible to Low risk	Faculty level ethics approval is necessary
Medium to High risk	Institutional level ethics approval is necessary

Please answer the questions below. Select one or more of the options that in your opinion might be applicable to your investigation

2. Does the proposed research intentionally involve the collection of data on people in the following categories?	
🟥	NMMU staff/students
🟥	Persons that are in a dependency relationship with the Principal Investigator (PI) and/or Primary Responsible Person (PRP)
🟥	Children under the age of 18
🟥	Handicapped (e.g. mentally or physically) persons
🟥	Socially and/or economically disadvantaged persons
🟥	Persons of diminished physical and/or mental and/or educational capacity (e.g. traumatised)
🟥	Persons who are not competent to give participation consent (e.g. due to language challenges)
X	None of the above

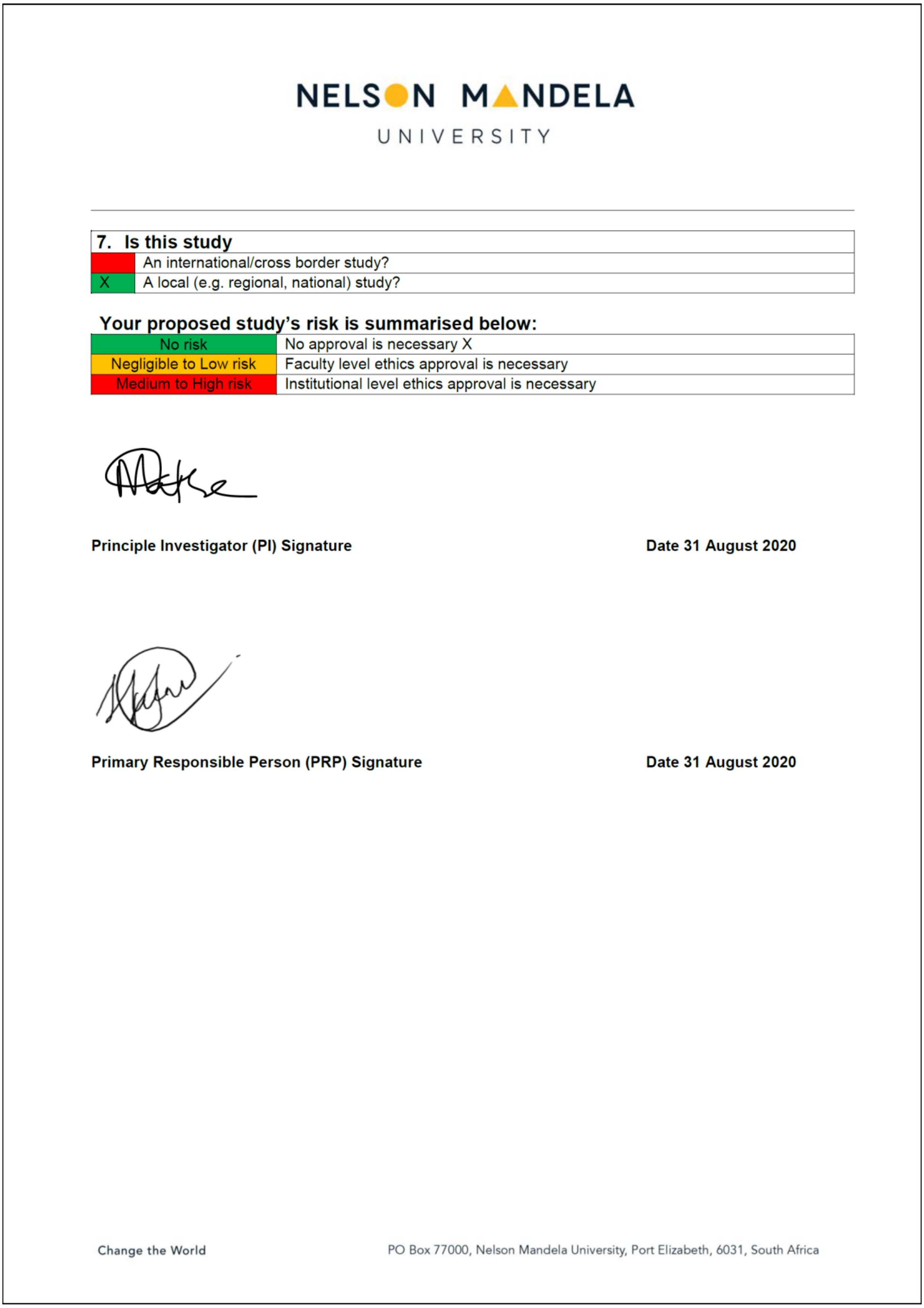
Change the World PO Box 77000, Nelson Mandela University, Port Elizabeth, 6031, South Africa

3.	**Are you administering any process and/or treatment that**
🟥	Involves participants undergoing psychological, physiological or medical testing or treatment.
🟥	Involves the collection and use of human biological samples (e.g. skin, blood, urine, saliva, hair, bones, tumour and other biopsy specimens) or their exhaled breath.
🟥	Could be hazardous to the physical health (e.g. possibly results in illness, injury, pain) of the participants and/or researcher.
🟥	Could be hazardous to the psychological well-being (e.g. possibly results in feelings of worthlessness, guilt, anger, fear) of the participants and/or researcher.
🟥	Could be hazardous to the legal well-being (e.g. possibly results in the discovery and prosecution of criminal activity) of the participants and/or researcher.
🟥	Could result in the participant learning about a genetic possibility of developing an untreatable disease.
🟥	Could be hazardous to the economic well-being (e.g. possibly results in the imposition of direct and/or indirect financial commitments on participants) and/or result in discomfort associated with the economic well-being of the participants and/or researcher.
🟥	Collects any articles/documents of property, personal or cultural from participants.
🟥	May result in a traumatic experience for the participants and/or researcher.
🟥	May result in the disclosure of sensitive and/or embarrassing information about the participants and/or researcher.
🟥	Involves covert observation of behaviour that is not normally in the public domain.
🟥	Could result in the participants feeling humiliated, manipulated and/or in other ways treated disrespectfully and/or unjustly.
🟥	Could result in discomfort associated to the physical health (e.g. the act of measuring blood pressure, minor side effects of taking medication) of the participants and/or researcher.
🟥	Could result in discomfort associated with the psychological well-being (e.g. feelings of anxiety due to being interviewed) of the participants and/or researcher.
🟥	Could result in the identification and/or re-identification of a participant from a resulting report.
🟥	Could result in risks to non-participants (e.g. distress to relatives upon discovering that a participant suffers from a serious genetic disorder, infectious disease risks to a community, social/economic discrimination of subgroup populations).
🟨	Is expected to result in the only foreseeable discomfort being that of inconvenience (e.g. time and effort required by participants to complete questionnaire/form, participate in a street survey).
🟩 X	Is expected to result in no foreseeable risk, harm or discomfort to the mental and/or physical well-being of the participants.

4.	**Are you administering a questionnaire / survey / interview / focus group that**
🟥	Collects sensitive data from the participants (e.g. personal data that is not normally in the public domain).
🟥	Does not guarantee the anonymity of the participant.
🟥	Does not guarantee the confidentiality of data collected from the participants.
🟩 X	None of the above.

5.	**Are you intending to access participant data from an existing stored repository (e.g. school, institutional or university records) that**
🟥	Requires access to participant information (in individually identifiable or re-identifiable form) as part of an existing published or unpublished source or database?
🟨	Requires access to participant information (in non-identifiable form, e.g. summarised form) as part of an existing published or unpublished source or database?
🟩 X	None of the above.

6.	**Do you intend publishing the findings of your study in a publication that**
🟨	Requires evidence of human ethics approval/acknowledgement?
🟩 X	Requires no evidence of human ethics approval/acknowledgement?



NELSON MANDELA
UNIVERSITY

7. Is this study	
🟥	An international/cross border study?
X	A local (e.g. regional, national) study?

Your proposed study's risk is summarised below:

No risk	No approval is necessary X
Negligible to Low risk	Faculty level ethics approval is necessary
Medium to High risk	Institutional level ethics approval is necessary

Principle Investigator (PI) Signature **Date 31 August 2020**

Primary Responsible Person (PRP) Signature **Date 31 August 2020**

Change the World

PO Box 77000, Nelson Mandela University, Port Elizabeth, 6031, South Africa