

# **ICT Readiness for Business Continuity in Local Government**

by

**Ruan Koen**



# **ICT Readiness for Business Continuity in Local Government**

by

**Ruan Koen**

**Dissertation**

submitted in fulfilment  
of the requirements  
for the degree

**Master of Information Technology**

in the

**Faculty of Engineering, the Built Environment and  
Information Technology**

of the

**Nelson Mandela Metropolitan University**

**Supervisor: Prof. Rossouw von Solms**

**Co-supervisor: Prof. Mariana Gerber**

April 2017



# Declaration

I, Ruan Koen, hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and recognized.
- This dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognized educational institute.

A handwritten signature in black ink, appearing to read 'Ruan Koen', with a long horizontal line extending to the right from the end of the signature.

---

Ruan Koen

# Abstract

Information and Communication Technology (ICT) has evolved into a pervasive commodity in modern enterprises. ICT enables enterprises, regardless of sector, to achieve their strategic objectives. Similarly, ICT is regarded as a critical enabler in South African municipalities to reach their objectives and ultimately deliver sustainable services to their communities. This dependence on ICT, therefore, necessitates a resilient ICT environment where minimal disruption to ICT is a primary goal. Unfortunately, as reported by the Auditor-General of South Africa, the majority of South African municipalities are neglecting to address the continuity of their ICT services. Failing to implement adequate ICT continuity controls restrict these municipalities from achieving their strategic goals and, as a result, fulfilling their constitutional mandate of service delivery.

It is, therefore, the objective of this study to devise a method, consisting of a theoretical foundation and a supporting tool-set, to assist municipalities in addressing a real-world ICT continuity problem. This method aims to be scalable and usable within different municipalities, and be simplistic and comprehensible enough to implement. The theoretical foundation will introduce the concept of ICT Readiness for Business Continuity, based on the recommendations of international best practices and standards, for example, the ISO 27031 (2011) standard. Furthermore, by considering various challenges within local government, the tool-set will ultimately help municipalities to help themselves in this regard.

# Acknowledgements

Foremost, I would like to express my sincerest gratitude to my supervisors Prof. Rossouw von Solms and Prof. Mariana Gerber for their continuous support during my Master's study. Their patience, motivation, enthusiasm, and immense knowledge played a major role in the completion of this study. Their guidance helped me throughout the duration of the research process and writing of this dissertation.

Furthermore, a thank you to the following benefactors for their financial assistance:

- The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the NRF.
- The financial assistance of the NMMU Post-Graduate Research Scholarship towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the NMMU.

I would also like to thank my fellow students, friends and the staff within the School of ICT for their support and willingness to lend an ear whenever needed, as well as the vibrant work environment they provided. Lastly, a big thanks to my parents for their support, belief and encouragement that helped me through this study.

# Contents

<b>Declaration</b>	<b>i</b>
<b>Abstract</b>	<b>ii</b>
<b>Acknowledgements</b>	<b>iii</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Background . . . . .	1
1.1.1 The Spheres of Government . . . . .	2
1.1.2 The Continuity of ICT . . . . .	3
1.2 The ICT Continuity Problem in Local Government . . . . .	6
1.3 Thesis Statement . . . . .	8
1.4 Delineation . . . . .	8
1.5 Research Objectives . . . . .	9
1.6 Research Design . . . . .	9
1.7 Layout of Dissertation . . . . .	10
1.8 Conclusion . . . . .	11
<b>2 Continuity in the ICT Environment</b>	<b>12</b>
2.1 Introduction . . . . .	12
2.2 The Continuity Mandate . . . . .	14
2.2.1 The Governance Mandate . . . . .	14
2.2.2 The Risk Mandate . . . . .	15
2.2.3 The Information Security Mandate . . . . .	17
2.3 Business Continuity: From Recovery to Resilience . . . . .	20
2.3.1 Disaster Recovery . . . . .	21
2.3.2 Business Continuity . . . . .	22



2.3.3	Aligning Business Continuity and ICT Recovery . . . . .	24
2.4	ICT Readiness for Business Continuity . . . . .	26
2.4.1	The Fundamentals of IRBC . . . . .	27
2.4.2	Components within the IRBC Life-cycle . . . . .	31
2.5	Conclusion . . . . .	37
<b>3</b>	<b>Towards IRBC in Local Government</b>	<b>39</b>
3.1	Introduction . . . . .	39
3.2	The State of ICT Continuity in Local Government . . . . .	40
3.3	Governing ICT in Local Government . . . . .	42
3.4	ICT Readiness for Business Continuity in Local Government .	47
3.4.1	Challenges within Local Government . . . . .	47
3.4.2	Criteria for IRBC in Local Government . . . . .	49
3.5	Conclusion . . . . .	51
<b>4</b>	<b>Research Design</b>	<b>52</b>
4.1	Introduction . . . . .	52
4.2	Research Paradigm . . . . .	53
4.3	Research Process . . . . .	55
4.4	Contextualisation of Research Process . . . . .	58
4.4.1	Phase One . . . . .	58
4.4.2	Phase Two . . . . .	60
4.4.3	Phase Three . . . . .	61
4.4.4	Phase Four . . . . .	62
4.5	Research Methods . . . . .	63
4.6	Conclusion . . . . .	64
<b>5</b>	<b>A Method towards IRBC in LG</b>	<b>66</b>
5.1	Introduction . . . . .	66
5.1.1	Chapter Objective and Consolidation . . . . .	67
5.2	Part A: Developing a Method for IRBC in Local Government .	68
5.2.1	Research Phase One . . . . .	68
5.2.2	Research Phase Two . . . . .	71
5.2.3	Research Phase Three . . . . .	73

5.3	Part B: A Method towards IRBC in Local Government . . . . .	79
5.3.1	Theoretical Foundation . . . . .	79
5.3.2	Tool-set for IRBC Planning . . . . .	85
5.4	Conclusion . . . . .	89
<b>6</b>	<b>Artefact Validation</b>	<b>91</b>
6.1	Introduction . . . . .	91
6.2	Data Collection . . . . .	92
6.3	Data Analysis and Results . . . . .	94
6.3.1	Scalability . . . . .	94
6.3.2	Comprehensibility . . . . .	95
6.3.3	Simplicity . . . . .	96
6.3.4	Usability . . . . .	97
6.4	Findings . . . . .	99
6.5	Conclusion . . . . .	100
<b>7</b>	<b>Conclusion</b>	<b>102</b>
7.1	Introduction . . . . .	102
7.2	Summary of Findings . . . . .	103
7.3	Accomplishment of Objectives . . . . .	104
7.4	Summary of Contributions . . . . .	106
7.4.1	Research Contribution as an Artefact . . . . .	106
7.4.2	Methodological Contribution . . . . .	108
7.4.3	Academic Publications . . . . .	109
7.5	Future Research . . . . .	110
7.6	Epilogue . . . . .	110
	<b>References</b>	<b>111</b>
<b>A</b>	<b>Academic Publications</b>	<b>117</b>
A.1	IST-Africa 2015 . . . . .	117
A.2	IST-Africa 2016 . . . . .	128
A.3	Journal of Public Administration (Submitted) . . . . .	140

<b>B</b>	<b>Questionnaires</b>	<b>161</b>
B.1	Semi-structured Interview Topics/Questions . . . . .	161
B.2	Validation Workshop Questionnaire . . . . .	163
<b>C</b>	<b>M-IRBC Tool-set</b>	<b>166</b>
C.1	IRBC Policy Exercise . . . . .	167
C.2	IRBC Policy . . . . .	170
C.3	Application Impact Analysis . . . . .	178
C.4	IRBC Strategy Exercise . . . . .	180
C.5	Reference Guide . . . . .	183

# List of Tables

2.1	Risk Treatment Methods with Examples from ISO/IEC 27005	17
2.2	The Plan-Do-Check-Act Approach . . . . .	28
2.3	The Elements of IRBC . . . . .	30
2.4	Example Selection of IRBC Strategy Options . . . . .	35
3.1	CGICTPF versus MCGICTP - Phase 1 Comparison . . . . .	46
3.2	Criteria for an approach towards IRBC in Local Government .	50
4.1	The Principles of Design-oriented IS Research . . . . .	54
4.2	Design-based Research: Elements in Phases . . . . .	57
4.3	Contextualised Research Phase 1 . . . . .	59
4.4	Contextualised Research Phase 2 . . . . .	60
4.5	Contextualised Research Phase 3 . . . . .	61
4.6	Contextualised Research Phase 4 . . . . .	62
4.7	Definition of Research Methods . . . . .	64
5.1	Elements of Research Phase 1 . . . . .	69
5.2	Elements of Research Phase 2 . . . . .	71
5.3	Elements of Research Phase 2 . . . . .	74
6.1	Questionnaire Design . . . . .	93

# List of Figures

1.1	Composition of South African Government . . . . .	2
2.1	Relationship Between Continuity and Various ICT Management Disciplines . . . . .	19
2.2	Relationship between Business Continuity and ICT within a Resilient Enterprise . . . . .	24
2.3	Relationship Between ICT Continuity and BCM . . . . .	25
2.4	IRBC Principles on a Typical ICT Disaster Recovery Time Line	29
2.5	Components of IRBC . . . . .	31
3.1	AGSA Audit Outcomes for Municipal ICT Continuity . . . . .	42
3.2	Timeline of Government ICT Initiatives . . . . .	43
4.1	Design-oriented IS Research - Iterative Phases . . . . .	55
4.2	Design-based Research Process . . . . .	56
4.3	Integrated Research Process . . . . .	58
5.1	Phases Towards Finalising the Method: Phase 1 - 3 . . . . .	68
5.2	Theoretical Foundation for Initial Draft Method . . . . .	73
5.3	Theoretical Foundation - First Revision . . . . .	76
5.4	Final Theoretical Foundation . . . . .	80
5.5	Tool-set for IRBC Planning . . . . .	86
5.6	IRBC Policy Tool: Exercise . . . . .	87
5.7	IRBC Policy Tool: Omissions Worksheet . . . . .	87
5.8	Application Impact Analysis Tool . . . . .	88
5.9	IRBC Strategy Exercise . . . . .	89
6.1	Phases Towards Finalising the Method: Phase 4 . . . . .	91
6.2	Example of Questionnaire Answer Scale . . . . .	94

6.3	Results for the Criterion: Scalable . . . . .	95
6.4	Results for the Criterion: Comprehensible . . . . .	96
6.5	Results for the Criterion: Simplistic . . . . .	97
6.6	Results for the Criterion: Usable . . . . .	98
6.7	M-IRBC's Overall Adherence to Criteria . . . . .	100
7.1	Summary of M-IRBC Components . . . . .	106

# Chapter 1

## INTRODUCTION

*The objective of this chapter is to introduce the research study. In doing so, the composition of the South African government is discussed to position the study, followed by an overview of the Information and Communication Technology (ICT) continuity landscape. This leads to an exploration of ICT continuity efforts within the South African local government. Finally, the problem statement and research objectives are defined which guide the rest of the study within a certain research process.*

### 1.1 Background

ICT has developed into a pervasive commodity within all sectors of business, both locally and throughout the world (IoDSA, n.d.). As Coertze and von Solms (2012) state, ICT is essential in managing the information and knowledge required for the daily operation of organisations and thereby significantly contributes to their success. ICT is, therefore, a major driver for enterprises within these sectors to achieve their strategic objectives.

It is fair to argue that the availability of these ICT systems is critical and contributes greatly to the strategic importance of ICT in general. This is not only applicable to enterprises, but holds true in government as well, especially in the South African local government where ICT has become a critical enabler for service delivery (Auditor-General of South Africa, 2014). This section will therefore briefly discuss the composition of the South African government, followed by an overview of the ICT continuity landscape.

### 1.1.1 The Spheres of Government

According to Cameron (2001), South Africa has one of the most advanced government systems in the world. In order to move away from a hierarchical intergovernmental system, the Constitution of South Africa, drafted in 1996, introduced a three-sphere system. Chapter 3 of the Constitution introduces the sphere system, which promotes a co-operative government. In South Africa, government constitutes national, provincial and local spheres of government, which are distinctive, interdependent and interrelated (Constitution of South Africa, 1996). This allows each sphere of government to function on its own and also be dependent on each other in working towards the greater goal of a prosperous South Africa.

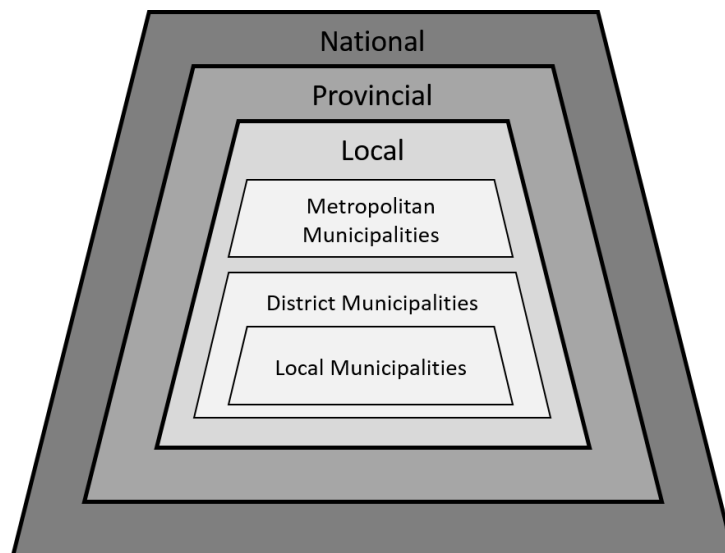


Figure 1.1: Composition of South African Government

The Constitution of South Africa (1996) states that local government consists of municipalities that must be established throughout the country. Each municipality has the right to govern, on its own initiative, the local government affairs of its community and is subject to conformance to national and provincial legislation (Constitution of South Africa, 1996). Three categories of local government exist as defined by the Constitution of South Africa (1996).

The first category namely, Category A, consists of metropolitan municipalities. Category A municipalities have exclusive municipal and legislative



authority in their area. The second category namely, Category B, includes local municipalities and these share executive and legislative authority with a Category C municipality. Lastly, Category C municipalities, known as district municipalities, have executive and legislative authority in an area that includes more than one local municipality. These relationships are illustrated in Figure 1.1.

Within each of these categories of municipalities, the municipal council has the executive and legislative authority of the municipality and national or provincial government may not compromise a municipality's ability or right to exercise its powers or perform its functions (Constitution of South Africa, 1996). Municipalities have several objectives, which include amongst others, to promote a safe and healthy environment and to ensure the provision of services to communities in a sustainable manner (Constitution of South Africa, 1996). Different functions within municipalities contribute to the achievement of these objectives. ICT enables all categories of municipalities within local government to achieve their objectives and to fulfil their duties. It is therefore crucial for these systems to be able to continue during any disruption.

### 1.1.2 The Continuity of ICT

If ICT were to become unavailable within the modern enterprise for extended periods, it might cause irreparable consequences. Herbane, Elliott, and Swartz (2004) state that the effects on the reputation of the enterprise might outlast the direct effects of the actual disruption, should the enterprise fail to recover ICT quickly or effectively. Consequently, efforts towards continuity have seen a shift from recovery to resilience.

The progression from ICT recovery to ICT resilience has not only evolved due to the innovation of new technologies, but because of its strategic business importance. As Herbane et al. (2004) stated, enterprises have not only recognised the need for an approach towards continuity beyond mere ICT disaster recovery but have linked business continuity management to strategically important dimensions of their operations. There is, however, still some confusion about the differences between disaster recovery and business continuity where these terms are used interchangeably, whilst a clear difference in function exists (Stanton, 2005).

The focus of disaster recovery is two-fold. Firstly, the notion of recovery, which indicates a post-incident response approach and secondly, a focus on ICT instead of the business as a whole. This aspect is clear from the fact that disaster recovery is defined as the recovery and resumption of critical technology assets in the event of a disaster and may include resuming individual systems or all critical aspects of the ICT environment (Protiviti Inc, 2013). The question in the modern enterprise is, what happens to business whilst ICT is recovering? Disaster recovery does have a role to play, but the limitations of such an approach have been called into question (Herbane, 2010).

Over the years, following numerous incidents and disasters, it has become apparent that an enterprise-wide approach was needed; ultimately taking precedence over ICT focused disaster recovery (Herbane, 2010). This enterprise-wide approach was needed to ensure that business continued as normal following an incident or disaster. The result was business continuity, defined as the capability of an enterprise to continue with the delivery of products or services at acceptable predefined levels following some disruptive incident (ISO 22301, 2012).

Disaster recovery would still play a major role as part of business continuity, however, the focus on continuity rather than recovery enabled a shift towards resilience. Resilience focus on the prevention of disruption to business. As part of a management system, business continuity management considers functionality and processes as core to proper enterprise-wide availability (Jackson, 2002). In essence, business continuity management could be described as the activity taking place before an incident, whilst disaster recovery happens afterwards (Stanton, 2005).

It is important, however, that the emergence of business continuity do not devalue the important role of ICT. Aligning ICT disaster recovery to business continuity is not a simple task, mainly because of the difference in focus. Disaster recovery plans are reactive in nature; whereas business continuity is rather proactive, focussing on the resilience of the business as a whole, in order to withstand any possible future disasters (Hamidovic, 2011). To address this misalignment, the BS 25777 British Standard was published, with the objective of aligning ICT continuity within the framework of business continuity (Hamidovic, 2011).

The BS 25777 standard helps the user to gain a thorough understanding of the ICT requirements for business continuity (BSI, 2008). Hamidovic (2011) states that the shift towards ICT continuity, supporting business continuity management, has allowed ICT services to be resilient and to be able to recover to predetermined time frames, as required by top management. The effectiveness of this approach has resulted in the international adoption and the ultimate replacement of the BS 25777 British Standard, by the ISO/IEC 27031 international standard (BSI, 2008).

The ISO/IEC 27031 (2011) standard, which is similar to the BS 25777 British Standard, has introduced the concept of ICT Readiness for Business Continuity (IRBC), thereby effectively moving away from the ICT continuity terminology. The content and goals of both standards do, however, remain largely similar.

As the name suggests, IRBC involves preparing the ICT environment to be ready and aligned to business continuity management and its objectives. IRBC is officially defined as: “The capability of an organisation to support its business operations by prevention, detection and response to disruption and recovery of ICT services” (ISO/IEC 27031, 2011). This involves implementing strategies that would reduce the risk of disruption, as well as respond to and recover from disruption to ICT services (Marbais, 2012). The ISO/IEC 27031 standard centres around five key principles, namely: incident prevention; incident detection; response; recovery; and improvement (ISO/IEC 27031, 2011). These principles form the essence of what IRBC strives to achieve and what an enterprise would get from adopting IRBC. Thus, as a modern approach to ICT continuity, IRBC should enable an ICT environment that is more resilient and able to recover effectively.

The ISO/IEC 27031 (2011) states that, the standard for IRBC applies to any enterprise irrespective of size, whether private, governmental, or non-governmental. ICT is core to any government in achieving its objectives and ultimately their service delivery efforts. Therefore, it is equally critical for governmental ICT systems to be resilient. The following section will ascertain the extent to which local government in South Africa has progressed towards resilient ICT systems.

## 1.2 The ICT Continuity Problem in Local Government

ICT is a critical enabler within all spheres of government. It is therefore important that it functions effectively. To this end, the Auditor-General of South Africa (AGSA) conducts annual audits of municipalities, amongst others. The AGSA identified ICT as a key risk area in municipalities. The AGSA reiterates that ICT, if used properly, ensures the confidentiality, integrity and availability of state information, enables service delivery and promotes national security (Auditor-General of South Africa, 2014). Four major shortcomings regarding municipal ICT are highlighted in the two latest AGSA Audit Reports, namely: ICT governance, security management, user access management and ICT continuity (Auditor-General of South Africa, 2014, 2015).

The AGSA explains that ICT continuity enables municipalities to recover critical business operations and application systems that would be affected by disasters or major system disruptions within reasonable time frames (Auditor-General of South Africa, 2014). Proper ICT continuity should enable a municipality to be resilient and able to recover systems within predetermined time frames. However, during the 2012-13 audit, the AGSA found that merely 30% of the municipalities had ICT continuity controls that were embedded and functioning, whilst 62% continued to experience challenges with design and a further 8% experienced challenges with implementation (Auditor-General of South Africa, 2014).

Some of the most common findings by the AGSA included, firstly, that most municipalities experienced challenges with the design and implementation of appropriate ICT continuity and recovery plans (Auditor-General of South Africa, 2014). The finding that 62% of municipalities had not designed their ICT continuity, which is an alarming figure, supports this contention. Secondly, the AGSA found that the management of backups remained a challenge, as most of the municipalities did not test their backups to ensure that they could be restored when required (Auditor-General of South Africa, 2014). Furthermore, these backups were also not necessarily stored at secure off-site facilities, to ensure that they could easily be retrieved during a disaster event.

The 2013-14 AGSA Audit Report did not indicate any significant improvement. ICT continuity is again emphasised as a major shortcoming in municipalities. When comparing the results from this audit to that of the previous audit, the findings on ICT continuity is somewhat alarming. Generally, little improvement has taken place since the previous audit. The amount of municipalities that have embedded and functioning continuity controls have declined from 30% to 26%. The only positive result involves municipalities that have already designed their ICT continuity controls, and these increased from 8% to 19%. Nonetheless, the 2013-14 Report still indicates that 55% of municipalities are yet to design their ICT continuity controls (Auditor-General of South Africa, 2015).

From the above, it is clear that ICT continuity is generally not addressed properly in most South African municipalities. This is a concerning situation, because municipalities are mandated by the Constitution of South Africa (1996) to deliver sustainable services to its communities and ICT is core to this undertaking. Municipalities should therefore, have the necessary ICT continuity controls in place to enable the availability of critical ICT systems during any disruption.

The situation discussed above emphasises a lack of ICT continuity controls in municipalities. The AGSA has continuously emphasised this problem within the audit reports. The lack of appropriate ICT continuity hinders municipalities in delivering services to its communities, especially during times of disruption to these systems.

The problem statement for this study is therefore:

*Local government - as mandated by the constitution is obligated to deliver sustainable services to the community. Most of these services are reliant on ICT systems to a certain extent. However, within local government, there exists a lack of adequate controls to facilitate a resilient ICT environment within the continuity domain.*

### 1.3 Thesis Statement

Based on the problem situation identified around ICT continuity in local government, it is clear that an approach is needed to assist municipalities within local government with their ICT continuity efforts.

The underlying thesis statement of this study is therefore:

*ICT is a critical enabler for service delivery within local government and requires prioritised ICT readiness controls to ensure resilience, consequently enabling the effective management of local government affairs to cater to the needs of the community.*

### 1.4 Delineation

The focus of this study is vested in the South African local government. Although local government consists of metropolitan, district and local municipalities, this study focusses on assisting primarily district and local municipalities with their ICT continuity. This is mainly due to a lack of financial and human resource capacity within these particular categories of municipalities that hinder their efforts towards ICT continuity design and implementation.

However, this does not mean that the contribution will be inappropriate within metropolitan municipalities, or any of the other spheres of government. It does, however, mean that the contribution will be designed with specifically district and local municipalities and their unique challenges, in mind. The use of international standards further allows for the contribution to be extrapolated outside the borders of South Africa.

Furthermore, the problem situation identified in this study is based on the 2012-13 and 2013-14 AGSA Audit Reports, which at the time were the latest audit reports released by the AGSA. The AGSA has subsequently released the new 2014-15 Audit Report in June 2016. These results were not taken into account for this study, primarily due to the study reaching its final stages at the time.

## 1.5 Research Objectives

*The primary objective of this dissertation is to construct a method towards IRBC, consisting of a theoretical foundation and a supporting tool-set, towards assisting the development and implementation of ICT Readiness for Business Continuity in local government. This method should be applicable to the unique municipal ICT environment.*

In order to achieve this objective, the following secondary objectives should be addressed.

- *To explore the modern ICT and business continuity landscape to identify different concepts and their inter-relationships and through standards and best practices, extrapolate relevant continuity approaches to fit the requirement in local government*
- *To determine the primary challenges and factors contributing to the lack of implemented ICT continuity controls in local government*
- *To articulate a holistic approach whereby municipalities can design, implement and manage effective ICT Readiness for Business Continuity*

This study addresses a real-world problem regarding ICT continuity within the South African local government. The objectives stated above will aim to address this problem situation.

## 1.6 Research Design

As discussed earlier, the AGSA has found that many municipalities in South Africa are experiencing challenges with designing and implementing ICT continuity. A real-world problem therefore exists and it needs to be addressed. To address this real-world problem, this study will compose an artefact. This artefact will be in the form of a method towards IRBC. Therefore, design-oriented Information Systems (IS) research was selected as the logical

research paradigm. An extensive and detailed discussion on design-oriented IS research, the research process and methods followed, will be espoused in Chapter 4.

## 1.7 Layout of Dissertation

This chapter introduced the problem and subsequent objectives to address the problem. It provided background on ICT continuity and the composition of the South African government, where this study finds its focus.

In order to explore the modern day ICT and business continuity landscape, Chapter 2 explores various related concepts and their inter-relationships. It further examines IRBC as a relatively unknown approach to ICT continuity.

Although many standards, best practices, and government frameworks provide local government with guidance on how to approach ICT continuity, many still encounter challenges. Chapter 3, therefore discusses the AGSA findings in more detail, but further, examines some of the challenges municipalities face that might hinder proper ICT continuity implementation. Based on these challenges, criteria is defined which will guide the ultimate development of a method towards IRBC in local government.

An in-depth explanation of the research design and further insight into the research paradigm and how the research process from different paradigms were integrated, is provided in Chapter 4. The requirements of the research process, in the form of elements, are further contextualised in Chapter 4.

Chapter 5 provides insight into how the integrated research process materialised. This provides a good understanding of how the complete method towards IRBC, as the primary objective of this study, was developed. This proposed method is presented within Chapter 5.

As part of the requirements of the research paradigm, the method has to be validated. For this purpose Chapter 6 reports on the validation of the method, in the form of a workshop with municipal representatives and presents the findings from a survey in the form of a questionnaire. The dissertation is concluded in Chapter 7, providing a summary of the findings and discussing how the study adhered to the design-oriented IS research paradigm principles.



Attached to the dissertation are various appendices. Appendix A, includes three academic research papers that stemmed from study. The first two are conference papers and were presented at international conferences (IST-Africa). The third paper was submitted to the Journal of Public Administration and feedback is still pending.

Appendix B includes the various questionnaires used during this study for the purpose of information gathering and artefact validation. Lastly, Appendix C includes various outputs from the proposed method. This includes a draft IRBC policy and various excerpts from the supporting tool-set. This dissertation together with the appendices completes the contribution of this study.

## 1.8 Conclusion

This chapter introduced this research study. Firstly, it provided some background on the research area, including ICT continuity and South African government. The problem situation was defined and subsequent objectives to address this problem were outlined. Accordingly, this study aims to construct a method to assist with ICT continuity in local government. The research process was briefly mentioned, before outlining the dissertation to follow.

# Chapter 2

## Continuity in the ICT Environment

*The aim of this chapter is to discuss the importance of ICT within modern enterprises, leading to a focus on the ability of ICT to support the business by enabling it to continue during disruption. It discusses the relationship between continuity and various ICT management disciplines. This is followed by an exploration of business continuity, which is reliant on ICT continuity. A brief history of ICT recovery and the advancement towards complete business continuity is discussed. This sets the foundation for an exploration into ICT Readiness for Business Continuity.*

### 2.1 Introduction

ICT has long been acknowledged as a powerful tool to help achieve important enterprise objectives (IT Governance Institute, 2008). ICT has become so prevalent within modern enterprises that some authors, like Carr (2003), believe that ICT has become a mere commodity. Regardless of one's opinion regarding this view, the role of ICT as a critical resource for the success of any enterprise is undeniable (Carr, 2003; Evans, 2003). Coertze and von Solms (2012) agree that ICT significantly contributes to the success of any enterprise by managing the information and knowledge required for its daily operation. ICT's strategic significance to any enterprise is therefore beyond doubt.

ICT serves many purposes within the modern enterprise, but arguably its most critical function is the storage, transmission and processing of important enterprise information. Globally, regardless of the size or type of enterprise, information is regarded as a critical strategic asset (IT Governance Institute, 2008). This notion is further emphasised by the fact that information assets can account for more than 50% of capital expenditure in many modern enterprises (Nolan & McFarlan, 2005). Therefore, the importance of ICT and the information transgressing these systems, are vital to the well-being of enterprises today.

The progression towards an ICT-centred enterprise has not only emphasised the importance of protecting the information traversing these systems but critically, the importance of ensuring the availability of the information and the systems it resides on. Any loss of information, or disruption to ICT and the information it holds, can have disastrous effects on the enterprise (Stanton, 2005). Herbane et al. (2004) state that, the effects on the reputation of the enterprise may outlast the direct effects of the actual crisis, if they are unable to recover ICT quickly or effectively. It is therefore critical for enterprises to take the necessary steps towards achieving some type of process to ensure that their ICT systems are resilient and able to recover to a predetermined state, consequently enabling the enterprise to continue with its normal operations with as little inconvenience as possible.

This chapter will explore the continuity of ICT in the modern enterprise and outline a standards-based approach to achieving a resilient ICT environment. Firstly, it will discuss the relationship between continuity and other management disciplines within enterprise ICT. This is followed by an overview of business continuity, which depends on proper ICT continuity, and particularly focusses on how it has evolved into the more resilience-focussed business continuity effort of the modern age. Lastly, this chapter will detail a more contemporary approach for a resilient ICT environment that supports the business continuity efforts of the enterprise, whereupon the chapter will be concluded.

## 2.2 The Continuity Mandate

The irrefutable importance of ICT in this information age means that it no longer serves as a mere technical instrument with a single function. ICT has evolved into a core business function and amalgamates many management disciplines to ensure that it operates effectively. These ICT management disciplines, which include amongst others - governance, risk management and information security management, strive towards an ICT environment which achieves its objectives and ultimately benefits the enterprise. These different disciplines within the enterprise ICT environment function interdependently. Therefore, the process of ensuring available ICT systems, will to a large extent rely on and interact with various ICT disciplines. This section will discuss some of these ICT disciplines and emphasise their relationship with continuity.

### 2.2.1 The Governance Mandate

Corporate governance is defined as the system by which enterprises are directed and controlled. ICT, as an enabler in any enterprise, requires proper governance to achieve its objectives. Consequently, corporate governance of ICT is defined as the system by which the current and future use of ICT is directed and controlled (ISO/IEC 38500, 2008). ISO/IEC 38500 (2008) further explains that the corporate governance of ICT involves evaluating and directing the use of ICT to support the organisation and monitoring this use to achieve plans; it essentially includes the strategy and policies for using ICT within an organisation. Corporate governance of ICT can, therefore, be seen as the foundation of the enterprise ICT environment and subsequently ensures that the other management disciplines within ICT, function according to set policies aligned to business objectives.

In South Africa, the Institute of Directors for Southern Africa (IoDSA) established a committee to specifically address corporate governance. The first report by the committee, known as King I, was recognised internationally when published, as the most comprehensive publication on the subject, embracing the inclusive approach to corporate governance (IoDSA, n.d.). The most recent report, namely King III (IoDSA, 2009), came into effect in March of 2010, and it falls in line with the South African Companies Act

no. 71 of 2008 (IoDSA, n.d.). King III, in contrast to previous revisions, applies to all entities regardless of the form of incorporation and establishment (PriceWaterhouseCoopers, n.d.). In essence, King III is thus applicable to private and public entities regardless of size or type of incorporation.

King III consists of several principles on good corporate governance. Chapter 5 of King III includes seven principles for proper governance of ICT. One of these principles applies to business continuity. Principle six states that the board should ensure that information assets are managed effectively (IoDSA, 2009). Within principle six, it is stated that the board is responsible for establishing a business continuity programme addressing the enterprise information and recovery requirements and ensuring that the programme is aligned with the successful execution of the enterprise business activities (IoDSA, 2009). Principle six also makes reference to the Confidentiality, Integrity, and Availability (CIA) of information, where ensuring the availability of information and information systems in a timely manner, is emphasised (IoDSA, 2009). Business and related ICT continuity, are therefore regarded as critical components of good governance and contribute to the success of the ICT environment and subsequently, the success of the enterprise.

Effective corporate governance of ICT ensures that the ICT environment aligns to the objectives of the enterprise and that ICT can deliver value (Posthumus, von Solms, & King, 2010). As emphasised in the King III Report, business continuity is a core component of proper corporate governance of ICT, and boards cannot shy away from it. It is, therefore, clear that business continuity and all its underlying processes should be governed effectively and receive adequate support from senior management. Essential to proper corporate governance of ICT is understanding and managing the risks to enterprise ICT. The following section will elaborate on this issue.

### **2.2.2 The Risk Mandate**

According to NIST SP800–30 (2002), a risk is the net negative impact of a vulnerability, considering both the probability and the impact of occurrence. The ISO/IEC 27005 (2011) standard refers to information security risk as the likelihood that a threat will exploit vulnerabilities of an information asset, or group of assets, and cause harm to the enterprise. Therefore, a

risk is essentially the chance of a threat to possibly have a negative impact, through exploiting a vulnerability of an information asset.

All enterprise assets are exposed to some level of risk. It is, therefore, important that these risks are managed effectively. Risk management is defined as the process of identifying, controlling, and mitigating information related risks (NIST SP800–30, 2002). Core to risk management is the activity of risk assessment. Risk assessment is the overall process of risk identification, risk analysis and risk evaluation (ISO 22301, 2012). A risk assessment typically allows for a structured method of getting an overall view of existing risks, the impact they might have on the enterprise and measures to deal with these risks (Saleh, Refai, & Mashour, 2011).

In order to address these risks and put measures in place, the enterprise has to perform some form of risk treatment. Shameli-Sendi, Aghababaei-Barzegar, and Cheriet (2016) outline four methods of risk treatment:

- Risk Acceptance
- Risk Avoidance
- Risk Transfer
- Risk Mitigation

The ISO/IEC 27005 (2011) gives examples of risk treatment. For clarification purposes, each of these examples has been categorised in one of the above-mentioned methods, illustrated in Table 2.1 below.

Within the enterprise ICT environment, different management disciplines will address ICT risks. The King III Report clearly dictates that ICT should form an integral part of the enterprise’s risk management (IoDSA, 2009). With regard to continuity of ICT, a potential risk might include a thunderstorm, causing electricity failure which effectively renders the enterprise ICT systems inoperable, due to improper surge protection in the server room. An event such as this may cause the enterprise great damage. In order to mitigate this risk, the enterprise may implement sound business continuity and recovery controls, to lessen the impact or likelihood of this risk occurring again.

King III also emphasises that management should regularly demonstrate to the board that the enterprise has adequate business resilience arrange-

Table 2.1: Risk Treatment Methods with Examples from ISO/IEC 27005

<b>Method</b>	<b>Example from ISO/IEC 27005</b>
<i>Risk Acceptance</i>	Taking or increasing risk in order to pursue an opportunity
<i>Risk Acceptance</i>	Retaining the risk by informed choice
<i>Risk Avoidance</i>	Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
<i>Risk Transfer</i>	Sharing the risk with another party or parties
<i>Risk Mitigation</i>	Removing the risk source
<i>Risk Mitigation</i>	Changing the likelihood
<i>Risk Mitigation</i>	Changing the consequences (Impact)

ments in place for disaster recovery (IoDSA, 2009). Therefore, it is clear that the role of business and related ICT continuity, is a crucial element in the enterprise's risk treatment endeavours. Risk management identifies, amongst others, various risks to the enterprise. These include risks that may render the enterprise inoperable, especially disruptions to ICT which are critical to enterprise success. Business continuity and the underlying ICT continuity activities are therefore reliant on proper risk management to identify these risks. Thus, risk management requires business continuity as treatment to these risks. Another discipline, closely related to business continuity, which aims to treat risks to the enterprise information, is that of information security.

### 2.2.3 The Information Security Mandate

Information has evolved into the lifeblood of modern enterprises and is core to most business processes, in effect, making it amongst the enterprises' most valuable assets and critical to its success (von Solms & von Solms, 2006). Consequently, due to this importance of information in the enterprise, great significance should be placed on the enterprises' ability to protect it (Whit-

man & Mattord, 2012). Failure to adequately protect enterprise information can have dire consequences on the enterprise.

King III states that the board of the enterprise should ensure information assets are managed effectively (IoDSA, 2009). Information security is defined as the preservation of the CIA of information (ISO/IEC 27000, 2012). Information security is a critical component in the boards' endeavour for proper information management and King III emphasises the need for enterprises to ensure the CIA of their information (IoDSA, 2009). Therefore, it is clear that information security is a critical process within the enterprise ICT environment. The ISO/IEC 27002 (2013) standard specifically addresses information security.

The ISO/IEC 27002 (2013) standard outlines information security controls which enterprises may select from when implementing an information security management system. These controls are essential to the treatment of various risks to enterprise information and the associated information systems. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, enterprise structures, as well as hardware and software functions (ISO/IEC 27002, 2013). Having a suitable set of information security controls implemented ultimately pursues the preservation of the CIA of information. However, Botha and von Solms (2004) state that although ensuring confidentiality and integrity is important, the availability aspect is of greater significance with regard to business continuity.

Stanton (2005) explains that there is still a debate over whether business continuity is part of information security management, or vice versa, and states that both these processes are actually two sides of the same coin, that of protecting the enterprise. One of the controls outlined within clause 17 of the ISO/IEC 27002 standard, is titled "Information security aspects of business continuity management". Within clause 17, the standard defines two security categories, the first being information security continuity and the second being redundancies - referring to the enterprise information systems (ISO/IEC 27002, 2013).

Essentially, the standard does not dictate the requirement of business continuity as part of the information security management system, but rather requires that information security be applied to the enterprise business con-



tinuity management systems. In different terms, the enterprise business continuity management system should ensure the preservation of the CIA of information within its continuity strategies. This might relate to data backup procedures or redundant systems such as hot-sites, which are implemented as part of business continuity but have to adhere to information security requirements.

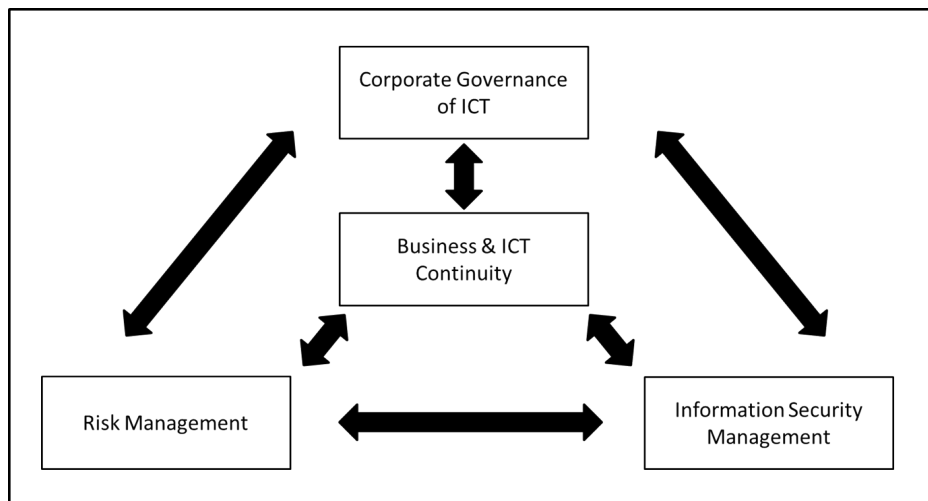


Figure 2.1: Relationship Between Continuity and Various ICT Management Disciplines

Information security and business continuity are therefore very closely related. Business continuity ensures that the availability aspect of information's CIA is preserved, whilst information security controls ensure that the confidentiality and integrity of information residing within backup systems is safeguarded.

This section briefly discusses how different disciplines within the ICT environment relate to and depend on, adequate business continuity systems within the enterprise. The continuity mandate within the enterprise greatly contributes to the success of the enterprise. Consequently, this makes business continuity a senior management mandate. The importance of effective corporate governance of ICT, which includes proper ICT risk management, information security management and business continuity management, is therefore ever more important to enterprise success.

Figure 2.1 illustrates the inter-relationships between these management disciplines. Corporate governance of ICT direct and control the actions re-

quired to address risks to the ICT environment, making it highly dependent upon risk management to identify these risks. The same holds true for information security, which is a governance directed undertaking to act as a treatment to various security risks to the enterprise information, as identified during the risk management process. Business continuity and its related ICT continuity, similarly has to address various potential risks to provide for the continuity of the enterprise and therefore requires sound governance, whilst from an ICT perspective in conjunction with information security enables the safeguarding of the CIA of the enterprise information.

Having discussed the inter-relationships between these different management disciplines, business continuity as a senior management mandate is clear. However, ICT forms a core part of the entire business continuity undertaking and therefore requires further elaboration to fully understand its role within the enterprise, and how business continuity and ICT should align.

## **2.3 Business Continuity: From Recovery to Resilience**

Business continuity and its related activities have become synonymous with daily operations in the majority of modern day enterprises. Reports indicate that 43% of companies struck by severe disasters never re-opened and that nearly 30% failed within two years (Cerullo & Cerullo, 2004). Business continuity is defined as the capability of an enterprise to continue delivery of products or services at acceptable predefined levels following a disruptive incident (ISO 22301, 2012). Herbane et al. (2004) assert that enterprises have not only recognised the need for an approach towards continuity beyond mere ICT disaster recovery, but have linked business continuity management to strategically important dimensions of their operations.

According to Belanger and van Slyke (2012), information serves three primary purposes within enterprises, namely: communication, process support, and decision-making. Information is highly dependent on the ICT systems where it is stored, transmitted and processed. Therefore, the enterprise is highly dependent on its ICT, which again needs proper ICT continuity measures to be available. However, confusion still exists about the differ-

ences between disaster recovery and business continuity, where the terms are sometimes used interchangeably - whilst a clear difference in function exists (Stanton, 2005). This section will explore these and related concepts within continuity and briefly look at the evolution towards business continuity as it is known today, as well as how business requirements and ICT recovery co-exist.

### 2.3.1 Disaster Recovery

ICT has revolutionised the way modern enterprises conduct their daily operations (Nickson, 2015). Modern enterprises are so reliant on ICT that disruption to the systems and the information it holds may cause irreparable damage (Stanton, 2005). It is fair to argue that ICT has drastically advanced within the information age and therefore with the evident changes in technology, the way organisations prepare for the continuity of the ICT systems also had to change.

Herbane (2010) argues that the development of what is known today as business continuity management can most notably be attributed to the technological revolution of the 1970s. Organisations wanted to protect their data processing systems and the focus was very much with the technologies themselves. Herbane (2010) further says that during this infancy period, the focus was very much on standby systems and critical data backups, rather than actions to prevent a failure from occurring. This period presented the advent of what came to be known as disaster recovery planning.

Disaster recovery is defined as the recovery and resumption of critical technology assets in the event of a disaster and may include resuming individual systems or all critical aspects of the ICT environment (Protiviti Inc, 2013; Stanton, 2005). As part of enterprise disaster recovery efforts, Jackson (2002) explains that during its infancy period, identification of critical applications was the order of the day and that these applications could easily be plucked from the production environment and plopped down in some hot site, all for the sake of preventing denial to information assets. The environments where these systems operated were, however, very simple and included standalone applications in a hard-wired, centralised environment (Jackson, 2002). The ICT environment of the modern enterprise, however, has drastically changed over the past decades.

Information is stored in big data warehouses anywhere in the world, accessed through large networks using personal mobile computers. The risks accompanying business interruption has expanded as enterprises are more dependent on ICT and become more linked to external networks (Cerullo & Cerullo, 2004). The majority of enterprise application systems and data facilities can no longer be taken from a centralised environment and mirrored somewhere else to ensure continuity. Therefore, it is undeniable that the progression and change in the ICT systems warranted a change in the way enterprises prepare for the unavailability of these systems.

It becomes evident that the emphasis of disaster recovery is two-fold, the first being on the ICT systems instead of the business as a whole and secondly, that of recovery, implying a post-incident response approach. Having mirrored ICT environments in today's ICT landscape can become extremely costly and very difficult. Therefore, the concern with disaster recovery resides in the lack of continuity of business operations whilst ICT is recovering in the background. Partly due to this issue, the limitations of a computer centre focused disaster recovery planning approach were called into question (Herbane, 2010).

Stanton (2005) makes it clear that having disaster recovery processes in place is not the same as having a full business continuity plan. Downtime to ICT means downtime to normal business operations, something which modern enterprises cannot afford. Therefore, as emphasised by Jackson (2002), there has been a focus shift within the industry, away from computer operations and communications recovery, to one where business functionality and processes are considered the start and end points for proper enterprise-wide availability. This notion will be further considered in the following subsection.

### **2.3.2 Business Continuity**

Herbane (2010) explains that recognition grew throughout major world events, as in the case of terrorist attacks impacting large organisations, that an enterprise-wide approach was needed to take precedence over ICT focused disaster recovery. This recognition would see the realisation of Business Continuity Management (BCM). BCM birthed the industry focus shift, from recovery planning to an enterprise focused approach (Jackson, 2002). How-

ever, BCM does not completely replace disaster recovery. Simply put, BCM could be described as the activity that takes place before an incident occurs, and disaster recovery the process which happens afterwards (Stanton, 2005).

The International Standards Organisation (ISO 22301, 2012) defines BCM in its standard as: *A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.* The main concept within this definition is that of enterprise-wide resilience which holds many benefits if implemented. Sahebjamnia, Torabi, and Mansouri (2015) agree that the concept of organisational resilience is attracting growing attention amongst academics and practitioners.

IBM (2009) defines enterprise resilience as the ability to rapidly adapt and respond to business disruption and maintain continuous business operations. Furthermore, enterprise resilience starts with understanding exactly what one's business needs in order to survive unexpected events and plan ahead for challenges that could come at any time (IBM, 2009). Therefore, in essence, resilience can be seen as the ability of the enterprise to withstand disruption to business operations (ISO/IEC 27031, 2011). BCM aims to achieve this state of resilience, not from an ICT standpoint alone, but from that of the enterprise as a whole.

With enterprise resilience in mind, Herbane et al. (2004) state that BCM has evolved into a process that identifies an enterprise's exposure to internal and external threats and synthesises hard and soft assets to provide effective prevention and recovery. BCM not only deals with incidents when they occur, but it also aims at establishing a culture within organisations that works towards resilience, therefore being able to provide continuity of products and services to customers (Hamidovic, 2011). In essence, BCM has brought about the ability for an enterprise to be prepared for incidents or disaster events alongside its recovery capabilities. It allows not only for the recovery of ICT and information systems, but for the continuance of normal business operations whilst ICT recovers.

This relationship between business continuity and ICT, and how these are contributing to a resilient enterprise is illustrated in Figure 2.2. It is

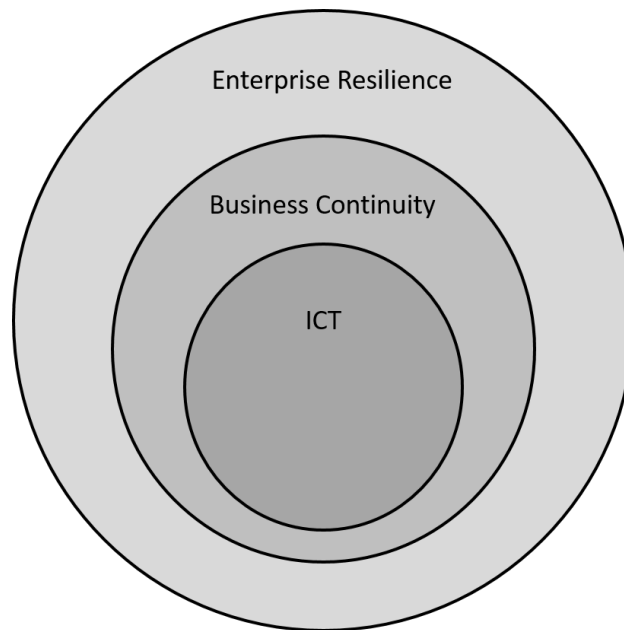


Figure 2.2: Relationship between Business Continuity and ICT within a Resilient Enterprise

evident, starting from a computer-oriented disaster recovery approach during the technological revolution, up until the mature BCM activities seen in modern day enterprises, that there has been a shift from post-incident recovery, to pre-incident enterprise resilience. However, although the focus has shifted from ICT recovery towards enterprise resilience, it is important that the role of ICT within the enterprise's business continuity activities, not be devalued. ICT remains core to the enterprise and ICT continuity is, therefore, core to business continuity and recovery activities. The following subsection will explore how modern day ICT continuity supports the business continuity objectives of the enterprise.

### 2.3.3 Aligning Business Continuity and ICT Recovery

ICT, as detailed before, remains a critical enabler for organisational activities. The shift from disaster recovery to BCM should therefore not disregard the importance of having available ICT systems. Should a misalignment between the enterprise business continuity and its ICT disaster recovery exist, it could have damaging consequences if a disruption were to occur. Aligning the ICT disaster recovery to business continuity is unfortunately not as

simple as one would think, partly due to the difference in focus mentioned by Hamidovic (2011). Many different terms and concepts have been used to describe recovery and continuity activities in the past, but owing to the realisation of its importance, organisations now operate in an age where standardisation has eliminated confusion and promoted world-wide collaboration to enhance business continuity holistically.

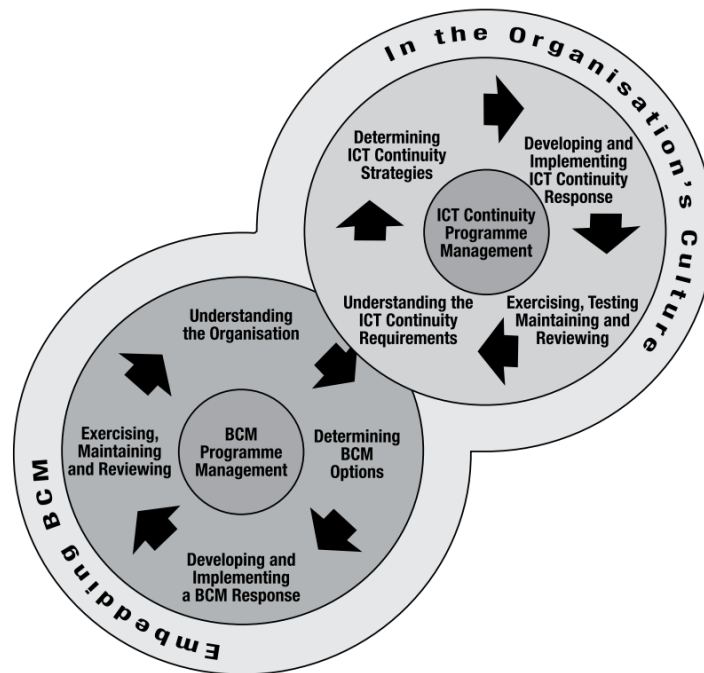


Figure 2.3: Relationship Between ICT Continuity and BCM (British Standards Institute, 2008)

To address this misalignment, the British Standards Institution published the BS 25777 British Standard in 2008 as a code of practice for ICT Continuity Management, to help organisations plan and implement an ICT continuity strategy (Hamidovic, 2011). The aim of this standard was to align ICT continuity within the framework of BCM, which was provided by the BS 25999 British Standard published in 2006 (Hamidovic, 2011). The alignment between ICT continuity management and BCM as outlined in the BS 25777 is illustrated in Figure 2.3, which emphasises the overlap between the two disciplines (British Standards Institute, 2008). The BS 25777 promotes ICT continuity as a holistic management activity and helps the user gain an understanding of the ICT requirements for business continuity (BSI, 2008).

The shift towards ICT continuity, which supports the overall BCM in the organisation, has allowed the required ICT services to be resilient and able to recover to the predetermined time frames as required by senior management (Hamidovic, 2011). The effectiveness of this approach has resulted in its adoption by the International Standards Organisation. The ISO/IEC 27031 (2011) standard, which was published in 2011, officially replaces and supersedes the BS 25777 standard (BSI, 2008). However, the ISO/IEC 27031 standard has introduced the concept of ICT Readiness for Business Continuity (IRBC), thus effectively moving away from the ICT continuity terminology. Much of the content of ICT continuity management, as well as the goal of aligning with BCM, does, however, remain the same in IRBC.

The International Standards Organisation also published an international standard for BCM which replaces and supersedes the BS 25999 standard. The ISO/IEC 22301 standard, published in 2012, defines a management system approach which is also adopted by ISO/IEC 27031 for IRBC. This approach, based on the Plan-Do-Check-Act Model, creates a continual life-cycle for implementing IRBC, starting from a planning phase and continually reviewing IRBC through monitoring and improvement activities. It is this management system which ultimately aligns IRBC and BCM.

ICT is such an important function within the enterprise and as illustrated in Figure 2.2, forms a core part of the enterprise business continuity, towards the objective of enterprise resilience. It is therefore, fair to argue that in order to achieve enterprise resilience, the ICT environment should be equally resilient. IRBC, if implemented effectively alongside business continuity, may result in an ICT environment that is as resilient as the enterprise itself, effectively bridging the gap between ICT and business continuity.

## 2.4 ICT Readiness for Business Continuity

The previous section discussed how enterprises evolved from an ICT data-centre focused recovery approach for incidents towards an enterprise-wide business continuity effort for the enterprise to predict and manage disruption to its business operations. It also looked at aligning these disciplines to promote a resilient enterprise. However, ICT and the all important information traversing, is still core to the majority of enterprises. Therefore, it is



critical that the ICT component of business continuity, be addressed effectively. This section discusses the concept of IRBC.

*“ICT Readiness for Business Continuity is the capability of an organization to support its business operations by prevention, detection and response to disruption and recovery of ICT services”* (ISO/IEC 27031, 2011). IRBC is a relatively unknown concept. Even though the ISO/IEC 27031 (2011) standard has been published for a number of years, the adoption of the standard in enterprises still remains mostly unverifiable (Ogu & Oyerinde, 2014). There is also little to no academic literature on the topic except for brief mentions about its existence and what it strives to achieve. Most of the detail surrounding IRBC therefore stems from the BS 25777 and ISO/IEC 27031 standards. The rest of this section will explore IRBC, as it is delineated in its standard. It should, therefore, be noted that the information regarding IRBC provided in this section, unless cited otherwise, originates from the ISO/IEC 27031 (2011) standard.

### **2.4.1 The Fundamentals of IRBC**

As is the case with most of the documents published by the International Standards Organisation, the ISO/IEC 27031 standard builds IRBC upon a solid foundation. This foundation comprises of (1) A well-defined approach, based on the Plan-Do-Check-Act Model to align itself to the enterprise’s BCM; (2) A set of principles which guide the implementation and functioning of IRBC in the enterprise and acts as an objective which the enterprise should pursue; and lastly (3), A set of elements to address as part of the enterprise IRBC strategy. Understanding these fundamentals and building the enterprise IRBC upon it should result in an effective IRBC programme, aligned to business continuity requirements, but ultimately benefiting the enterprise holistically. The first fundamental is the Plan-Do-Check-Act approach.

#### **Plan-Do-Check-Act**

As mentioned previously, the alignment between BCM as defined in the ISO 22301, and IRBC, is largely due to the Plan-Do-Check-Act Model upon which both these management disciplines builds itself. Through the use of the

Plan-Do-Check-Act approach, IRBC involves the enterprise in establishing processes to develop and enhance its key IRBC elements to improve their capability to respond to any type of disruption, including changing risk situations. The Plan-Do-Check-Act approach is repetitive in nature and allows the IRBC system to adapt to ever changing risk environments through continual monitoring and improvement activities.

Table 2.2: The Plan-Do-Check-Act Approach

<b>Phase</b>	<b>Description</b>
<i>Plan</i>	Establish the necessary policies, objectives and procedure
<i>Do</i>	Implement and operate the policies and procedures
<i>Check</i>	Monitor and review its effectiveness against the stated objectives
<i>Act</i>	Maintain and improve by taking corrective action, based on the review

\* Note: From ISO 22301 (2012)

Each stage of Plan-Do-Check-Act is defined in Table 2.2. The different IRBC components that form part of each stage within the Plan-Do-Check-Act phases will be discussed at a later stage. The cyclic nature of the Plan-Do-Check-Act approach becomes evident when examining the different activities that take place within each phase. Essentially, testing activities within the Act-phase may lead to a need for revision of a certain strategy and initiate Plan-phase activities. The phases of the Plan-Do-Check-Act approach and its incumbent activities emphasise the adoption of the IRBC principles throughout its life-cycle.

### **Principles of IRBC**

IRBC has five key principles, that typify the essence of what IRBC is, and what it aims to achieve. The principles, namely: (1) incident prevention, (2) incident detection, (3) response, (4) Recovery, and (5) improvement, also support and emphasise the aim of the Plan-Do-Check-Act approach.

Principle 1 includes protecting ICT services from threats, such as environmental and hardware failures, operational errors, malicious attacks, and

natural disasters, which are critical to maintaining the desired levels of ICT availability for the enterprise.

Principle 2 caters for detecting incidents at the earliest opportunity to minimise the impact to ICT services, reduce the recovery effort, and ultimately preserve the quality of service.

Principle 3 involves responding to incidents in the most appropriate manner to enable efficient recovery and effectively minimise downtime. Poor reaction to a minor incident may escalate the incident to something more serious.

Principle 4 requires the identification and implementation of the appropriate recovery strategy to ensure timely resumption of ICT services as well as the integrity of data. Recovery priorities also allow the most critical services to be recovered first, so critical business functions can continue, whilst less critical services can be reinstated later.

Principle 5, arguably the most important principle, includes documenting, analysing and reviewing lessons from incidents. Understanding the lessons learned from these incidents allows the enterprise to better prepare, control and avoid incidents and disruption in the future.

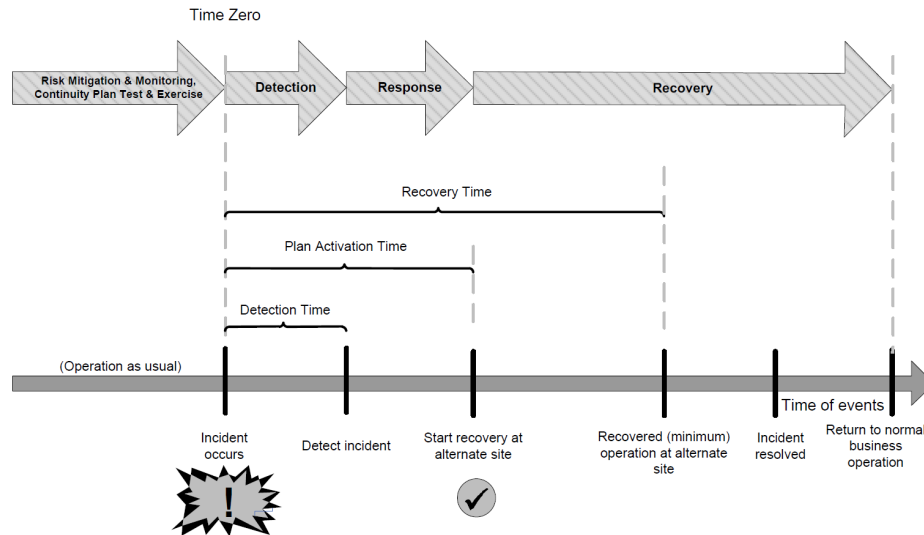


Figure 2.4: IRBC Principles on a Typical ICT Disaster Recovery Time-line (ISO/IEC 27031, 2011)

Figure 2.4 illustrates how the IRBC principles correlate to a typical disaster recovery time line. During operation as usual, the IRBC incident pre-

vention activities take place, where ICT is continually monitored and testing and planned exercises occur. An incident is detected and there is a quick response from the recovery team. The appropriate recovery strategy is invoked and soon after the most critical functions are operating at an alternate site whilst recovery of the primary site is occurring. Upon returning to business as usual when the incident has been resolved, the incident will be well documented and preparation will commence to better respond or avoid similar incidents in the future. The functioning of an effective IRBC system and the principles of IRBC is evident in this example. Proper response and recovery as detailed in the example of Figure 2.4, is dependent on a sound IRBC strategy and how it addresses the different elements of IRBC.

### IRBC Elements

The ISO/IEC 27031 (2011) standard has outlined six elements that are central to IRBC response and recovery activities. These elements, outlined in Table 2.3, each represent a set of aspects within the enterprise ICT environment that need to be considered during response and recovery planning. Each element should be addressed when formulating the enterprise's IRBC strategy, and an appropriate strategy option defined and implemented for that element as part of the IRBC plan.

Table 2.3: The Elements of IRBC

<b>Element</b>	<b>Description</b>
<i>People</i>	The specialists with appropriate skills and knowledge, and competent backup personnel
<i>Facilities</i>	The physical environment in which ICT resources are located
<i>Technology</i>	Hardware, network connectivity, and software
<i>Data</i>	Application data, voice data and other types of data
<i>Processes</i>	Supporting documentation to describe the configuration of ICT resources and enable the effective operation, recovery and maintenance of ICT services
<i>Suppliers</i>	Other components of the end-to-end services where ICT service provision is dependent upon an external service provider or another organisation within the supply chain

\* Note: From ISO/IEC 27031 (2011)

Each element represents different strategy options which, if combined in the IRBC strategy, should cater for the majority of business disruptions and aim to mitigate or appropriately respond to these disruptions. Both the IRBC strategy and plan will be discussed in the following subsection. At this stage, it is only important to list these elements and note that they are fundamental to drafting a proper IRBC strategy.

This subsection explored some of the fundamentals of IRBC and illustrated how IRBC is approached, what IRBC strives to achieve and how key elements form the basis of formulating a proper IRBC strategy. The core components within an IRBC programme will be discussed further and placed within a Plan-Do-Check-Act phase.

### 2.4.2 Components within the IRBC Life-cycle

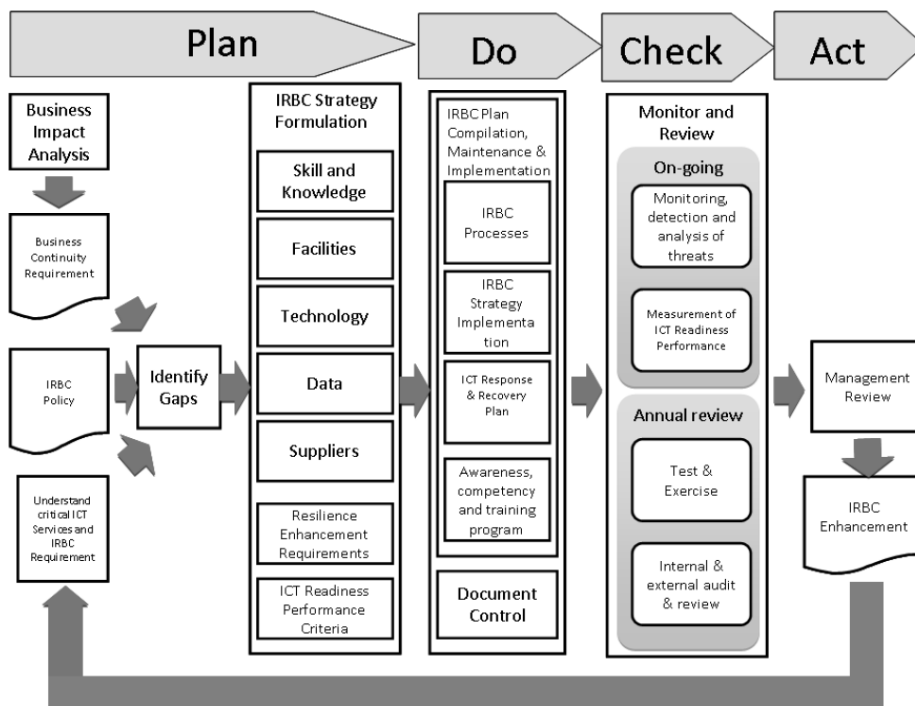


Figure 2.5: Components of IRBC (ISO/IEC 27031, 2011)

The previous subsection mentioned that each phase in the Plan-Do-Check-Act approach for IRBC has different components that need to be addressed for successful implementation. This subsection will discuss the most critical components and place them within a Plan-Do-Check-Act phase. Figure 2.5

illustrates all the components involved within the different stages of IRBC. Some of the most important components include the IRBC policy, business impact analysis, IRBC strategy and the IRBC plan.

### **The IRBC Policy**

To be effective, IRBC must be fully integrated with the enterprise management activities, be endorsed and be promoted by senior management. As with any management activity, the enterprise should have a documented IRBC policy. This policy will be refined and enhanced as the IRBC process matures. The policy should be regularly reviewed and updated in line with enterprise requirements and should be aligned with the wider business continuity objectives. The quantity of resources required to support IRBC will depend upon the size of and complexity of the enterprise and should be defined within the policy. The policy should also provide the enterprise with goals to which it must aspire and against which its IRBC effectiveness can be measured. Essentially, the IRBC policy should:

- Establish and demonstrate commitment of senior management to the IRBC program
- Include or make reference to the enterprise's IRBC objectives
- Define the scope of IRBC - including limitations and exclusions
- Be approved and signed off by senior management
- Be communicated to appropriate internal and external stakeholders
- Identify and provide relevant authorities for the availability of resources such as budget; personnel necessary to perform activities in line with the IRBC policy
- Be reviewed at planned intervals and when significant changes, such as environmental changes, change of an organisation's business and structure, occurs

### **Business Impact Analysis**

A business impact analysis is defined as: *“The process of analysing operational functions and the effect that a disruption might have upon them”* (ISO/IEC 27031, 2011). As part of the enterprise BCM programme, different business functions must be categorised according to their priority for continuity. This categorisation is based on the results of the business impact analysis, and defines a minimum level at which each function needs to be performed upon resumption. This process should very much involve senior management as they are ultimately accountable. Senior management outline the enterprise business continuity requirements and based on these requirements, the Minimum Business Continuity Objective (MBCO) per product or service can be defined.

The MBCO is essentially the minimum tolerable level of ICT services acceptable during or after disruption, in order for the enterprise to achieve its business objectives. The MBCO consists of the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of each product or service. The RTO is defined as the, *“Period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions must be recovered after a disruption has occurred”*; and RPO is defined as the, *“Point in time to which data must be recovered after a disruption has occurred”* (ISO/IEC 27031, 2011). The RTO of a critical business function will be much less, in order to meet the business continuity requirement for that function. In essence, the quicker critical business functions can be resumed, the lesser the impact will be on the enterprise. It is, however, important for senior management to be aware of any gaps between IRBC arrangements and the business continuity requirements of the enterprise.

Senior management should be informed of any gaps between IRBC capability and the business continuity requirements. These gaps might indicate the existence of risks that require additional resilience and recovery resources. These resources might include financing, additional staff or facilities, to name a few. These gaps should be documented and senior management should sign off on the ICT service definitions, the documented list of critical ICT services and the risks associated with gaps identified between IRBC capability and business continuity requirements. This should include, where appropriate, the sign off of identified risks. The options for addressing the gaps and risks

identified should then be explored by determining IRBC strategies.

### **IRBC Strategy**

Essentially, IRBC strategies define the approaches to implement the required controls for resilience so that the five principles of IRBC, mentioned in the previous subsection, can be achieved. The strategies chosen should be capable of supporting the business continuity requirements of the organisation. The enterprise should take into account the implementation and ongoing resource requirements when developing the strategy. External suppliers may be contracted to provide specialist services and skills that play an important role in supporting the strategy. The strategy should take into account internal constraints and factors such as:

- Budget
- Resource availability
- Potential costs and benefits
- Technological constraints
- The enterprise's risk appetite
- The enterprise's existing IRBC strategy
- Regulatory obligations

The different strategy options should take into account the various components required to ensure the continuity and recovery of critical ICT services. The options should consider increasing protection and resilience, as well as provision for recovery and restoration from an unplanned disruption and may include: internal arrangements, services delivered to the organisation and service provided externally by one or more third parties. IRBC may be achieved through many strategy options that address the elements of IRBC, discussed in the previous subsection. Table 2.4 below illustrates examples of strategy options for each of the different IRBC elements.

Each IRBC element has many different strategy options, and the onus is on the enterprise to choose effective strategy options based on its risk appetite and eventual cost of the strategy options. Senior management should



Table 2.4: Example Selection of IRBC Strategy Options

Element	Selected Strategy Option
<i>People</i>	Multi-skill training of ICT staff and contractors to enhance skill redundancy
<i>Facilities</i>	Alternative facilities provided by third-party specialists
<i>Technology</i>	Hot-, Warm-, Cold-standby ICT systems
<i>Data</i>	Appropriate backup and restoration mechanisms to ensure confidentiality and integrity of data
<i>Processes</i>	Clearly documented processes in sufficient detail to enable competent staff to execute them
<i>Suppliers</i>	Dual supply of utilities such as power and telecommunications

be informed should any implemented strategy options be deemed unable to meet business continuity requirements and subsequently be advised on their current capability. The selected strategy options should cater for likely risks and effects of disruption, align with the business continuity strategies and suit the enterprise's overall objectives and risk appetite.

At this stage, the enterprise's senior management has indicated full support of the implementation of IRBC and outlined this commitment within the IRBC policy. Based on the results of a business impact analysis, critical business functions and their supporting ICT systems have been identified. MBCO's have been defined for these business functions. Any gaps between the capability of IRBC and the business continuity requirements have also been identified and communicated to senior management to consider. To enable these business functions to be resilient, an IRBC strategy has been developed. The IRBC strategy defines different strategy options within the six elements of IRBC and the strategy options selected should enable IRBC to achieve the MBCO. These actions have all taken place as part of the Plan-phase. The next crucial component of IRBC is the IRBC Plan which forms part of the Do-phase.

### **IRBC Plan**

The ISO/IEC 27031 (2011) states that, the enterprise should have documentation to manage potential disruptions and consequently enable continuity of

ICT services and recovery of critical business activities. A small enterprise may have a single plan document that outlines all the activities required to recover the ICT services of the entire enterprise. In contrast, a large enterprise may have multiple plan documents, each specifying recovery details of particular components of its ICT services. Regardless of the complexity of the enterprise IRBC plan, it should at a minimum contain certain components.

The purpose and scope of each specific plan should be defined, accepted by senior management and understood by those responsible for invoking the plan. Relationships with other plans or documents should be clearly referenced and methods to obtain said documents, clearly described. Every IRBC plan, whether it is the incident response plan or response and recovery plan, should set out prioritised objectives in terms of, (1) The critical ICT services, (2) MBCO's for these services, (3) recovery levels needed for each service and (4) situations in which the plan will be invoked.

The IRBC plan should define clear roles and responsibilities of people or teams having authority during and following an incident. The procedures for invoking a specific plan should be well documented. This process should allow plans, or parts thereof, to be invoked as quickly as possible, either in advance of an anticipated disruptive event or immediately following the occurrence of a disruption. The IRBC plan should delineate, (1) How to mobilise the assigned individual or team, (2) immediate assembly points, (3) subsequent team meeting locations and any alternate meeting locations and (4) circumstances which the enterprise deem unnecessary for IRBC response, such as minor faults and outages managed by the help-desk.

Management should nominate an owner for the IRBC plan documentation, who should be held accountable for regular review and update of the documentation. This should be employed in conjunction with a version control system, where changes are formally notified to relevant parties through a maintained document distribution record. Lastly, the plan should also contain, where appropriate, essential contact details of all key stakeholders. Apart from these general components, each plan document should contain the detail of the IRBC strategy that will ultimately allow the ICT service to recover and resume back to normal activities.

Taking into account what has been discussed above, IRBC, how it functions and what its objectives are, becomes clear. Essentially, IRBC sets out to achieve a resilient ICT environment, supporting the enterprise business continuity towards a resilient enterprise. Based on Figure 2.2, IRBC, therefore, addresses the ICT component within business continuity, and focuses on attaining pre-incident resilience, through its principles, rather than relying on recovery alone. Therefore, for the enterprise to be resilient against disruption, its ICT environment should be ready to support the wider business continuity process.

## 2.5 Conclusion

This chapter explored continuity in the ICT environment. ICT, and the information it processes, is undeniably critical to the success of modern enterprises. ICT has become so prevalent within enterprises, that without it, most enterprises would fail to reach their objectives and consequently cease to exist. This importance, therefore, brings rise to many risks to enterprise ICT, which might render the ICT inoperable and the information inaccessible. Proper corporate governance of ICT sets out to, amongst others, address these risks by directing and controlling various management disciplines within the ICT environment. These management disciplines subsequently bring about different measures to successfully treat many of these risks. Governance emphasises the need for business continuity, which sets out to implement measures to enable the enterprise to continue business should any risks materialise and lead to enterprise disruption.

Business continuity can only be as effective as the ICT continuity and recovery measures it has in place. In modern enterprises, however, post-incident recovery no longer satisfies the requirements for an available ICT environment. The ICT environment should be as resilient as the enterprise itself. IRBC, within the framework of business continuity, aims towards a resilient ICT environment that ultimately supports a resilient enterprise. This in effect, brings about an enterprise able to withstand a large proportion of risks that might hinder its normal functioning and promotes an enterprise that can continue functioning under the most adverse conditions.

Chapter 3 will focus on local government and investigate the state of ICT continuity within the South African municipalities. It will look at what government has accomplished to address ICT and specifically ICT continuity, within its departments and municipalities. Chapter 3 will then argue towards the need for IRBC within municipalities and explore challenges within them that might hamper effective adoption of IRBC. This will provide the basis for defining criteria, that an IRBC implementation in municipalities should adhere to in order to be successful.

## Chapter 3

# Towards ICT Readiness for Business Continuity in Local Government

*This chapter intends to examine different aspects to consider in working towards ICT Readiness for Business Continuity (IRBC) in local government. Firstly, the state of ICT continuity in municipalities will be explored. Core to this exploration is the findings from the Auditor-General of South Africa (AGSA) on the state of ICT in municipalities. Furthermore, it briefly discusses different government initiatives, including policies and frameworks, which seek to enable corporate governance of ICT within government departments, including municipalities. Finally, this chapter examines some of the challenges behind the unsatisfactory state of municipal ICT and argue towards criteria for successful IRBC in municipalities.*

### 3.1 Introduction

It is evident that ICT plays a vital role within enterprises, regardless of type or incorporation. ICT, including the information traversing it, is core to any enterprise and is subsequently seen as an enabler. This same notion holds true in local government, where ICT functions as an enabler within municipalities to deliver sustainable services to their communities (Auditor-General of South Africa, 2014). The Constitution of South Africa (1996) mandates municipalities to deliver sustainable services to their communities.

It is, therefore, critical for municipalities to have proper ICT systems in place. More importantly, these ICT systems have to be resilient.

Cerullo and Cerullo (2004) explain that the dependence on ICT systems has broadened the potential causes of ICT disruptions and it is, therefore, critical that enterprises quickly respond. Hence, priority should be given to proper ICT continuity practices, promoting resilient and recoverable ICT systems within municipalities. Unfortunately, the AGSA has reported that this is not the case.

These findings will be further explored within this chapter to determine the state of ICT in municipalities, specifically with regard to ICT continuity, which should stress the extent of the problem and the need for IRBC. Chapter 2 introduced IRBC as a more contemporary approach to ICT continuity, which focuses on achieving a more resilient ICT environment. Furthermore, the current attempts by the government to address the corporate governance of ICT within government departments, including municipalities, will be discussed. Finally, this chapter will examine some of the challenges faced by municipalities, which have hindered the implementation of corporate governance of ICT, which affects ICT continuity. The AGSA, as well as most of the government documents, refer to ICT continuity; however, this chapter argues towards criteria for IRBC implementation in municipalities, as opposed to ICT continuity, due to its focus on resilience. The criteria will ultimately be the foundation for an approach towards IRBC, in the form of a method, to address the ICT continuity problem.

## **3.2 The State of ICT Continuity in Local Government**

South Africa, as a young democracy, has mandated within its constitution, the establishment of state institutions to support constitutional democracy. These institutions, known as Chapter nine institutions, are defined within Chapter 9 of the Constitution of South Africa (1996). These institutions function independently and are only subject to the constitution and the law; they are therefore impartial and must exercise their powers and perform their functions without fear, favour or prejudice (Constitution of South

Africa, 1996). Importantly, no person or organ of state may interfere with the functioning of these institutions (Constitution of South Africa, 1996). Thus, these institutions aim to uphold the democracy of South Africa, through their various functions, completely impartial from political or state interference.

The AGSA is one of these Chapter nine institutions. The Constitution of South Africa (1996) states that the AGSA must audit and report on the accounts, financial statements, and financial management - which involves the use of ICT of, amongst others, municipalities and report to the National Assembly at least once a year. Annual audits of municipalities are therefore conducted by the AGSA.

Within its municipal audits, the AGSA has identified six key risk areas. ICT has been outlined as one of these risk areas within municipalities. The AGSA emphasises that municipal ICT should enable the CIA of state information, enable service delivery and promote national security (Auditor-General of South Africa, 2014). The AGSA, therefore, states that it is critical that good ICT governance, effective management and a secure ICT infrastructure be in place (Auditor-General of South Africa, 2014). The AGSA audit of municipalities reports mainly on the assessment of four major areas, namely: ICT governance, user access management, information security and ICT continuity.

ICT continuity is core to municipal ICT. The AGSA states that ICT continuity controls enable municipalities to recover critical business operations and application systems that would be affected by disasters or major system disruptions (Auditor-General of South Africa, 2014). This section examines the AGSA audit outcomes for two of the latest municipal audits, which include the 2012-13 and 2013-14 financial years (Auditor-General of South Africa, 2014, 2015).

The audit outcomes in Figure 3.1 below, illustrates a worrisome situation. Predominantly, the majority of South African municipalities, have not yet designed, nor implemented ICT continuity. In both financial years, more than half of the 278 municipalities have not yet designed ICT continuity controls, being 62% and 55% respectively for the financial years in question. It can be argued that these municipalities are therefore susceptible to disruption and might cease to deliver services to their communities, following some disaster or serious incident disrupting ICT services.

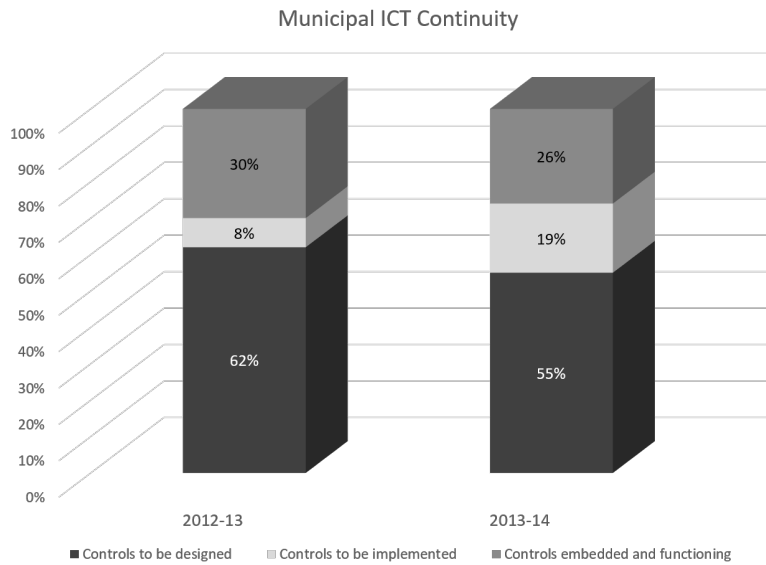


Figure 3.1: AGSA Audit Outcomes for Municipal ICT Continuity. Adapted from Auditor-General of South Africa (2015)

A slight improvement in the amount of municipalities that need to design controls are visible in the 2013-14 audit, indicating that some municipalities have attempted to rectify the situation. Subsequently, slightly more municipalities have entered the implementation stage. However, the concerning finding is that the amount of municipalities that had embedded and functioning ICT continuity controls declined by 4%, to only 26%.

Based on these findings it is clear that the majority of municipalities in South Africa are struggling with ICT continuity implementation and design. Many municipalities have not yet designed any controls and a large portion has failed to maintain embedded and functioning ICT continuity controls. It, therefore, begs to be asked, what government has done to rectify this situation. The following section will briefly examine different government initiatives to address the corporate governance of ICT, which affects ICT continuity within government departments, including local government.

### 3.3 Governing ICT in Local Government

Modern day enterprises cannot deny the strategic importance of ICT. The world-wide introduction of laws, standards and best practices, like the King



Code on Corporate Governance for South Africa (IoDSA, 2009), the American Sarbanes-Oxley Act (Sarbanes-Oxley Act, 2002), as well as the ISO/IEC 38500 standard (ISO/IEC 38500, 2008) to name only a few, ratifies this notion. It would be naïve to think, noting the identified issues of ICT continuity in municipalities, that government in South Africa has not realised the strategic importance of ICT. In fact, this realisation came as early as 1998. The Presidential Review Commission (PRC) Report of 1998 (Presidential Commissioners, 1998) which emphasised the importance of ICT, stated that important ICT decisions should not be delegated to the technologists, but stem from senior political and managerial leadership (Presidential Commissioners, 1998). Since the PRC Report, the government has embarked on various initiatives to address the corporate governance of ICT within government departments. Figure 3.2 illustrates the progression of government initiatives to address ICT, since the release of the PRC Report.

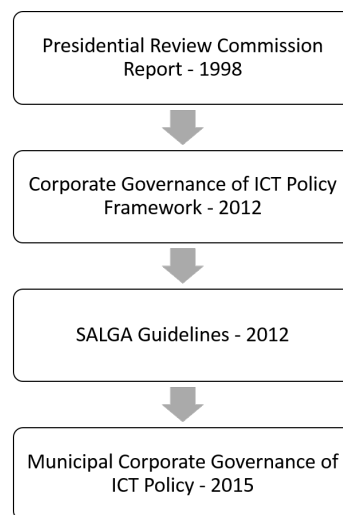


Figure 3.2: Timeline of Government ICT Initiatives

The PRC Report emphasised the need for ICT to be aligned to government business goals (Presidential Commissioners, 1998). Sadly, ten years after the publication of the PRC Report in 2008-09 and again during the 2009-10 financial year, the AGSA reported within its information systems review, that nothing has happened with regard to the governance of ICT, which directly affects ICT continuity (Department: Public Service and Administration, 2012). The AGSA subsequently recommended that a government-wide corporate governance of ICT framework be implemented to address ICT risks,

which would, in turn, address the continuity of ICT, as part of this governance mandate.

The governance framework recommended by the AGSA in the 2008/09 audit report materialised in the year 2012, addressing both the corporate governance- and governance of ICT, with all its inherent risks, including ICT continuity. This framework, namely the Corporate Governance of ICT Policy Framework (CGICTPF), aims to institutionalise ICT as an integral part of corporate governance within government departments and would be implemented in three phases (Department: Public Service and Administration, 2012). Importantly, the CGICTPF is applicable to all spheres of government (Department: Public Service and Administration, 2012) which made this the guiding ICT document for municipalities, at that time.

The CGICTPF requires as part of the implementation of Phase 1, a Business Continuity Plan which in turn informs a Business Continuity Strategy, Business Continuity Policy and an ICT Continuity Plan (Department: Public Service and Administration, 2012). Essentially, it directs government departments on *WHAT* must be done. Being a governance framework, one would not expect the CGICTPF to provide much technical detail. However, as stated before, the CGICTPF is applicable to all government spheres, whether national or local. Consequently, a challenge emerges where a small municipality with limited resources must implement the same framework as a national department with adequate resources.

The CGICTPF is a very high level and complex governance framework and therefore, municipalities with resource capacity limitations have struggled to implement it given the time frame set out for each of the implementation phases (Department: Western Cape Local Government, 2015a). In support, especially for low-capacity municipalities, the South African Local Government Association (SALGA) published a guidance document in 2012 to aid municipalities in this regard.

The SALGA guidelines, titled: *A Municipal Guide/Roadmap to Successful ICT Governance*, aligns with the CGICTPF and provides municipalities with more guidance regarding the governance of ICT (SALGA, 2012). However, regarding ICT continuity, the SALGA guidelines do not provide much more detail than the CGICTPF itself. Instead, it provides guidance in the form of short-term goals, without any further explanation. This might hinder

implementation at municipalities with resource deficiencies, especially if the municipality lacks skilled ICT staff and finances. In essence, both the CGICTPF and the SALGA guidelines only dictate *WHAT* has to be done, and do not provide detail on *HOW* it should be done. The lack of implementation guidance becomes evident in the subsequent audits.

As seen in Section 3.2, the AGSA reports a decline in municipalities with embedded and functioning ICT continuity controls (Auditor-General of South Africa, 2015). This finding comes two years after the publication of the CGICTPF and the SALGA guidelines, resulting in municipalities surpassing the deadline for ICT continuity implementation, as required by Phase 1 of the CGICTPF, by one year. In the 2013/14 audit report, the AGSA, in response, notified that, “The national coordinating and monitoring structure customised the corporate governance of ICT policy framework (CGICTPF) for local government and drafted a municipal CGICTPF”. This resulted in the Municipal Corporate Governance of ICT Policy (MCGICTP) (Auditor-General of South Africa, 2015).

The MCGICTP aims to address the insufficiencies of the CGICTPF and caters for local government specifically (Department: Western Cape Local Government, 2015b). It again reiterates the important role of ICT in local government and emphasises the need for the corporate governance of ICT to become a municipal council and management function. However, although this new policy is set to be implemented in the 2015/16 financial year, little has changed.

A critical analysis of the draft MCGICTP, against the CGICTPF, indicates that it is predominantly the same. The MCGICTP again requires the implementation of corporate governance and governance of ICT in three phases. Each phase has predominantly the same requirements as the CGICTPF, with the only difference being an extended time-frame for each phase, as well as updated terminology to suit the municipal environment. A comparison between Phase 1 of the CGICTPF and MCGICTP is shown in Table 3.1 below. It is evident that the requirements of the MCGICTP are merely adapted from the CGICTPF. The only major difference within the requirements of Phase 1, is that the MCGICTP has expanded the security and continuity policy of the CGICTPF into more specific policies that would normally be catered for within the larger security and continuity policies.

Table 3.1: CGICTPF versus MCGICTP - Phase 1 Comparison

CGICTPF	MCGICTP
<i>PHASE 1: March 2014</i>	<i>PHASE 1: June 2017</i>
Corporate Governance of ICT Policy Framework and Governance of ICT Framework approved and implemented	Municipal Corporate Governance of ICT Policy approved and implemented
Governance of ICT Charter approved and implemented	ICT Governance Charter approved and implemented
Approved and implemented Risk Management Policy that includes the management of business-related ICT risks	Approved and implemented Risk Management Policy that includes the management of Municipal-related ICT risks
Approved and implemented Internal Audit Plan that includes ICT audits	Approved and implemented Internal Audit Plan that includes ICT audits
Approved and implemented ICT Management Framework	Approved and implemented ICT Management Framework
Approved and implemented departmental Portfolio Management Framework that includes ICT portfolio/programme and project management	Approved and implemented municipal Portfolio Management Framework that includes ICT portfolio/programme and project management
Approved ICT Continuity Plan informed by Departmental Business Continuity Plan and Strategy	Approved ICT Disaster Recovery Plan informed by Municipal Continuity Plan and Strategy
Approved and implemented ICT Security Policy	Approved ICT Security Controls policy
-	Approved Data Backup and Recovery policy
-	Approved ICT Service Level Agreement Management policy
-	Approved ICT User Access Management policy
-	Approved ICT Operating System Security Controls policy

\* Note: Table data retrieved from the CGICTPF and MCGICTP respectively (Department: Public Service and Administration, 2012; Department: Western Cape Local Government, 2015b)

In essence, the MCGICTP again addresses *WHAT* must be done, with very little guidance as to *HOW* it should be done. Extended time frames for deliverables will not necessarily lessen the burden on resource-stricken munic-

ipalities. Based on the audit outcomes after the release of the CGICTPF, it can be argued that the MCGICTP will not be of any greater assistance than the CGICTPF itself, especially taking into account the unique challenges faced by municipalities. The following subsection will aim to identify some of the main challenges that are hindering municipal attempts at implementing effective governance of ICT which results in effective ICT continuity.

### **3.4 ICT Readiness for Business Continuity in Local Government**

Chapter 2 introduced IRBC as a more contemporary approach to ICT continuity. IRBC works towards a resilient ICT environment which enables a resilient enterprise. The objective of this study is essentially to assist with the planning and ultimate implementation of IRBC in municipalities, in order to address the concerns of the AGSA regarding ICT continuity. The various attempts by the government to address the governance of ICT, and in effect - ICT continuity, have proven ineffective. It is core to the success of any municipality to have effective IRBC in place.

IRBC in municipalities will greatly reduce the risk of disruption and effectively enable the municipality in its service delivery efforts. However, to date, municipalities have largely failed in their attempts towards ICT continuity. Therefore, to implement IRBC in municipalities it is important to firstly identify the various challenges that prevent municipalities from achieving the continuity mandate defined in the MCGICTP. Upon considering these challenges, criteria can be defined which an approach for IRBC in local government should adhere to, for it to be successful.

#### **3.4.1 Challenges within Local Government**

The concerning findings from the AGSA reports in the past several years have given little reason for municipalities to ignore the major inadequacies of its ICT controls and in this case ICT continuity in particular. Municipalities require proper ICT continuity, but as seen in the previous section, past and present initiatives have proven fruitless in overcoming what seems to be an overwhelming amount of challenges. To address this real-life problem, it

is essential to consider the challenges in municipalities. These challenges predominantly revolve around capacity.

Capacity, in a municipal sense, refers to the availability of and access to tangible resources which include human, financial, material, or technological resources, and furthermore to have the knowledge to implement policies and deliver public services (Brynard & De Coning, 2006). Capacity also refers to intangible resources, for instance commitment to, and leadership for, the implementation and delivery of public services (Brynard & De Coning, 2006). It is fair to argue, that the lack of capacity in municipalities, both in terms of tangible and intangible resources, will drastically weaken their efforts of implementing effective ICT continuity controls.

In the case of local government, unfortunately, one size does not fit all. In its guidelines, SALGA states that cognisance must be taken that low, medium and higher capacity municipalities, across all classes of the local government sphere, exist (SALGA, 2012). Furthermore, SALGA deduces five distinct categories of municipalities based on their fiscal capacity and resource availability and subsequently found that about 30% of municipalities fall into the 'poor resources and low-capacity' category (SALGA, 2012). The AGSA also points out that budget constraints limit the development of ICT policies and procedures within municipalities (Auditor-General of South Africa, 2014, 2015). Thus, it is evident that many municipalities are facing financial challenges when it comes to implementing ICT controls, with ICT being a budget intensive undertaking, but there are also challenges beyond finances.

Human resource capacity, including skills and knowledge, are critical to the success of any ICT undertaking. Unfortunately, low-capacity municipalities do not always possess qualified or capable personnel. Kanyane (2006) notes that amongst others, weak leadership in strategic management which includes corporate governance, misplacement of skills within municipalities and political considerations in appointments of senior managers without required qualifications, has tremendously weakened the performance of municipalities. Specifically, with regard to ICT, SALGA stated that because of a large skill shortage, ICT staff in many municipalities are made up of under-qualified professionals with watered-down skills that are not capable of handling real-life ICT challenges (SALGA, 2012). This notion is sup-

ported by the AGSA who reports a lack of skills to appropriately design and implement ICT controls (Auditor-General of South Africa, 2014, 2015). Therefore, it becomes evident that a knowledge and skills shortage in many municipalities, especially within the ICT department, exist.

In many cases, laws, policies or procedures that have good intentions may also be a thorn in the path of progress. South African municipalities are self-governing entities, subject to conformance with provincial and national legislation. With regard to ICT, therefore, they operate in a very isolated non-uniform manner (Constitution of South Africa, 1996; SALGA, 2012). Resultantly, the municipal ICT environments might differ, from both a topological and a technological perspective and therefore, their software and hardware resources might also be different. Providing municipalities with a one-size-fits-all ICT framework and disregarding the fact that municipalities are unique entities, sets them on a path to failure. Consequently, any approach to help local government should, therefore, be usable in any environment enabling functionality within the greater majority of municipalities, irrespective of technological, financial or human resource capabilities or differences.

### 3.4.2 Criteria for IRBC in Local Government

Implementing IRBC to ultimately address the problem of ICT continuity in municipalities, as identified by the AGSA, requires consideration of the challenges that have crippled current attempts. Some of the major challenges have been discussed in the previous subsection, and paired with the fact that the MCGICTP provides little guidance as to *HOW* municipalities should implement their ICT controls, leaves many low-capacity municipalities unable to meet the requirements of the AGSA.

To successfully implement IRBC in municipalities requires an approach built around the various challenges. Consideration should be taken of the financial constrictions, skills and human resource shortages as well as unique municipal environments. An approach towards IRBC in municipalities should therefore adhere to certain criteria.

Municipalities, especially those who fall into the ‘poor resources and ‘low-capacity’ category, should be facilitated by a *Scalable* approach appropriate to its resource capacity. An undertaking such as IRBC, in an effort to address

all the related risks, can become a bottomless pit. The approach should, therefore, be dynamic, in order to scale to financial capability, size and the risk-appetite of the municipality.

The CGICTPF and MCGICTP as stated before, are rather complex and at a high level, providing little technical detail. The lack of human resource capacity, in terms of knowledge, skill and availability, in many municipalities results in little being done to implement these policies. An approach for IRBC should, therefore, be *Simplistic* and *Comprehensible*. A simplistic approach translates to an approach that is easier to implement, and someone with or without specialised skill should be able to plan and implement IRBC. Furthermore, the approach should also be comprehensible; the person responsible for IRBC should easily understand what they are doing and how the different components relate and interact throughout the process.

The South African government structure, advanced as it may be, results in municipalities being self-governing entities. This leads to municipalities having unique ICT requirements and differing in many aspects. An approach towards IRBC should, therefore, be *Usable* in any municipality regardless of technology in use, or different operating environments. Should an approach be automated, it has to be compatible and usable throughout each of the 278 municipalities.

Table 3.2: Criteria for an approach towards IRBC in Local Government

Scalable
Simplistic
Comprehensible
Usable

South African government has attempted through various initiatives to address the inadequacies of ICT in local government but has fallen short in most cases. The criteria for an approach towards IRBC, as argued in this subsection, is listed in Table 3.2, for future reference. Such an approach for IRBC to address the municipal ICT continuity problem, which is proposed in this study in the form of a method, should aim to adhere to these criteria to make it more suitable and acceptable to the municipal environment. Therefore, through using this method, municipalities should benefit by 'knowing'



*HOW* to implement IRBC and being able to help themselves, in addressing their ICT continuity problems.

### 3.5 Conclusion

This chapter explored different aspects relating to ICT continuity in local government, in working towards IRBC. As in the case of modern enterprises, ICT is core to municipal objectives and ultimately enables municipalities to deliver services to their communities. The importance of adequate business and ICT continuity is, therefore, undeniable. As with modern enterprises, municipalities should also work towards having a resilient ICT environment. It would be beneficial for municipalities to have IRBC embedded and functioning.

Unfortunately, the AGSA reports that the majority of municipalities do not have embedded and functioning ICT continuity controls. The number of municipalities that do have has declined, despite various government initiatives to address municipal ICT. It has become evident that the current initiatives by the government does not suit the unique challenges of municipalities and provides little guidance as to how the different ICT controls should be implemented.

Municipalities fall into different categories with regard to resource capacity and most are regarded as ‘poor resource and low-capacity’ municipalities. Many struggle with financial constraints, staff and skills shortages, as well as having to adapt government policies to their unique environments.

To circumvent these challenges and help municipalities address their ICT continuity problems, this chapter outlined a list of four criteria, seen in Table 3.2, which a method towards IRBC should adhere to, for such a method to be appropriate in the municipal environment. Designing a method towards IRBC in municipalities and tailoring it around their unique challenges, should increase the chances of IRBC implementation being successful. The following chapter will outline the research design required to develop such a method for municipal IRBC.

# Chapter 4

## Research Design

*This chapter outlines the design of this research study. A brief discussion introducing the research paradigm is followed by an exploration of the research process, delineating the approach of the study to reach its intended objectives. The research process is further contextualised to this study. Lastly, the research methods used throughout the research process will be defined.*

### 4.1 Introduction

The problem statement defined for this study in Chapter 1, concerns a real-world problem experienced by local government in South Africa. This problem and the various challenges faced by local government, especially within resource restricted municipalities, have been outlined in the previous chapter. The objective of this study is therefore, to address this problem situation and ultimately address or minimise the effect these challenges have on the various municipalities' ability to achieve a resilient ICT environment.

This chapter will, therefore, describe and delineate the research approach followed towards fulfilling the objective of this study. It will briefly discuss the research paradigm, which places the research within an established set of practices and provides principles to which the study should adhere. Furthermore, the research process used will be explored and defined for the purpose of steering the research towards the set objectives. This process will be further contextualised to this study. Lastly, the research methods used throughout the study will be outlined.

## 4.2 Research Paradigm

The primary objective of this study is to construct an artefact in the form of a method to assist the development of ICT Readiness for Business Continuity (IRBC) in local government. In the context of this study, a method refers to: “*An organised collection of concepts, beliefs, values, and normative principles supported by material resources*” (Lyytinen, 1987). Madsen, Kautz, and Vidgen (2006) further explain, based on the definitions by Andersen et al. (1990) and Mathiassen (1998) that, a method consists of prescriptions for performing a certain process, aided by principles, techniques or computer-based tools.

The method proposed in this study consists of a sound theoretical foundation and a supporting tool-set, which collectively forms an artefact. This goal, therefore, places this study suitably within the design-oriented information systems (IS) research paradigm, as described by Österle et al. (2011). Design-oriented IS research aims at the development of artefacts, which include constructs, models, methods and instantiations that lead to concrete manifestations (Österle et al., 2011). These manifestations may take many different forms, including amongst others: guidelines, frameworks, software, or business models, which aim towards addressing real-world problems. Furthermore, Österle et al. (2011) state that design-oriented IS research is not a non-judgemental scientific discipline but says that it is rather a normative discipline in the sense that the construction of artefacts is guided by the desire to yield a specific benefit and satisfy objectives.

This study further aligns itself to design-oriented IS research, as it builds upon a ‘to be’ conception, explained by Österle et al. (2011), and takes into account restrictions and limitations. These limitations are evident in South African municipalities, who form an important stakeholder of this study. With regard to stakeholders, design-oriented IS research targets individuals or enterprises, which include amongst others - public administration, that provides resources for the research, and in return, expect favourable results for themselves (Österle et al., 2011). In the case of this study, its objective essentially aims to help municipalities with their efforts towards a resilient ICT environment. Therefore, the development of an artefact in the form of a method, emphasises the suitability of this paradigm.

Table 4.1: The Principles of Design-oriented IS Research

<b>Principle</b>	<b>Explanation</b>
<i>Abstraction</i>	Each artefact must be applicable to a class of problems
<i>Originality</i>	Each artefact must substantially contribute to the advancement of the body of knowledge
<i>Justification</i>	Each artefact must be justified in a comprehensible manner and must allow for its validation
<i>Benefit</i>	Each artefact must yield benefit - either immediately or in the future - for the respective stakeholder groups

\* Note: From Österle et al. (2011)

With this in mind, Österle et al. (2011) explains that design-oriented IS research advocates academic freedom and researchers are free to decide on objectives and research methods - this, as long as they adhere to the specific principles of design-orientated IS research. These principles, namely, abstraction; originality; justification and benefit, are described in Table 4.1. In essence, as long as the research complies with the principles of design-oriented IS research, the method for conducting the research is in the hands of the researcher. Österle et al. (2011) do, however, outline some frequently used methods, which include amongst others, surveys, case studies or expert interviews. Typical methods for artefact design may further include demonstration, prototype construction or modelling. In terms of evaluating the artefact, Österle et al. (2011) state that evaluation can be achieved through laboratory experiments, pilot applications, simulation procedures, expert reviews or field experiments, to name a few.

Although many methodologies exist in literature with regard to different types of design research, this study is best suited to the design-oriented IS research paradigm. The requirement of an artefact, and the resulting artefact's ultimate benefit to the municipalities as stakeholders, in addressing a real-world problem, makes it ideal within the scope of this study. In order to yield this artefact, the research must follow a well defined process. Österle et al. (2011) provide a process for conducting research within this paradigm. The next section will elaborate on this process.

### 4.3 Research Process

Österle et al. (2011) state that design-oriented IS research specifically follows an iterative process consisting of four phases. These four phases include, (1) Analysis (2) Design (3) Evaluation (4) Diffusion. These phases and their iterative nature are illustrated in Figure 4.1. The phases provided by Österle et al. (2011), provide the researcher with a predetermined process to achieve the stated objective of the study. Unfortunately, the phases themselves lack the comprehensive explanation and guidance needed by researchers in a larger study. Fortunately, as Österle et al. (2011) stated, design-oriented IS research advocates academic freedom, provided researchers adhere to the principles of design-oriented IS research. Therefore, considering this notion and for the purpose of this study, a research process, whose goals can be aligned to that of design-oriented IS research, has been identified within a different research paradigm. This paradigm is known as design-based research.

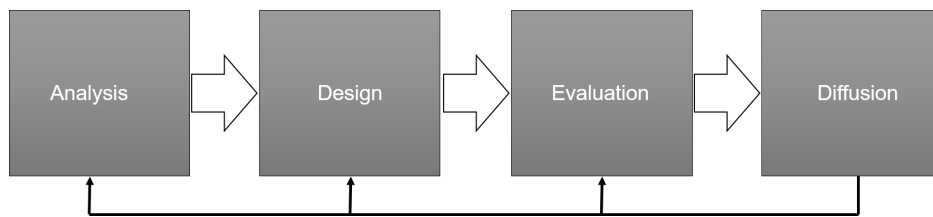


Figure 4.1: Design-oriented IS Research - Iterative Phases

Design-based research is predominantly used within the learning sciences. However, Wang and Hannafin (2005) state that the design-based research paradigm, which advances design, research and practice simultaneously, has demonstrated considerable potential. Barab and Squire (2004) describe design-based research as being: “Not so much an approach as it is a series of approaches, with the intent of producing new theories, artefacts and practices that account for and potentially impact learning and teaching in naturalistic settings”.

Furthermore, Wang and Hannafin (2005) support what is stated by Barab and Kirshner (2001), in that design-based research challenges the assumption that research is contaminated by the external influence of the researcher. They explain that researchers instead manage the research processes in collaboration with stakeholders, design and implement interventions systemat-

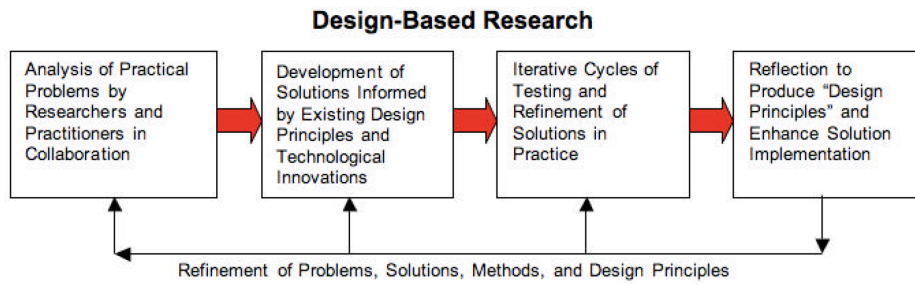


Figure 4.2: Design-based Research Process (Reeves, 2006)

ically to refine and improve initial designs and ultimately seek to advance both pragmatic and theoretical aims affecting practice (Wang & Hannafin, 2005).

Wang and Hannafin (2005) assert that design-based research is a form of hybrid methodology, where researchers draw on procedures and methods from both a designer and researcher point of view. Importantly, design-based research does not replace other methodologies but rather provides an alternative approach that emphasises direct, scalable and concurrent improvements in research, theory and practice (Wang & Hannafin, 2005).

From the above, similarities between design-oriented IS research and design-based research, mainly in what it strives to achieve, becomes evident. The similarities between these research paradigms are further emphasised with regard to their approach. The phases of the design-based research process, in most cases, are built around the characteristic of an iterative cycle of analysis, design, implementation and redesign (Wang & Hannafin, 2005). This notion aligns the design-based research process to that of design-oriented IS research, defined by Österle et al. (2011). The goal of producing an artefact and the iterative nature in which it is achieved, align these approaches. Therefore, for the purpose of this study, the four phases of design-based research defined by Reeves (2006) and illustrated in Figure 4.2, have been deemed suitable to accomplish the objectives of this study, whilst adhering to the principles of design-oriented IS research.

The phases provided by Reeves (2006) are further detailed by Herrington, McKenney, Reeves, and Oliver (2007), who map it to elements of a typical research project, required within each phase. This mapping is illustrated in Table 4.2. Each of the research elements mentioned in Table 4.2 is further

Table 4.2: Design-based Research: Elements in Phases

Phase	Element
<i>Phase of design-based research</i>	<i>The elements that need to be completed</i>
<i>PHASE 1: Analysis of practical problems by researchers and stakeholders in collaboration</i>	Statement of problem
	Consultation with researchers and stakeholders
	Research objectives
	Literature review
<i>PHASE 2: Development of solutions informed by existing design criteria and technological innovations</i>	Theoretical Method
	Development of criteria to guide the design of the intervention
<i>PHASE 3: Iterative cycles of testing and refinement of solutions in practice</i>	Description of proposed intervention
	<b>First iteration</b>
	Participants
	Data collection
	Data analysis
	<b>Second and further iterations</b>
	Participants
Data collection	
Data analysis	
<i>PHASE 4: Reflection on criteria of produced artefact; and enhance solution implementation</i>	Design Criteria
	Designed artefact(s)
	Professional development

\* Note: Adapted from Herrington et al. (2007)

explained by Herrington et al. (2007) leaving little room for misinterpretation. Consequently, as opposed to the phases of the design-oriented IS research process, sufficient clarification about the requirements of each phase is detailed through these elements, and provides the researcher with clear objectives for each phase.

Therefore, following the research process from the design-based research paradigm, is mainly attributed to the better frame of reference and guidance provided in the underlying phases, which is found to be lacking from the design-oriented IS research process. Design-oriented IS research luckily provides the flexibility to the researcher to do this. Thus, in essence, to help

municipalities address the issue of ICT continuity, an integrated approach consulting both design-oriented IS research and design-based research, was followed. This process is illustrated in Figure 4.3.

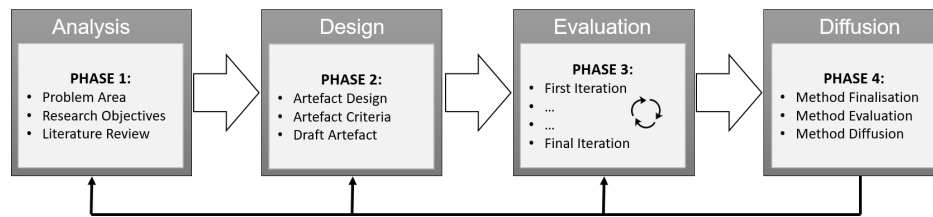


Figure 4.3: Integrated Research Process

The approach illustrated in Figure 4.3 sufficiently caters for the design of an artefact, in the form of a method, to assist municipalities in developing IRBC. Through its iterative nature, in participation with municipalities as stakeholders, it enables the design of an artefact through continuous testing and refinement until it is found to be acceptable by researchers and stakeholders. The following section will further contextualise this integrated research process, to adequately outline how this process was used to address the problem.

## 4.4 Contextualisation of Research Process

Considering the goal of developing an artefact, to assist municipalities towards achieving a resilient ICT environment, the previous section outlined an integrated research process, illustrated in Figure 4.3. The integrated phases of Österle et al. (2011) and Reeves (2006), supported by the elements provided by Herrington et al. (2007), provides clear guidance on how the research process unfolds and what to deliver within each phase. This section elaborates on the elements provided in Table 4.2, by positioning and contextualising the elements within this research study. Each phase has been divided into a separate table within the following subsections.

### 4.4.1 Phase One

Phase 1 primarily revolves around properly defining the problem area. This is a common task within most research studies, however, in this study it involves



consultation between the researcher and stakeholders, and it is, therefore, important that local government is involved in this process. Upon defining a suitable problem statement, sound objectives should be developed to guide the study towards its intended contribution, which in this case is in the form of an artefact. This is followed by a comprehensive literature review, both on the problem area, as well as the subject area in general.

Table 4.3: Contextualised Research Phase 1

<b>Phase</b>	<b>Element</b>	<b>Position</b>
<i>Phase of design-based research</i>	<i>The elements that need to be completed</i>	<i>Position within study</i>
<i>PHASE 1: Analysis of practical problems by researchers and stakeholders in collaboration</i>	Statement of problem	Consultation with stakeholders from local government, results in identification of problem situation to be addressed
	Consultation with researchers and stakeholders	
	Research objectives	Research objectives are defined to address the problem situation
	Literature review	A literature review is conducted to further explore the problem area

\* Note: Adapted from Herrington et al. (2007)

Table 4.3 summarises the context of this study. In essence, within this study, Phase 1 involves meeting and consulting members from municipalities, as well as directly associated government departments, to clearly define the problem around ICT continuity. This includes discussing some of the challenges municipalities face in addressing their ICT continuity concerns and what efforts they have taken in the past in working towards effective ICT continuity controls.

Once the problem is clear, sound research objectives to address this problem situation are defined. The research objectives guide the study towards reaching what is finally the completed artefact, which in this case takes the form of a method, to help municipalities towards a resilient ICT environment.

Lastly, a comprehensive literature review is conducted. This includes studying various literature sources. In the case of this study, it is essential to also study different government and municipal policies, frameworks and legislation to appropriately understand the stakeholder environment. Standards and best practices are also consulted, to determine what is regarded

as the norm within the industry.

Upon completion of this phase, the researcher should have a comprehensive view of the problem area and the environment within which intervention is required.

#### 4.4.2 Phase Two

The emphasis within Phase 2, largely concerns the development of criteria which should guide the design of the proposed intervention. This criteria forms the basis for the design and ultimate development of the artefact as intervention, in addressing the problem defined in Phase 1.

Table 4.4: Contextualised Research Phase 2

<b>Phase</b>	<b>Element</b>	<b>Position</b>
<i>Phase of design-based research</i>	<i>The elements that need to be completed</i>	<i>Position within study</i>
<i>PHASE 2: Development of solutions informed by existing design criteria and technological innovations</i>	Theoretical Method Development of criteria to guide the design of the intervention	Analyse literature and feedback from local government and extract design criteria
	Description of proposed intervention	Develop initial draft artefact (method) based on criteria and literature

\* Note: Adapted from Herrington et al. (2007)

Phase 2 is summarised in Table 4.4. In the context of this study, the criteria, which is formulated in Chapter 3, stems from literature but is also largely derived from the consultation with members from municipalities and the feedback received regarding the challenges they face in implementing ICT continuity. The criteria form the basis for designing the artefact and should aim to circumvent most of the challenges hindering current attempts of achieving ICT continuity.

Once the criteria are outlined, a first draft of the artefact is designed. This study proposes an artefact in the form of a method, which consists of a theoretical foundation and supporting tool-set, as discussed in the beginning of Section 4.2. This method to help municipalities towards IRBC, is initially

drafted from literature and based on the criteria to make it suitable within the municipal environment.

Phase 2 is finalised with the design of an initial draft artefact. This initial artefact will be refined through various cycles with municipalities as part of Phase 3.

### 4.4.3 Phase Three

The majority of the research study takes place within Phase 3. It involves the iterative cycles of refinement in collaboration with the stakeholders. Starting with the draft artefact from Phase 2, various cycles of refinement, including data collection, analysis and revision is conducted with stakeholders, until such a time where both the researcher and the stakeholders deem the artefact acceptable.

Table 4.5: Contextualised Research Phase 3

Phase	Element	Position
<i>Phase of design-based research</i>	<i>The elements that need to be completed</i>	<i>Position within study</i>
<i>PHASE 3: Iterative cycles of testing and refinement of solutions in practice</i>	<b>First iteration</b>	First iteration starts with draft artefact (method) as designed in Phase 2
	Stakeholders	Members from local government
	Data collection	Artefact (method) is tested for acceptance and feedback received
	Data analysis	Interpretation and analysis of feedback
	Implementation of intervention	Revision of artefact (method) based on data analysis
	<b>Second and further iterations</b> (Same elements as first iteration)	Second iteration starts with revised artefact (method) from previous iteration. Refinement of artefact continues until acceptable level is reached

\* Note: Adapted from Herrington et al. (2007)

Phase 3 is positioned in the context of this study and summarised in Table 4.5. Each iteration in this study involved members from municipalities. The artefact is presented and various research methods are used throughout each iteration. Data is collected, which involves feedback from the mem-

bers regarding concerns, possible improvement and considerations from their working environment.

The collected data is analysed and literature is further studied to address some issues. This results in the refinement of the artefact in preparation of the next iteration, which includes the same elements. This refinement takes place until members from municipalities deem the method suitable in their environment and is accepted by both researcher and municipalities.

Upon completion of Phase 3, an accepted artefact, in this case - a method, is delivered. The method can now be evaluated within Phase 4.

#### 4.4.4 Phase Four

Phase 4 is the reflection phase. An accepted artefact should now be validated. Part of this validation includes verifying whether the artefact complies with the criteria defined as part of Phase 2. The artefact is finalised and diffused to the stakeholders.

Table 4.6: Contextualised Research Phase 4

Phase	Element	Position
<i>Phase of design-based research</i>	<i>The elements that need to be completed</i>	<i>Position within study</i>
<i>PHASE 4: Reflection on criteria of produced artefact; and enhance solution implementation</i>	Design Criteria	Ensure method complies with identified criteria defined in Phase 2: <ul style="list-style-type: none"> <li>• Scalable</li> <li>• Simplistic</li> <li>• Comprehensible</li> <li>• Usable</li> </ul>
	Designed artefact(s)	Finalised method for IRBC in local government
	Professional development	Make available (Diffuse) to local government and publish solution

\* Note: Adapted from Herrington et al. (2007)

In the context of this study, Phase 4 involves a validation workshop, with members of municipalities. Phase 4 is positioned in this study and illustrated

in Table 4.6. The aim of this workshop is to test whether the method for IRBC, actually complies with the established criteria.

Upon validation, the method is finalised and made available in municipalities and further reported on in publications.

Each phase of the research process is dependent on various research methods, which are used to accomplish the requirements of each of the different phases. The following section will elaborate on these research methods.

## 4.5 Research Methods

The contribution of this study, defined within the primary objective, is an artefact in the form of a method. This method consists of various deliverables to aid municipalities in developing IRBC. To achieve this objective and deliver the artefact, secondary objectives, have to be fulfilled. These objectives will be achieved using a mixed-method approach within the research process defined in the previous section.

A comprehensive literature review is conducted to explore the ICT continuity landscape and all of its related processes and disciplines. Best practices and international standards are studied to identify the relevant IRBC requirements. Surveys in the form of semi-structured interviews are conducted with local government, to identify challenges within municipalities that could hinder IRBC development, as well identify requirements specific to municipalities. Furthermore, various focus group sessions are conducted within local government to refine the artefact. Throughout the iterative cycles the artefact is illustrated using modelling techniques, and near the end, the supporting tool-set is developed. The research methods mentioned are defined in Table 4.7, and placed within each of the research process phases.

As part of the design-oriented IS research principle of *Justification*, the artefact in its entirety is validated within a workshop seminar with representatives from local government, who evaluate the artefacts' compliance to the criteria (*Scalable, Simplistic, Comprehensible, Usable*) using a survey in the form of a questionnaire - this occurs within Phase 4.

Table 4.7: Definition of Research Methods

Research Method	Phase in Process	Definition
Literature Review	Phase 1 & 2	An iterative process of obtaining information sources relevant to one's study (Olivier, 2009)
Semi-structured Interview	Phase 1	A verbal interchange where the interviewer attempts to elicit information from another person by asking questions. Although there is a set of predetermined questions, this interview is conversational in nature and allows participants to explore issues they feel are important (Longhurst, 2003)
Modelling	Phase 2 & 3	A model captures the essential aspects of a system or process, whilst it ignores the non-essential aspects, and can serve as a blueprint for new systems or processes (Olivier, 2009)
Focus Group	Phase 3	Involves a group of people who meet in an informal setting to talk about a topic set by the researcher and allows the group to explore the subject from as many angles as they please (Longhurst, 2003)
Questionnaire	Phase 4	An instrument consisting of a series of questions and/or attitude opinion statements designed to elicit responses which can be converted into measures of the variable under investigation (Franklin & Osborne, 1971)

## 4.6 Conclusion

This chapter outlined the research design of this study. This study was placed within the design-oriented IS research paradigm. Essentially, this paradigm aims to produce an artefact, through collaboration with stakeholders, to ultimately yield benefit to the stakeholders. The paradigm is built around four principles, namely, *Abstraction*, *Originality*, *Justification* and *Benefit*. These principles will have to be met, upon completion of the study, in order to adhere to design-oriented IS research. Importantly, design-oriented IS research advocates academic freedom, allowing the researcher to decide on the methods used, subject to adherence to the principles.

Unfortunately, design-oriented IS research, does not provide a comprehensive research process. It defines four research phases, namely, analysis, design, evaluation and diffusion. However, little detail is provided to guide researchers through each phase. It is due to this issue, that this study integrates the research process from another paradigm with that of design-oriented IS research. The paradigm of design-based research, which is predominantly used within the learning sciences, defines elements within each of its research process phases. These elements provide sound guidance to the researcher in conducting the study. This study therefore follows an integrated process from both design-based research and design-oriented IS research, whilst strictly aligning to the principles of design-oriented IS research.

In order to achieve the objectives of this study, various research methods are used within a mixed-method approach to complete the different research phases. Using these methods in an iterative cycle of collaboration with local government, whilst adhering to the principles of design-oriented IS research to ultimately yield benefit to stakeholders, will prove crucial in addressing the challenges with ICT continuity in municipalities. The following chapter will elaborate how these methods and the research process materialised throughout the study and present the developed artefact.

# Chapter 5

## A Method towards ICT Readiness for Business Continuity in Local Government

*Knowing the importance of ICT within local government, this chapter proposes a method, comprised of a theoretical foundation and a supporting tool-set, for municipalities to plan their ICT Readiness for Business Continuity (IRBC) and guide them towards a higher level of resilience. The various phases of the research process, conducted in collaboration with municipalities to develop and refine this method, are discussed. The finalised method towards IRBC for local government is proposed, to assist resource restricted municipalities to work towards a resilient ICT environment.*

### 5.1 Introduction

ICT, within modern enterprises and local government alike, is undoubtedly a critical enabler for business activities. In local government, disruption to ICT can directly affect the municipalities' ability to deliver services. It is therefore crucial that these ICT services remain uninterrupted as far as possible. This study introduced IRBC as a means towards such a state, where ICT is made resilient and able to withstand disruption of ICT to an acceptable degree. However, within local government, many municipalities do not possess



adequate resources to implement IRBC and therefore, require a more *Scalable, Simplistic, Comprehensible* and *Usable* approach. This chapter argues towards such an approach. However, it is important to firstly consolidate the study as a whole, to gain an understanding of the various contributing parts and thoroughly explain the objective of this chapter.

### 5.1.1 Chapter Objective and Consolidation

It is critical that the research design, discussed in Chapter 4, be considered throughout this study. To this point, the problem and the resulting objectives of this study, have been defined in Chapter 1. The primary objective of this study involves developing an artefact, in the form of a method, to address this problem. Chapter 4 outlined an integrated research process, as part of the research design, to rigorously develop such an artefact.

As per Chapter 4, this integrated research process consists of four distinct phases, each with its own underlying elements, that have to be achieved in order to facilitate the artefact's development. These phases, together with the underlying elements, were followed meticulously and are described in this chapter as well as Chapter 6. Some of the elements that form part of Phases 1 and 2 have been completed as part of Chapter 1, 2 and 3 already. These elements and how they materialised will be discussed in the rest of the chapter.

Considering the elements of the integrated research process, the objective of this chapter is two-fold and therefore divided into two parts - A and B. For the purpose of Part A, it is important to explore how the proposed artefact materialised. The artefact takes the form of a method as it was defined in the previous chapter. The finalised method materialised upon completion of the first three phases of the integrated research process. Therefore, Part A of this chapter elaborates on these phases in detail, aligning each phase to its required elements and discussing the outcomes from each element.

Part B presents the final method, consisting of a theoretical foundation and a supporting tool-set. This method is a direct output from Phase 3 of the integrated research process and is designed around the criteria defined in Chapter 3. The method detailed in Part B of this chapter therefore represents the finalised contribution of this study.

The last requirement of the integrated research process is to validate this method against the design criteria. The validation forms part of Phase 4 (Diffusion) of the integrated research process and will be discussed in Chapter 6.

## 5.2 Part A: Developing a Method for IRBC in Local Government

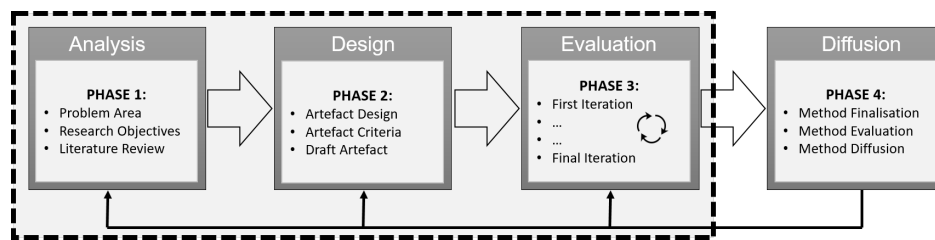


Figure 5.1: Phases Towards Finalising the Method: Phase 1 - 3

As mentioned in the previous section, Chapter 4 detailed a rigorous integrated research process, constituting the research design for this study. Core to this research process is the four phases, each requiring certain elements to be fulfilled. This section details Part A of this chapter and as illustrated in Figure 5.1 it elaborates on the first three phases of the integrated research process. These phases develop and finalise the method to address the problem situation. These three phases are therefore discussed below.

### 5.2.1 Research Phase One

As seen in Table 5.1, Phase 1 essentially involves an analysis of the problem situation. Researchers and stakeholders collaborate to establish and gauge the problem area and a problem statement, as well as objectives to address this problem, are outlined. A literature review also forms part of the entire process of Phase 1. Each element in effect delivers a sound understanding of the problem area and provides the foundation for progression into Phase 2, where the artefact can be drafted based on the outcomes of Phase 1.

The findings from the AGSA Reports highlighted an initial problem regarding ICT continuity in municipalities. These findings from the AGSA,

Table 5.1: Elements of Research Phase 1

<b>Phase</b>	<b>Element</b>
<i>Phase of design-based research</i>	<i>The elements that need to be completed</i>
<i>PHASE 1: Analysis of practical problems by researchers and stakeholders in collaboration</i>	Statement of problem
	Consultation with researchers and stakeholders
	Research objectives
	Literature review

\* Note: Adapted from Herrington et al. (2007)

discussed in Section 3.2, provided the basis from which further exploration into the problem could commence. This exploration would see the collaboration with various municipal stakeholders materialise.

As part of Phase 1, two stakeholders were identified that could assist in this regard. The first stakeholder, a representative from the Ministry of Co-operative Governance and Traditional Affairs (CoGTA), was met on the 30<sup>th</sup> of March 2015. CoGTA has a mandate towards local government, dictated in Chapter 7 of the Constitution of South Africa (1996). Furthermore, as part of their mission, CoGTA supports the delivery of municipal services to the right quality and standard, as well as promotes good governance and building administrative capability within municipalities (Ministry of CoGTA, 2016).

The meeting with CoGTA, to a large extent, involved setting the scene and gathering knowledge around the inner workings of municipal ICT's. Some of the discussion topics included the role of the AGSA, as well as who directs municipal ICT. The CoGTA representative introduced the various government ICT policies and frameworks, which include the CGICTPF and SALGA guidelines (discussed in Chapter 3). At this stage the MCG-ICTP, although not yet made public, was also introduced as the new ICT policy document specifically applicable to municipalities, as recommended by the AGSA. In essence, the meeting with the CoGTA representative provided essential insight into municipal ICT and its operations, particularly from a governance point of view.

The meeting with CoGTA was followed by a meeting with ICT managers from a district municipality and its underlying local municipalities in the Western Cape province, on the 31<sup>st</sup> of March 2015. This district municipi-

pality was identified and chosen, due to their long-standing clean ICT audit results, as well as their willingness to collaborate in this study. This district municipality, therefore, became the primary collaborative stakeholder and was involved throughout the rest of the research process.

The meeting with the ICT managers of these participating municipalities involved a semi-structured interview. The topics/questions utilised in the semi-structured interview are attached as Appendix B.1. The aim of the semi-structured interview was to get a general view of their ICT environment, their processes and some of the challenges they face. This led to an extensive discussion and elaboration from their side on the problem at hand - that of ICT continuity. Many related problems were highlighted throughout the semi-structured interview. Some of these include:

- Provincial government realised that good governance within municipalities will help ease issues around service delivery. This specific district municipality, due to their effective ICT environment, collaborated with CoGTA in drafting the MCGICTP (discussed in Chapter 3). It was highlighted that the MCGICTP had been accepted at a national level, therefore also linking to what was discussed by the CoGTA representative.
- Municipal processes should be considered when attempting to address the problem with ICT continuity. For instance, political interference may hinder policy acceptance at the municipal council level. In some cases it may take up to two years for a policy to be accepted. Even though a policy is directed from national government, it still has to be accepted by the municipal council, which in cases, cause delays.
- The ICT department in many municipalities is not represented at a strategic management level. This results in cases where ICT managers' report to the chief financial officer of their respective municipalities, instead of the municipal manager directly.
- In some cases, ICT policies do not get accepted at council due to their technical nature. Councillors refrain from attending workshops to discuss the policy, due to not understanding the policy content.

Therefore, taking into account the AGSA findings, as well as the major challenges highlighted by the ICT managers of the stakeholder district municipality, a sound problem statement (mentioned in Chapter 1) could be defined. Based on this problem, objectives to address this issue were outlined to guide the study towards the intended artefact. These objectives were also stated in Chapter 1.

An extensive literature review followed, and various academic literature, government reports and policies, legislation, standards and best practices were studied. As mentioned previously, the extent of this literature is discussed in Chapters 2 and 3. This studied literature provided the necessary theoretical basis to continue with the research process, towards drafting an initial artefact. Thus, the elements in Phase 1, to define the problem statement by consulting stakeholders, to draft the research objectives and to conduct a sound literature review have all been addressed.

## 5.2.2 Research Phase Two

Table 5.2: Elements of Research Phase 2

Phase	Element
<i>Phase of design-based research</i>	<i>The elements that need to be completed</i>
<i>PHASE 2: Development of solutions informed by existing design criteria and technological innovations</i>	Theoretical Method
	Development of criteria to guide the design of the intervention
	Description of proposed intervention

\* Note: Adapted from Herrington et al. (2007)

Phase 2 of the integrated research process, guides the initial development of the proposed method. Table 5.2 depicts the required elements of Phase 2. The first element in this phase requires an examination of the feedback from the stakeholders and literature studied during Phase 1. This enables the extraction of a set of criteria which guides the initial draft and further development of the method. A method, as defined in Chapter 4, consists of an organised collection of concepts and is supported by material resources; in other terms, it provides (1) prescriptions for performing a certain process and

(2) is aided by, amongst others, computer-based tools. The method towards IRBC in local government has to adhere to the criteria to be defined during this Phase, throughout its development.

The design criteria applicable to the method, as required in Phase 2, has been explored and clearly outlined in section 3.4.2. This criteria is based on the outcomes from the meeting with stakeholders, during Phase 1 and findings from various literature sources. From both the stakeholder meetings, as well as literature, it became clear that many of the challenges in municipalities revolve around:

- Resource capacity
- Diverse municipal ICT environments
- Challenges with approving policies
- Skills shortages

As a result, the criteria which guide the design and development of the method were highlighted in Table 3.2 and include the following criteria: *Scalable*, *Simplistic*, *Comprehensible*, and *Usable*. These criteria form the basis for the design and development of the method, to try and circumvent some of the challenges municipalities face with ICT continuity.

Considering the problem statement and the challenges municipalities face with implementing ICT continuity, the initial theoretical foundation of the method, considered various aspects that are directly associated with ICT continuity. An illustration of these components in the initial draft method and its relationships are illustrated in Figure 5.2. This theoretical foundation, in the early stages of the study, aimed to focus on the ICT component of BCM. This ICT BCM life-cycle is built upon the Plan-Do-Check-Act approach, and includes a policy, plan, as well as issue-specific plans such as the disaster recovery plan. Furthermore, this ICT BCM life-cycle directly interacts with the overall municipal BCM system, and the municipal information security management system, which are influenced by the municipal risk assessment and business impact analysis activities.

At this stage, the model illustrated in Figure 5.2, only represents the initial theory which will ultimately develop into the method as a deliverable.

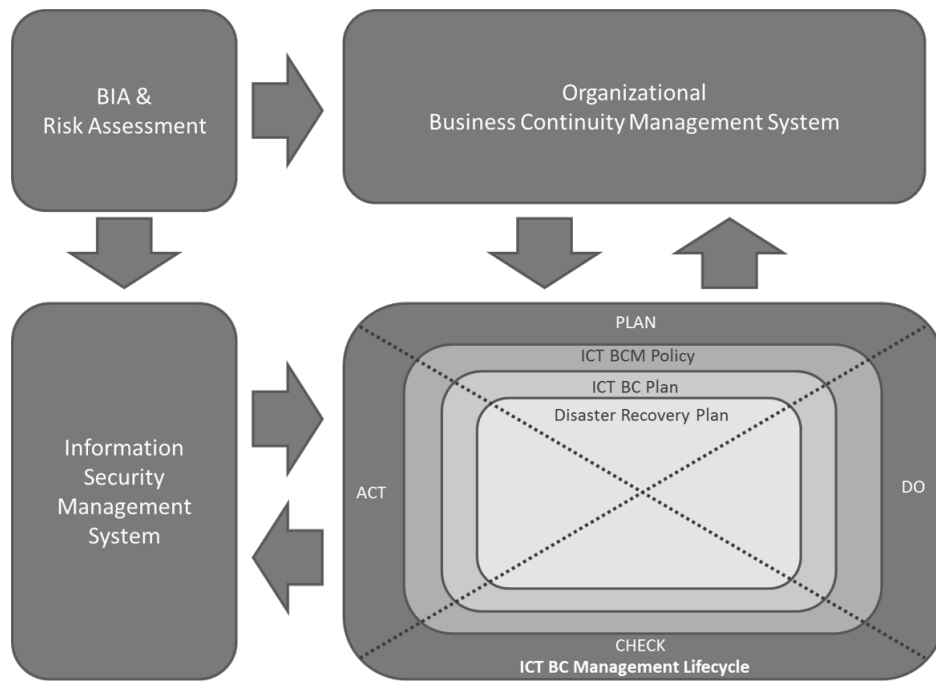


Figure 5.2: Theoretical Foundation for Initial Draft Method

This theoretical foundation still has to be expanded and further defined, as well as supported by a tool-set. In order to facilitate this process, this theoretical foundation had to be refined in collaboration with the stakeholder and further expanded - to firstly adhere to the defined criteria, as well as materialise into a comprehensive finalised method.

The elements in Phase 2, to develop criteria which guided the initial draft of the method and subsequent description of this method, have been fully addressed. Upon completion of the method's theoretical foundation, the next stage in the research process involved its refinement with the stakeholder, as part of Phase 3 of the integrated research process.

### 5.2.3 Research Phase Three

Considering the elements addressed in Phase 2, an initial method materialised. Phase 3 is critical in facilitating the refinement of the method, as illustrated in Table 5.3. In the case of this study the theoretical foundation of the method, drafted during Phase 2, can now be further refined and the method in its entirety - consisting of the theoretical foundation and a supporting tool-set, subsequently developed. This entire process is accom-

Table 5.3: Elements of Research Phase 2

Phase	Element
<i>Phase of design-based research</i>	<i>The elements that need to be completed</i>
<i>PHASE 3: Iterative cycles of testing and refinement of solutions in practice</i>	<b>First iteration</b>
	Participants
	Data collection
	Data analysis
	<b>Second and further iterations</b>
	Participants
	Data analysis

\* Note: Adapted from Herrington et al. (2007)

plished within Phase 3, and the stakeholders, who ultimately benefit from the artefact, again play an important role throughout.

For this study, Phase 3 comprised of three iterations of refinement in collaboration with the stakeholder. The stakeholder, as mentioned previously, includes the ICT management and role-players from a specific district municipality. Each of the three iterations involved a focus group session, where the artefact was presented and discussed. The collective decisions and suggestions were subsequently implemented in preparation for the next iteration. Each of the iterations is further discussed below.

### Refinement Iteration One

The first iteration of refinement happened at the district municipality on the 4<sup>th</sup> of June 2015. The theoretical foundation, depicted in Figure 5.2, was presented to the members present, who are directly involved with this municipalities' ICT function. These members stemmed from amongst others, ICT management, risk and technology.

The presentation outlined the overall objective of this study. This included the proposed contribution which was extrapolated from the initial meetings in Phase 1 to address the problem of ICT continuity. Subsequently, the draft theoretical framework of the method was proposed and its components described at a conceptual level.

The subsequent focus group discussion around the theoretical foundation provided valuable feedback. The stakeholder raised some concerns and made



a few valuable suggestions. One of the major concerns revolved around the focus on ICT business continuity management, as well as the required interaction with the municipal business continuity management system. The stakeholder emphasised that, even in some of the high-resource municipalities, a full business continuity management system remains unattainable. Consequently, it would prove difficult, especially in resource restricted municipalities, to implement the ICT focused controls without an associated business continuity management system. This is particularly true where ICT components are reliant on interaction with other business continuity components.

The stakeholder suggested that focus be entirely shifted towards ICT, which would include the recovery of ICT. The stakeholder noted that, in many cases, local municipalities are dependent on shared disaster recovery systems with the district municipality they fall under. Ultimately, if these municipalities were enabled to cater for the continuity and recovery of their own ICT environment, it would prove beneficial to both the community of the local municipality and the district municipality - on which there would be less dependence.

The stakeholder suggested that the envisaged method should ultimately allow for interaction, but not be totally dependent on ICT risk management activities, information security and business continuity. Therefore, resource restricted municipalities should be able to implement some form of ICT continuity and recovery, without necessarily having, for instance, an information security management system. Lastly, the stakeholder emphasised that requirements from the components within the proposed system, illustrated in the theoretical foundation, should be well defined, to cater for municipalities where staff and skill shortages exist.

The suggestions and concerns mentioned by the stakeholder provided the basis for revisions to the theoretical foundation, and in doing so - preparing for the following refinement iteration.

### **Refinement Iteration Two**

The theoretical foundation of the method was updated during the first refinement iteration, based on the feedback from the stakeholder. The refinement attempted to address all the issues raised by the stakeholder. The updated

theoretical foundation is illustrated in Figure 5.3. Essentially, the major change is the shift in focus to ICT continuity and recovery and the ability for this process to function independently. This resulted in IRBC becoming the focal point of this research project and the associated method.

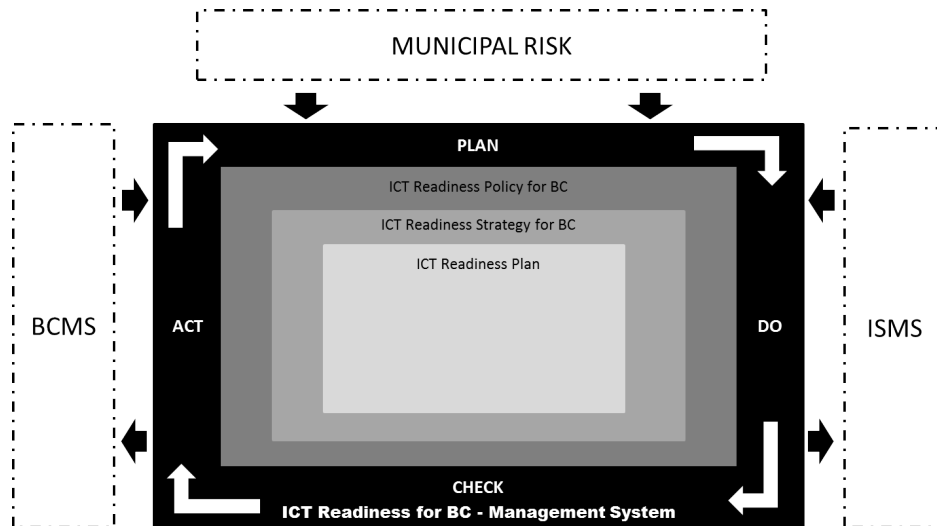


Figure 5.3: Theoretical Foundation - First Revision

The second iteration took place during a meeting with the stakeholder on the 19<sup>th</sup> of August 2015. The updated theoretical foundation was presented to the stakeholder. However, in contrast to the previous iteration cycle, this cycle required a more detailed explanation of the theoretical foundation. IRBC, as a fairly unknown concept, had to be introduced to the stakeholder. The origin and the focus on resilience by IRBC, as explained in Chapter 2, as well as its ability to function independently, had to be explained. Each component in Figure 5.3, was subsequently discussed with the stakeholder.

The updated theoretical foundation included various components. Both the Business Continuity (BCMS), and Information Security Management Systems (ISMS), as well as municipal risk, were included. However, within this theoretical foundation, these three components remain optional to a large extent, to make it suitable for the low resource capacity municipalities who cannot fully implement these systems. The IRBC management system, also based on the Plan-Do-Check-Act approach, includes three components, an IRBC policy, IRBC strategy and an IRBC plan. These constitute the major components involved.

The stakeholder, to a large extent, welcomed the method's updated theoretical foundation, as well as the concept of IRBC. The fact that it addressed many of the concerns and suggestions from the first iteration cycle, placed it in a favourable position. The stakeholder did, however, raise some issues.

Firstly, although the theoretical foundation, in its current state, seems viable, each component will have to be clearly defined. This concern would largely depend on the method's supporting tool-set.

Secondly, upon discussion around some of the pre-requisites of the IRBC system, the requirement of a business impact analysis was raised as a concern. Again, it was emphasised that there might be municipalities who do not conduct such activities, for whatever the reason, and it would, therefore, hinder the IRBC implementation.

Lastly, some concerns were raised by the stakeholder about the uncertainty whether the components illustrated in the model included everything required by IRBC and also, whether each of the components illustrated would have to go through its own Plan-Do-Check-Act cycle. These questions had to be addressed in the next refinement.

In conclusion of this refinement iteration, the proposed method's theoretical foundation - especially the IRBC concept, in general, was accepted by the stakeholder. However, amendments were still required, based on the issues raised during the discussions.

### **Refinement Iteration Three**

The third and final refinement iteration, in collaboration with the stakeholder, occurred on the 17<sup>th</sup> of November 2015. The focus of this iteration was firstly to outline the changes made to the method's theoretical foundation in response to the issues raised in the previous iteration. However, more importantly, this iteration presented the supporting tool-set. As mentioned earlier, the method consists of a theoretical foundation and a supporting tool-set.

The changes to the theoretical foundation, based on the feedback from the previous cycle, addressed the stakeholders' concerns and was consequently finalised. This finalised theoretical foundation is illustrated and discussed in the following section. The focus of this iteration, however, was on the method's supporting tool-set.

The tool-set is constituted of various exercises resulting in a number of draft output documents. Therefore, in preparation of this refinement iteration, a proof-of-concept of the proposed supporting tool-set and drafts of its various outputs was produced. This included:

- A draft IRBC policy
- A spreadsheet-based tool for the creation of the policy
- A spreadsheet-based tool for municipalities to conduct a business impact analysis
- A spreadsheet-based tool for selecting an IRBC strategy

The stakeholder thoroughly examined the draft policy and suggested changes to make it more suitable to the municipal environment. The stakeholder also examined the operation and output of the supporting tool-set, and subsequently deemed it to be at an acceptable level. The feedback required from the stakeholder regarding the supporting tool-set, mainly revolved around its alignment to the municipal environment. This included feedback on issues like the use of correct terminology, as well as the feasibility of the supporting tool-set to fulfil its intended purpose.

Apart from minor suggestions regarding the supporting tool-set, as well as amendments to the IRBC policy, the supporting tool-set of the proposed method was deemed acceptable by the stakeholder. Therefore, taking into account that both the theoretical foundation and supporting tool-set were deemed acceptable by the stakeholder, pending minor alterations, refinement iteration three concluded Phase 3 of the research process.

The elements in Phase 3 required multiple iterations of refinement until the method was deemed acceptable by the stakeholder. Thus, having concluded three iterations and having both the theoretical foundation and the supporting tool-set accepted by the stakeholder, Phase 3 was concluded satisfactorily. Therefore, the following section explores the theoretical foundation and the associated tool-set, as the complete and finalised method towards IRBC in local government.

## 5.3 Part B: A Method towards IRBC in Local Government

The problem situation, highlighted in Chapter 1 and 3, is that many municipalities in South Africa, experience challenges regarding the design and implementation of ICT continuity controls. This study therefore aimed to address this problem and importantly not only focus on *WHAT* must be done, but also provide guidance on *HOW* it can be done. As discussed in Chapter 3, municipalities have received many directives on *WHAT* they need to do with regard to the governance of their ICT function. This section, therefore, elaborates on a devised method, to help municipalities with *HOW* they can approach their ICT continuity.

The method proposed in this section resulted from an initial artefact drafted in Phase 2, which was refined through three iterations with the particular stakeholder. As previously stated, the proposed method for IRBC in local government consists of a theoretical foundation, as well as a supporting tool-set. This method including these components will be termed “M-IRBC” from this point onwards. M-IRBC aims to assist municipalities to plan their IRBC system, as they work towards achieving a resilient ICT environment.

### 5.3.1 Theoretical Foundation

The M-IRBC theoretical foundation, deemed acceptable by the stakeholder as part of Phase 3 of the integrated research process, is illustrated in Figure 5.4. The final theoretical foundation is based on the IRBC model provided in the ISO/IEC 27031 (2011) standard, whilst also taking into account the unique municipal environment. The theoretical foundation illustrates the most basic components, a municipality with limited resources, will require in an initial attempt towards implementing IRBC.

The theoretical foundation can be divided into two sets of components. Firstly, the external components, which include, municipal risk, ISMS and BCMS; and secondly, the IRBC system itself, consisting of the Plan-Do-Check-Act phases with underlying components in each phase. The majority of these components have been discussed in Chapter 2, however, this section will place these components into context and refer back where applicable.

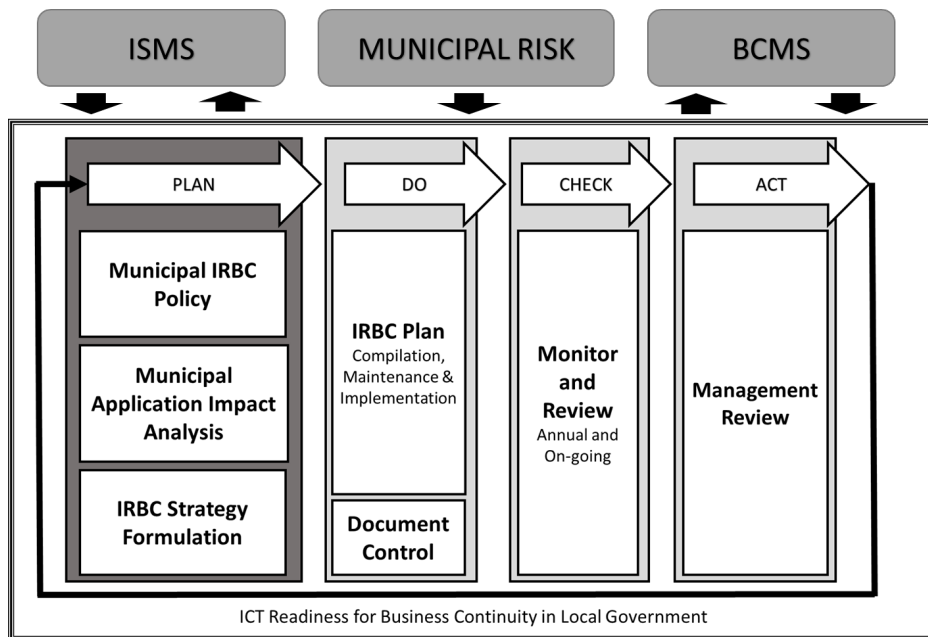


Figure 5.4: Final Theoretical Foundation.

### Municipal Risk

Starting with the external components of the theoretical foundation, the first major component is that of ‘Municipal Risk’. As discussed in Subsection 2.2.2, ICT is vulnerable to a multitude of different threats which, if realised, can cause harm to ICT systems and impact negatively on a municipality’s reputation. IRBC, therefore, acts as a means to mitigate many of the risks that could lead to ICT disruption. Furthermore, the ISO/IEC 27031 (2011) supports this notion and states that IRBC should enable the municipality to respond to the constantly changing risk environment. ‘Municipal Risk’ should, therefore, be considered as a vital input and driving force, towards the implementation and operation of municipal IRBC.

### BCMS

The second external component which interacts with IRBC is that of the municipal BCMS. During the first refinement iteration, the stakeholder emphasised that many lower-capacity municipalities do not have and in many cases are incapable, of implementing a BCMS. Although the standard for IRBC was written to supplement and integrate with a BCMS, Marbais (2012) states that enterprises frequently want to implement mitigation, response and re-

covery measures in advance of a broader business continuity management programme. This would be the case in most of the resource-scarce municipalities, who do not have the capacity to implement a proper BCMS but still require a resilient ICT environment.

It is due to this reason that M-IRBC followed the route of IRBC. The theoretical foundation caters for those municipalities, amongst others, who want to and can implement a BCMS. In that case, there will be an interaction between the BCMS and the IRBC programme, as each system requires certain input and output from each other. However, IRBC can function in isolation, which essentially means that there are no critical dependencies between these systems, even though the associated standard recommends IRBC be implemented as part of a broader BCMS. The BCMS component in this theoretical foundation is, therefore, optional, which caters for the ‘smaller’ low-capacity municipalities.

## **ISMS**

The final external component for IRBC in municipalities is the ISMS. An ISMS aims to safeguard the CIA of enterprise information (ISO/IEC 27000, 2012). This information resides on the ICT systems of every municipality. Thus, it is critical to ensure collaboration between the IRBC and ISMS activities to not only allow the availability of information but also support its confidentiality and integrity. Although the stakeholder did not identify the ISMS in the same way it did with the BCMS, M-IRBC still has to consider the possibility that a municipality might not have a full ISMS.

However, in this case, the CIA of the municipal information remains critical regardless of an ISMS. Therefore, it is important that the municipality, regardless of its resource capabilities, cater for the CIA of the information, especially where backup and redundant systems are involved in the IRBC activities. These systems should be secure, and the information on it, protected. In the cases where the municipality does have an ISMS, these systems co-exist and interact. The IRBC programme works towards the availability aspect of the information protected by the ISMS, whilst the ISMS works towards the confidentiality and integrity of the information within the IRBC backup and redundancy systems.

### **Municipal IRBC Life-cycle**

Moving into the IRBC system itself, Figure 5.4 illustrates each of the Plan-Do-Check-Act phases as a cycle, where each phase includes various components. Section 2.4.1, briefly discusses the Plan-Do-Check-Act approach. It highlights how this approach is repetitive in nature and allows the IRBC system to adapt to an ever changing risk environment. The Plan-Do-Check-Act approach, therefore, allows for continuous monitoring and improvement of the municipal IRBC system. A review as part of the Check-phase may lead to management acting on some issue and setting in motion another cycle of the approach.

### **Municipal IRBC Policy**

The IRBC policy falls within the Plan-phase. Section 2.4.2, briefly discusses the IRBC policy and the various topics that need to be addressed within the policy. In the case of municipalities, the policy initiates the municipal IRBC system as a whole and forms the directive on what is expected from municipal IRBC. Based on the feedback from the stakeholder, the first challenge will be to have the IRBC policy accepted at the council. Once council accepts the policy, the person responsible should have the necessary resources to continue the planning towards implementation.

The municipal IRBC policy is therefore written at a very high level, with the least amount of technical detail, in order to facilitate adopting the policy at the council level. Essentially, the policy provides objectives and guides further requirements that need to be achieved. Any undertaking which follows during the IRBC life-cycle has to be able to measure itself to the objectives and requirements stated in the policy. Furthermore, the policy should delineate the appropriate scope of the municipal IRBC and appoint responsible persons, especially with regard to authorities that provide resources for IRBC implementation. Lastly, the policy should be reviewed at planned intervals. Upon acceptance of the IRBC policy, an impact analysis should be conducted.



### **Municipal Application Impact Analysis**

During the process of planning the enterprise IRBC system, due to the fact that the IRBC system ideally integrate with the enterprise BCMS, the enterprise would have conducted a business impact analysis. Section 2.4.2 discussed the principles of a business impact analysis. In essence, this function categorises different business functions according to its priority for continuity. This includes setting MBCOs, that include RTOs and RPOs. However, in the case of the municipal IRBC system, the theoretical framework has to cater for municipalities who do not have a BCMS and therefore would not have conducted a business impact analysis.

Marbais (2012) states that a simple way to develop the MBCO required by IRBC, when implementing IRBC apart from a BCMS, is to conduct a more focused application impact analysis (AIA). The AIA takes a systems-based approach instead of a business function approach, in that the focus lies with the systems supporting various business functions. Epstein and Khan (2014) explain that an AIA is a simple science of material impact, for a service or process not being available. The higher the impact the loss of the systems might have, the quicker that system has to be able to recover. Furthermore, the AIA sets the stage for business and ICT to align, in agreeing on the recovery priorities, to restore certain processes in the event of a disruption (Epstein & Khan, 2014).

Epstein and Khan (2014) state that the AIA must be completed for all the application systems. They state that by taking a risk-based approach, the AIA identifies applications systems and its associated critical processes. This is a systematic and efficient means to identify and update the continuity requirements of all the business functions within the enterprise, thus providing a clear picture on where to focus recovery efforts, should a disruption occur (Epstein & Khan, 2014). Essentially, with regard to its continuity objectives, this process should address the gap between what the municipality requires, and what ICT can deliver. In order to achieve the set MBCOs determined during the AIA, the municipality must develop an appropriate IRBC strategy accordingly.

## **IRBC Strategy**

As discussed in Section 2.4.2, the IRBC strategy defines the approaches that need to be implemented, in order to enhance ICT resilience. Importantly, the chosen strategies should be able to deliver and meet the MBCOs defined during the AIA. The various strategy options are divided into the six IRBC elements. These IRBC elements, not to be confused with the elements of the integrated research process, include: people, facilities, technology, data, processes and suppliers, and are described in Table 2.3.

These elements form the foundation of the strategy around which IRBC will ultimately achieve its goals. Each element has different strategy options to choose from, and the municipality can choose more than one strategy per element if it so desires. However, within the municipality, resources will have to be granted to implement these strategies. Therefore, careful consideration should be taken with regard to available resources when choosing strategy options.

As part of the overall planning of IRBC it is critical that the municipal IRBC be aligned to the ISMS and BCMS - should they exist. As an example, regarding municipal information, the CIA of the information being stored, backed-up and recovered, should be preserved - a process directly attributed to the ISMS. The strategy involved with the 'data'-element of IRBC, will, therefore, have to align with the controls in the ISMS.

The ability to choose different strategies within each IRBC element greatly assists in personalising the IRBC system to each unique municipal ICT environment and resource capacity. Upon drafting the IRBC strategy with its different options, implementation of the chosen strategies can commence as part of the Do-phase, and an IRBC plan is developed.

## **IRBC Plan**

The IRBC plan and its requirements were discussed in detail within Section 2.4.2. Ultimately, the IRBC plan, depending on the size and resource capacity of the municipality, will be a document or set of documents, outlining how the municipality will manage disruption to ICT and essentially enable a resilient ICT environment. The IRBC strategy, at a high level, dictates the various strategies the municipality plan on implementing in order to achieve

resilience. The IRBC plan is essentially a detailed implementation of the IRBC strategy.

The IRBC plan defines the processes of how the various strategies are enabled. This may include response and recovery plans for various systems. The MBCOs, RTOs and RPOs will be outlined within the plan, as well as clear roles and responsibilities. Procedures for invoking the IRBC plan should also be clearly defined.

As stated in Section 2.4.2, the IRBC plan should delineate, (1) how to mobilise the assigned individual or team, (2) immediate assembly points, (3) subsequent team meeting locations and any alternate meeting locations, and (4) circumstances which the enterprise deems unnecessary for IRBC response, such as minor faults and outages managed by the help-desk.

The components discussed in this section, form the primary components of the municipal IRBC system, part of the theoretical foundation. As part of the Check-phase, various testing, monitoring and reviewing activities occur, to see whether the IRBC system, adheres to the requirements set within the IRBC policy. Should any inadequacies be identified, management can ‘Act’, and set in motion a new refinement cycle of the whole IRBC system for it to be updated - in effect completing the whole Plan-Do-Check-Act cycle. The second part of M-IRBC is discussed in the following subsection.

### 5.3.2 Tool-set for IRBC Planning

As stated before, the M-IRBC theoretical foundation is supported by a tool-set. Unfortunately, due to the technical nature of IRBC as a whole, the supporting tool-set only provides municipalities assistance with the Plan-phase of the municipal IRBC system. As seen in Figure 5.4, the Plan-phase is highlighted in a darker shade of grey, indicating the components that are supported with the tool-set.

Figure 5.5 illustrates a process for the supporting tool-set. The tool-set consists of three exercises and, upon completion, delivers four tangible outputs. Three of these outputs, namely: an IRBC policy; a list of systems categorised according to their MBCOs; and an IRBC strategy document, all form part of the major components of the IRBC Plan-phase. The last output from the supporting tool-set, is a reference guide, which aims to further assist the municipality, through directing them to the necessary information they

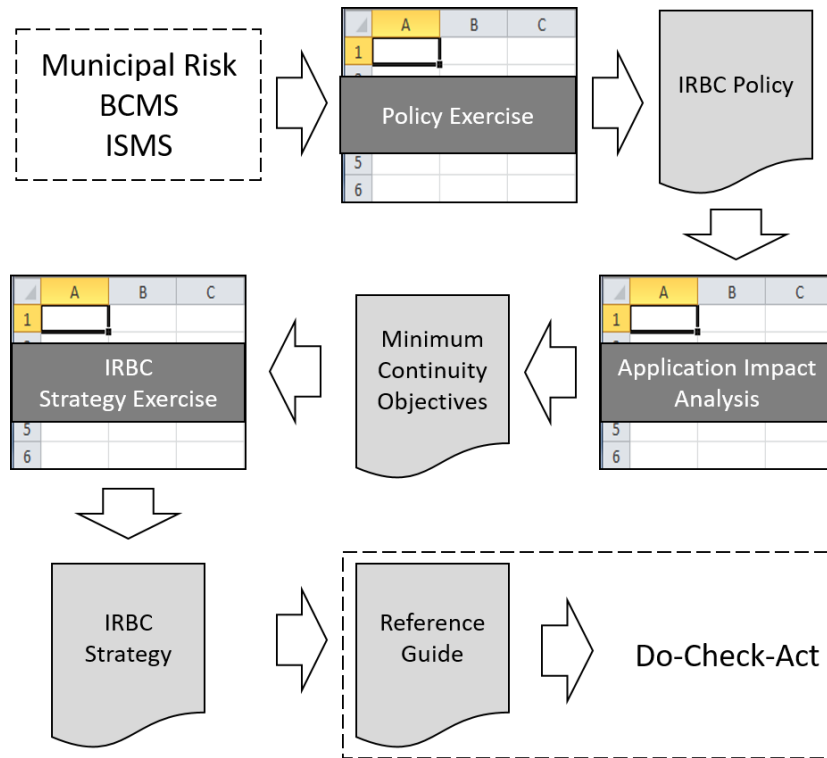


Figure 5.5: Tool-set for IRBC Planning

will require when they move on to the Do-Check-Act phases of the life-cycle.

As part of the entire theoretical foundation, any requirements from the external components are considered when starting with the first exercise. The IRBC policy exercise, reverse engineers certain principles and requirements that are critical to effective IRBC and provides them as statements to which the user must agree or disagree. The IRBC policy exercise is attached as Appendix C.1 and is partly illustrated in Figure 5.6. By agreeing with a statement, a policy statement will be generated and inserted into the policy. This process enables the tool to provide a unique policy, based on the answers given. This avoids generating a static policy that would not be unique to the specific municipality, therefore making it applicable to different municipalities.

The user should either agree or disagree with certain statements within the exercise. Relevant reasons will be provided about why the said statement is important to IRBC, but the tool ultimately allows the user to omit the resulting policy statement. However, the user will have to provide sufficient justification as to why the statement should be omitted within a ‘policy-

Principles Exercise for the ICT Readiness for Business Continuity Policy				
The following exercise serves as a precursor to the Municipal ICT Readiness for Business Continuity Policy. The following statements represent important principles or criteria that are included in the Policy. Should you definitely disagree with any of the following statements, the "Policy Omissions" worksheet will provide instructions as to which policy statements or sections to omit from the policy. You will however be required to give relevant accountability for each omission. Read through the given statements and indicate in Column C whether you agree. Should you disagree a relevance message will appear in the adjacent cell within Column D. You may change your decision or subsequently agree to omit the statement using the option in Column E (Note: by agreeing with the statement, it will automatically be included in the policy - indicated by a NO in Column E).				
#	Statements:	Do you agree with this statement:	Why is this important?	Do you wish to omit the resulting policy statement or section regarding this principle/criteria?
1	Disruptions to ICT can constitute strategic risks to the reputation of the municipality and its ability to operate.			NO
2	It is critical to develop and implement a readiness plan for the continuity of ICT systems, to ensure that the municipality has a resilient ICT environment which also support the municipal ISMS, BCMS and Risk mitigating activities.			NO
3	The municipality acknowledges the benefit of being compliant with international best practice with regard to its ICT Readiness objectives			NO
4	In order for the municipality to achieve ICT Readiness for Business Continuity (IRBC), it needs to put in place a systematic process to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services.			NO

Figure 5.6: IRBC Policy Tool: Exercise

omissions' worksheet, partly illustrated in Figure 5.7 and found in Appendix C.1. Once justification is provided for all omitted statements, the user will be granted access to the generated policy (See Appendix C.2), with the justification statements to insert where applicable. Once the policy is accepted at the council, the responsible person can commence with the AIA. As ex-

Policy Omissions				
This worksheet lists any IRBC policy statements with its corresponding section in the IRBC policy, of statements you chose to omit. Any statement/s you chose to omit from the IRBC policy, should be erased and replaced with a statement of applicability, within the policy, confirming that the municipality accepts the omission.				
#	Omitted?	Please provide a statement of applicability:	Remove the following statement in the policy:	Section:
1	DEFAULT			
2	DEFAULT			
3	NO			
4	NO			
5	NO			

**Example:**  
The municipality does not make use of international standards, as it rather relies on the knowledge of municipal staff.

Figure 5.7: IRBC Policy Tool: Omissions Worksheet

plained before, the objective of the AIA is essentially to align municipal needs with ICT capability. The AIA exercise provides a simplified platform, in a spreadsheet layout, in which the various system impact data can be captured. The AIA exercise tool is attached as Appendix C.3. The tool provides the

user with a predetermined list of systems that should be present in most municipalities. This list was collected from the stakeholder during Phase 3 of the research process. These systems act as the starting point from which the AIA can commence. A portion of the AIA exercise is depicted in Figure 5.8, showing the list of predetermined systems. Guidance is provided throughout the process at each step. The user is further aided by options in drop-down lists, to decide for example on impact ratings, from ‘no-impact’ to ‘severe-impact’, as well as options for the RTOs for critical systems.


#	Municipal Business Function reliant on ICT	Do you regard this business function critical to the daily operation of your municipality?	On a scale between 1 (None) and 6 (Severe), what impact would the unavailability of this function have on your municipality?	Related ICT System (Hardware/Software)
	Identify activities or functions that support the delivery of key services that should be included in the municipal IRBC.	Information regarding the criticalness of a certain business function can come from interviews, questionnaires and workshops etc. with the relevant stakeholders.	The municipality should address impacts relating to its aims and objectives, and interested parties. These may include: Adverse effects on staff or public well-being; Breach of regulations or SLA's; Damage to reputation; Financial loss; Deterioration of service quality; and environmental damage.	Fill in the related systems applicable to your municipality. Utilities such as electricity and telecommunications should also be taken into account and relevant strategies implemented for these utilities.
1	Vehicle Registration		<input type="text" value="1"/>	e-NATIS; LAN; WAN
2	Personnel Management / HR			CAPMAN; PROMUN; ORGPLUS; LAN;
3	Finance Management			PROMUN; Excel; LAN; WAN
4	Research (Legal)			LexisNexis; LAN; WAN
5	Contract Management			Collaborator; LAN
6	Library Services			PALS; LAN; WAN
7	Customer Service			PROMUN; LAN; WAN
8	Reporting			Microsoft Office Suite; LAN
9	Research (General)			Internet browser; LAN; WAN
10	Traffic Administration			TCS; LAN; WAN
11	Water Care			Adroit Telemetry system; LAN; WAN

Figure 5.8: Application Impact Analysis Tool

The outcome of the AIA is a list of municipal business functions or activities, reliant on ICT systems, sorted from most critical to least critical with its recovery objectives defined. Through a process of collaboration with various municipal business functions and managers, in the form of questionnaires and interviews, the recovery objectives of ICT systems can be aligned with the needs of the municipality and capability of current ICT systems. The end result is a list of critical ICT systems, and their corresponding recovery objectives. This list of categorised ICT systems, provides direct input to the IRBC strategy formulation exercise.

The IRBC strategy exercise provides a comprehensive spreadsheet-tool, dividing various strategy options into its relevant IRBC elements. Guidance and sufficient explanation of each element and strategy option are provided throughout. This is partly illustrated in Figure 5.9 where three of the IRBC

elements are shown with some of their strategy options. The user is enabled to pick relevant strategies, based on the requirements from the AIA and the resources made available for the IRBC project. A list of the selected strategies and an explanation of each is then generated. This generated strategy will form the foundation from which the IRBC plan will be developed and implemented. The IRBC strategy exercise is attached as Appendix C.4.

	People: Skills & Knowledge		Facilities		Technology	
	The specialists with appropriate skills and knowledge, and competent backup personnel.		The physical environment in which ICT resources are located.		1) hardware (including racks, servers, storage arrays, tape devices and fixtures); 2) network (including data connectivity and voice services), switches and routers; and 3) software, including operating system and application software, links or interfaces between applications and batch processing routines;	
Strategy Description:	The municipality should identify appropriate strategies for maintaining core ICT skills and knowledge. This may extend beyond employees to contractors and other stakeholders who possess extensive ICT specialist skills and knowledge.		According to identified risks, the municipality should devise strategies for reducing the impact of the unavailability of the normal ICT facilities.		The ICT services upon which critical business activities depend should be available in advance of the resumption of their dependent critical business activities. Technology platforms and application software should be put in place within timescales demanded by the municipality as a whole.	
Strategy Options:	Strategy:	Selection:	Strategy:	Selection:	Strategy:	Selection:
	Documentation of the way in which critical ICT services are performed		Alternative facilities (locations) within the organization, including displacement of other activities		Hot standby, where ICT infrastructure is replicated across two sites	
	Multi-skill training of ICT staff and contractors to enhance skill redundancy		Alternative facilities provided by other organizations		Warm standby, where recovery takes place at a secondary site where ICT infrastructure is partially prepared	

Figure 5.9: IRBC Strategy Exercise

Once the IRBC strategy is generated, the main components that form the Plan-phase of the municipal IRBC system, are complete. As stated before, due to its technical nature, the supporting tool-set, can only assist the municipality with the Plan-phase. However, as part of the tool-set, the municipality is provided with a reference guide (See Appendix C.5), to assist in the development of the IRBC plan, and the rest of the activities within the remaining Do-Check-Act phases. In conclusion, the theoretical foundation, supported by a tool-set, forms the complete method towards IRBC in local government (M-IRBC).

## 5.4 Conclusion

This chapter proposes a method towards IRBC in local government, called M-IRBC. M-IRBC comprised of a theoretical foundation and a supporting

tool-set, which aims to address the challenges with ICT continuity in municipalities. M-IRBC is the output to the goal of the research process, defined in Chapter 4, to deliver an artefact.

The artefact in the form of a method, was developed and refined over the course of three phases, in collaboration with stakeholders, as part of the integrated research process of this study. This chapter therefore reported on each of the research phases, and outlined the evolution of the method through various refinement iterations, until it was deemed acceptable by the stakeholder.

The finalised method towards IRBC (M-IRBC) was then presented, discussing each of the components of the theoretical foundation. This was followed by an explanation of the supporting tool-set, aided by a process model, which supports the theoretical foundation and aims to help municipalities with *HOW* they can implement IRBC and achieve a resilient ICT environment. The following chapter will report on Phase 4 of the integrated research process, which deals with the validation of the method.



# Chapter 6

## Artefact Validation

*The goal of this chapter is to report on the validation of the method towards IRBC in local government (M-IRBC). It begins with a discussion around the data collection approach. This is followed by an analysis of the results, structured around M-IRBC's design criteria. Lastly, the primary findings are discussed. Ultimately, this validation determines whether M-IRBC adheres to the design criteria. Adhering to the criteria results in M-IRBC being regarded as appropriate to be used within municipalities.*

### 6.1 Introduction

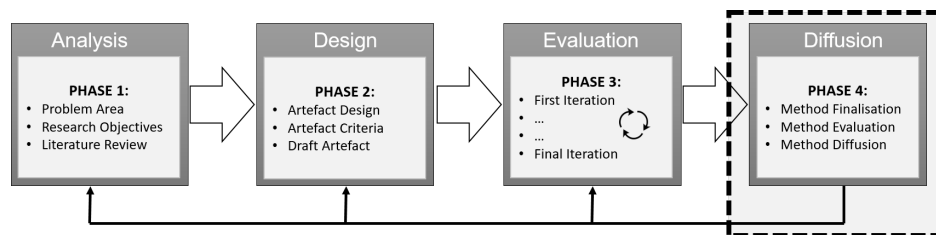


Figure 6.1: Phases Towards Finalising the Method: Phase 4

The objective of this study is to construct an artefact in the form of a method, to help address the problem with ICT continuity in local government. The integrated research process (Chapter 4) provided the platform from which this objective could be reached - pending adherence to the principles of the design-oriented IS research paradigm. The outcomes from the first three phases of the four-phased integrated research process were dis-

cussed in Chapter 5. This chapter reports on Phase 4 of the integrated research process. This phase is highlighted in Figure 6.1.

Phase 4 is associated with the validation and diffusion of the completed artefact. The artefact delivered by this study, as discussed in Chapter 5, is a method towards IRBC in local government (M-IRBC). As part of Phase 1 to 3, M-IRBC was developed, finalised and deemed acceptable by the stakeholder. Phase 4, therefore, includes validating M-IRBC against the design criteria - defined within Phase 2. This will ascertain whether M-IRBC adheres to these criteria, which are: *Scalable*, *Simplistic*, *Comprehensible* and *Usable*.

This chapter will, therefore, discuss the data collection approach followed during this validation process, including the design of the data collection instrument and the setting in which the data collection occurred. This is followed by an analysis of the results and lastly consolidating these results into the most notable findings.

## 6.2 Data Collection

To facilitate the completion of Phase 4, as illustrated in Figure 6.1, a workshop was hosted for the purpose of validating M-IRBC. The workshop spanned two days, the 25<sup>th</sup> and 26<sup>th</sup> of April 2016. A total of 22 representatives, primarily from the ICT function of different municipalities, attended the workshop. It should be noted that these representatives were not from the original stakeholder municipality, who partook in Phases 1 and 3. These representatives were primarily from the ‘poor resources and low-capacity’ category of municipalities. The design criteria against which the M-IRBC is validated in this chapter, were largely formulated around the challenges faced by municipalities that fall into this category. Therefore, representatives from these municipalities were deemed most appropriate.

Regarding the workshop design, each day consisted of a theoretical background session, followed by a practical session. Each municipal representative received a fully functioning copy of the M-IRBC’s supporting tool-set. During the theoretical background sessions, the attendees were presented components from the M-IRBC theoretical foundation and had the opportunity to ask questions throughout. A practical session followed the theory

sessions. During the practical session, each attendee had the opportunity to use the M-IRBC supporting tool-set and work through the different exercises, as illustrated in Figure 5.5. The aim of each practical session was for each attendee to work on the various exercises within the supporting tool-set as if they were conducting it for their own municipality.

Table 6.1: Questionnaire Design

Criterion	Question	Statement
<i>Scalable</i>	4	The M-IRBC allows IRBC to scale to the size and resource capacity of a municipality.
	6	The M-IRBC can be equally successful in both larger and smaller municipalities.
<i>Simplistic</i>	3	It is possible to complete the exercises in this M-IRBC without extensive guidance or knowledge about the subject area.
	5	A person with limited technical ability would be able to successfully complete the tool-set exercises.
<i>Comprehensible</i>	2	In general, the concept of IRBC becomes clear and understandable throughout the M-IRBC process.
	7	A person without prior knowledge about IRBC would be able to comprehend the goals and objectives of what IRBC strives to achieve upon completing the M-IRBC exercises.
<i>Usable</i>	1	The M-IRBC and its exercises would be compatible to function in any municipality.

Upon completion of the practical sessions, as part of a survey, each representative completed a questionnaire, which can be seen in Appendix B.2. The objective of the questionnaire was to test whether M-IRBC adheres to the criteria defined within Phase 2 and ultimately validate its suitability for the municipal environment. The questionnaire was set up to consist of various statements. Each statement tested adherence for a different criterion. Table 6.1 indicates the various closed-ended statements included in the questionnaire, as well as which criterion each statement evaluated.

The respondents had to indicate whether they agree or disagree with the

particular statement using a Likert scale. The scale included four options, namely: strongly disagree; disagree; agree and strongly agree. Figure 6.2 illustrates an example of the scale with one of the questionnaire statements. In conjunction with the seven statements, the questionnaire also included three open-ended questions, where representatives could indicate whether M-IRBC were lacking anything, needed improvement in some areas, or anything positive that they had identified. The results from the questionnaires are reported in the next section.

4. The IRBC spreadsheet-based tool-set allows IRBC to scale to the size and resource capacity of a municipality.			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 

Figure 6.2: Example of Questionnaire Answer Scale

## 6.3 Data Analysis and Results

As seen in Table 6.1, the questionnaire validating M-IRBC included statements testing the artefact against the design criteria. This section, therefore, reports on the results per criterion. Each subsection will briefly reiterate the primary reason for the criterion and present the results of the questionnaire.

### 6.3.1 Scalability

The criterion ‘*Scalable*’, is probably the most crucial in the context of South African municipalities. As discussed in Chapter 3, in an attempt to improve municipal ICT, the MCGICTP is directed from the national government to all municipalities regardless of size or resource capacity. However, the MCGICTP is unfortunately not a one-size-fits-all policy. As stated by the primary collaborative stakeholder, low capacity municipalities will have major resource capacity challenges when attempting to implement the MCGICTP. Thus, to address the problem with ICT continuity, M-IRBC had to allow a scalable solution.

The scalability provided by M-IRBC results in the municipality being able to plan IRBC according to their capability and implement the most

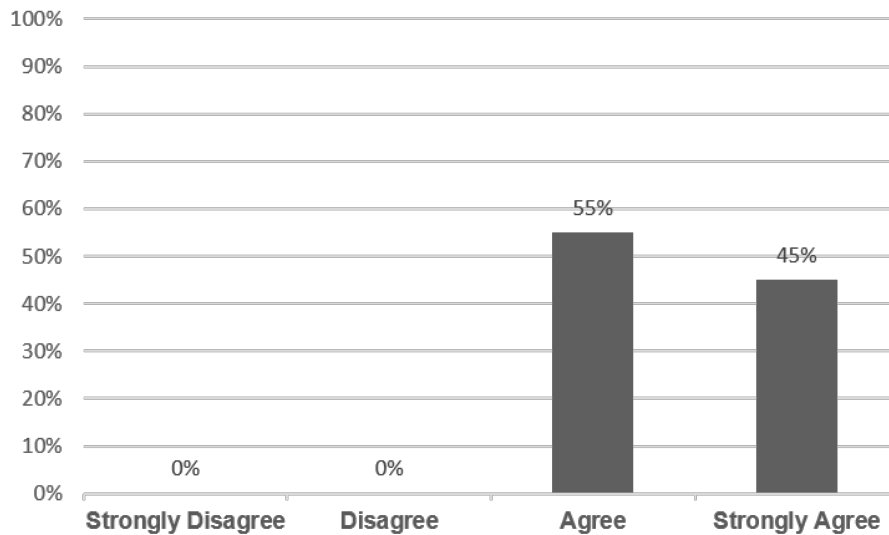


Figure 6.3: Results for the Criterion: Scalable

critical components. They are able to decide on strategy options that fit to their financial, skills and human resources. Two statements in the questionnaire tested for scalability. The graph in Figure 6.3 illustrates the results. From the 22 respondents, 55% agreed that the method is scalable to any size and resource capacity municipality, whilst 45% strongly agreed. With this criterion, the results are completely leaning towards the positive side of the scale, with none of the respondents disagreeing to this criterion in any of the statements.

### 6.3.2 Comprehensibility

M-IRBC has to be comprehensible. This criterion does not necessarily directly link to a specific identified issue in local government. Although it does align closely to the criterion of *Simplistic*, discussed in the next subsection. ‘*Comprehensible*’, rather, stems from the fact that IRBC in itself is regarded as a fairly unknown approach to ICT continuity and recovery, therefore, requiring a good understanding. Comprehensible, in this context, thus translates to the ability of the relevant person to comprehend the role IRBC plays within the ICT function and municipality as a whole; as well as understanding how the various components relate and interact to form the entire IRBC system.

Essentially, the municipality should easily understand what they are implementing, when they are implementing it. A simple example would be for instance when the responsible person is conducting the AIA, this person has to know why it is taking place and where the output will be required. Therefore, for this criterion, there has to be an understanding of the entire IRBC system as a whole, which leans heavily on the M-IRBC's theoretical foundation.

The results for this criterion were a little more dispersed. Based on the two questions related to this criterion, 9% of the respondents disagreed that the method is comprehensible. However, a combined 91% either agreed or strongly agreed that the method is comprehensible. These results are illustrated in Figure 6.4.

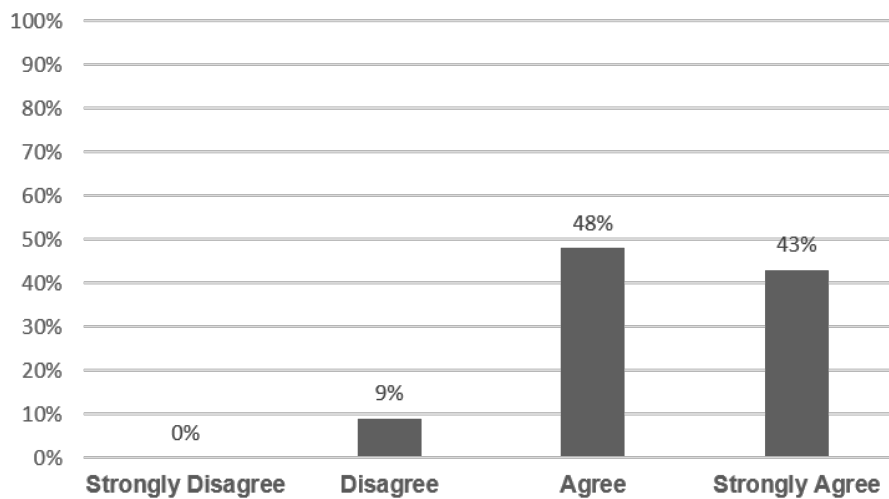


Figure 6.4: Results for the Criterion: Comprehensible

### 6.3.3 Simplicity

The criterion '*Simplistic*' does align to that of '*Comprehensible*' but addresses a slightly different challenge. Various problems around human- and skill-resource capacity become evident from the collaborative stakeholder feedback, as well as findings from literature. Essentially, some municipalities may have an ICT function run by a single ICT professional. In such a case, there will be limited personnel to do the work necessary for IRBC implementation. This specific person may also not have the specialised skills or

knowledge around the area of ICT continuity and recovery. Therefore, the method towards IRBC and especially the supporting tool-set, has to be simplistic.

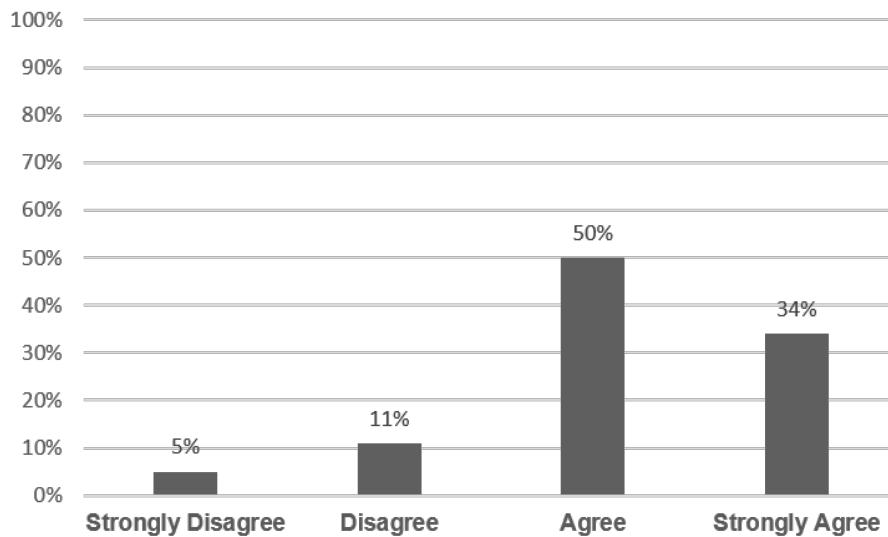


Figure 6.5: Results for the Criterion: Simplistic

Simplistic goes hand-in-hand with the criterion of comprehensible to allow for the process of implementing IRBC to not require a specialist in the field of ICT continuity to effectively implement it. With regard to this criterion, 50% agreed that M-IRBC is simplistic, while 34% strongly agreed. A total of 16% either strongly disagreed, or disagreed with this contention. The results for simplistic are illustrated in Figure 6.5.

### 6.3.4 Usability

The criterion ‘Usable’, is mainly attributed to the M-IRBC supporting tool-set. It is evident, based on the feedback from the collaborative stakeholder and literature that municipalities differ. The constitution makes municipalities self-governing entities and they can, therefore, decide how they wish to operate, which may result in different ICT environments and systems. Therefore, the method towards IRBC and in this case specifically the supporting tool-set, has to be usable in any municipal ICT environment.

The medium used to support the theoretical foundation of M-IRBC could come in various formats. The usability of a customised computer program

compiled in a specific programming language would be highly restrictive in municipalities. The municipality using the program would have to run a specific operating system and possibly require other supporting operating system specific software. This would result in M-IRBC not being usable in any South African municipality. Therefore, this study proposes a supporting tool-set, which includes the use of word processing applications and various spreadsheet-based exercises. M-IRBC would therefore, be usable in any municipality as long as they have these programs installed, regardless of hardware or operating system.

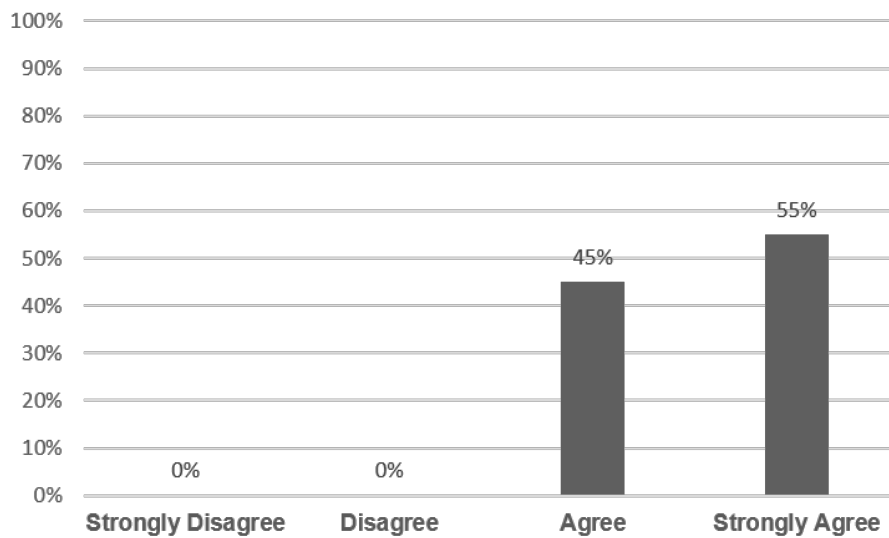


Figure 6.6: Results for the Criterion: Usable

Figure 6.6 illustrates the results for this criterion. A total of 55% of the respondents strongly agreed that the spreadsheet-based tools will be usable in their municipality, whilst a further 45% agreed. None of the respondents disagreed to any extent about the supporting tool-sets' usability.

As mentioned before, the questionnaire also included open-ended questions. Feedback from the open-ended questions was primarily good, with most respondents giving positive feedback. The most notable responses include:

- “The M-IRBC would benefit municipalities and help with their ICT continuity challenges”



- “The M-IRBC is complex for someone with no knowledge about ICT and disaster recovery”
- “It would be nice if the technical implementation aspects of IRBC could be included in the tool-set”
- “Clarity is needed on how district municipalities and local municipalities can interact, due to many local municipalities relying on district municipalities for ICT continuity”

The findings from the questionnaire results will be discussed below.

## 6.4 Findings

The results discussed in the previous section provided a good overview of the questionnaire outcomes for each of the criteria. The questionnaire results indicated that all of the criteria, i.e.: *Scalability*, *Simplicity*, *Comprehensibility* and *Usability* tested positive, with the overwhelming majority of the respondents either agreeing or strongly agreeing that M-IRBC satisfies each criteria. Both scalability and usability received a 100% agree or strongly agree response; whilst comprehensibility received 91%. With regard to the principle of simplicity, 16% disagreed that M-IRBC was simplistic, whilst the overwhelming majority of 84% agreed. These findings are illustrated in Figure 6.7.

Although the results are generally very good, there were a few results which contained a small percentage of respondents who did not agree with the given statements. These responses involved the criteria of simplistic and comprehensible. Although the amount of respondents who disagreed were very low, a look at the questionnaires’ sample population provides some explanation. Information regarding the sample population was important in order to understand the results and analyse the results from a suitable perspective. To know more about the population, the attendees had to answer a few general questions beforehand, not pertaining to the artefact.

Some of the findings from these questions indicated that not all of the attendees, sent by their municipalities, were from a pure ICT background. Three of the representatives did not come from an ICT background whatsoever, and mainly stemmed from a general audit and risk background. The

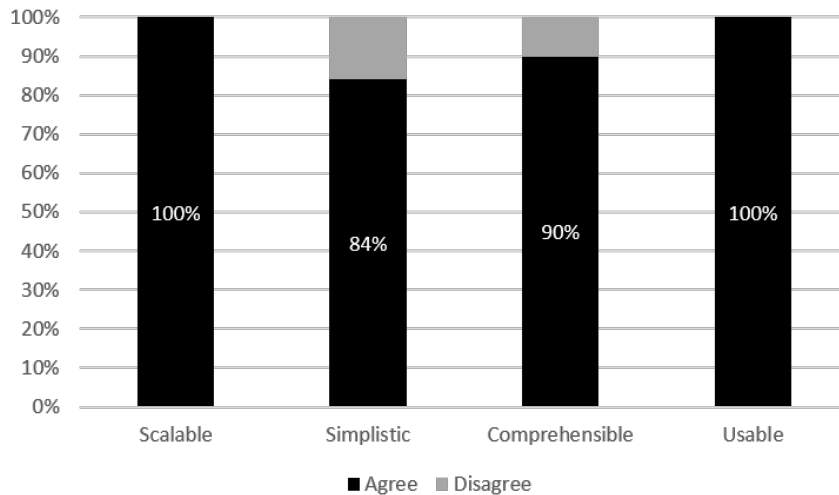


Figure 6.7: M-IRBC's Overall Adherence to Criteria

representatives were also asked whether they were familiar with IRBC and the ISO 27031 standard prior to the workshop, whereupon 73% responded that they were not familiar with IRBC at all. This most probably explains why the criteria of comprehensible and simplistic, due to the technical nature of IRBC, had negative responses.

Linking to the criterion of simplicity, and to confirm the findings around the scalability of the method towards IRBC, the respondents were asked how many employees worked in their respective ICT departments. On average, the ICT departments of the attendee municipalities consisted of merely three staff members, with many of them being a single-person run ICT function, which definitely speaks to the human resources available, and size of the ICT department, in many municipalities.

Taking into account the results as a whole, the overall feedback is very positive; and it indicates that the criteria have largely been satisfied, and that especially low-capacity municipalities would greatly benefit from using M-IRBC.

## 6.5 Conclusion

This chapter validated the proposed M-IRBC against the design criteria set during Phase 2 of the integrated research process. In doing so, this chapter

addressed Phase 4 of the integrated research process, and ultimately concluded the research process.

Firstly, this chapter discussed the data collection method, which was a survey in the form of a questionnaire. A two-day workshop was hosted where the survey was conducted with representatives from various municipalities. The questionnaire aimed to measure whether the criteria of *Scalable*, *Simplistic*, *Comprehensible* and *Usable*, were satisfactorily incorporated into M-IRBC. The results from the questionnaire were discussed on a per-criteria basis. Lastly, the findings from the questionnaire were discussed and indicated an overwhelming positive response to M-IRBC. At this stage, information regarding the sample population was also outlined to explain some of the results, as well as support the findings regarding the criteria.

Resultantly, this chapter concluded that M-IRBC did indeed meet the criteria it aimed to adhere to. Thus, M-IRBC can be regarded as appropriate within local government even considering all of the challenges faced by municipalities within this sphere. The following chapter concludes this study by summarising the main findings and contributions made, whilst also indicating how this study complied to the principles of the design-oriented IS research paradigm.

# Chapter 7

## Conclusion

*This chapter will conclude this study by summarising the main findings and discussing how the objective of this study was addressed. Furthermore, the various contributions from this study will be highlighted, whilst also indicating how the study adhered to the principles of the research paradigm. Lastly, some suggestions for future research will be made before sharing some final words in concluding this study.*

### 7.1 Introduction

The pervasive nature of ICT and its strategic importance to the modern enterprise is evident. Enterprises, including government, have realised the benefits ICT delivers if utilised effectively. The availability of ICT is therefore of utmost importance to reap the full benefits.

This study has highlighted the fact that ICT is a critical enabler for service delivery within the South African local government and therefore, the availability of ICT in local government is crucial. However, it was found that municipalities in this government sphere struggle with the design and implementation of ICT continuity to enable this level of availability.

This study has proposed an artefact, titled M-IRBC, to address this problem situation. This chapter, therefore, summarises the findings and indicates how the study reached its intended objective. The contributions of this study will also be discussed, whilst highlighting how the study adhered to the design-oriented IS research paradigm principles. Suggestions for future research will be made, followed by some final thoughts.

## 7.2 Summary of Findings

ICT is core to municipalities' endeavour to deliver sustainable services to their communities. As such, these ICT systems have to be resilient. However, it is evident that a majority of municipalities in South Africa experience challenges with designing and implementing ICT continuity controls. Many of these municipalities lack the specialised skills or financial and administrative resources to do so. There also seems to be some confusion and different opinions regarding the various continuity concepts and their inter-relationships.

As technology evolved throughout the information age, it required that measures ensuring the availability of ICT also evolve. The shift from a reactive approach to ICT continuity, focussing on post-incident disaster recovery measures, to a proactive approach promoting pre-incident resilience of ICT, is evident from the discussion in Chapter 2. Whilst enterprises are focusing on enterprise-wide resilience through their BCM initiatives, IRBC aims at achieving a resilient ICT environment, within the BCM framework.

Chapter 3 elaborated on the problem situation identified in Chapter 1, and further discussed different government policies and frameworks aimed at properly governing ICT in government entities, including municipalities. However, it is emphasised that these government initiatives like the CG-ICTPF, SALGA guidelines and the MCGICTP, provide direction on *WHAT* must be done, but little guidance on *HOW* it can be done.

Furthermore, Chapter 3 investigated why these government policies and frameworks, as well as the availability of international standards and best practices, have proven to be ineffective in municipalities. Resultantly, it becomes clear that many municipalities fall within the 'poor resources and low-capacity' category of municipalities. Essentially, they do not have the necessary financial, skills or human resources to implement these policies and these municipalities require assistance, by means of a tailor-made approach, that fit their unique challenges. To this end, criteria was defined which would guide the development of such an approach.

In order to achieve the objective of this study and address the set problem by assisting municipalities with their ICT continuity efforts, Chapter 4 outlined the research approach. As a result, within the scope of the design-oriented IS research paradigm, a unique integrated research process was de-

defined with the intention to design an artefact in the form of a method, which adheres to the specific criteria identified in Chapter 3, to address the problem.

Chapter 5 discussed the first three phases of the integrated research process and in doing so provided insight into how the method towards implementing IRBC in municipalities materialised. The method towards IRBC in local government, titled M-IRBC, was proposed. M-IRBC consists of two components, namely: a theoretical foundation and a supporting tool-set. M-IRBC was developed with the criteria, defined in Chapter 3, in mind. Adhering to these criteria would make M-IRBC more suitable to the unique municipal environment in that it considers the challenges municipalities face and attempts to work around them.

To ascertain whether M-IRBC adhered to the criteria it was important to properly validate it. Chapter 6 reported on the validation of M-IRBC that was done through conducting a workshop with municipal representatives from the ‘poor resource and low-capacity’ category of municipalities. Data was collected using a survey in the form of a questionnaire. It was established that M-IRBC predominantly met the defined criteria and that it would fit the unique municipal environment and help address the lack of ICT continuity controls.

### **7.3 Accomplishment of Objectives**

In order to address a real-world problem regarding ICT continuity within South African local government, Chapter 1 defined the objective of this study. The primary objective of this study was to construct a method, consisting of a theoretical foundation and a supporting tool-set, to assist the development and implementation of IRBC in local government. This method would have to be applicable to the unique municipal ICT environment.

Three secondary objectives were defined to help accomplish the primary objective. These were:

1. To explore the modern ICT and business continuity landscape to identify different concepts and their inter-relationships and through standards and best practices, extrapolate relevant continuity approaches to fit the requirement in local government

2. To determine the primary challenges and factors contributing to the lack of implemented ICT continuity controls in local government
3. To articulate a holistic approach whereby municipalities can design, implement and manage effective ICT Readiness for Business Continuity

The first of these secondary objectives was to explore the business and ICT continuity landscape and achieve a broad view on various concepts within this domain. It also required that the inter-relationships between these concepts be clarified, and relevant approaches be extrapolated. Consequently, this objective was achieved within Chapter 2. The literature on the various concepts outlined the evolution of these concepts towards the ultimate focus on resilience seen in modern day enterprises. IRBC, stemming from the ISO/IEC 27031 (2011) standard, provided an approach towards a resilient ICT environment that fits the requirement in local government.

Chapter 3 addressed the second secondary objective. By means of a literature review as well as a semi-structured interview with relevant stakeholders, various challenges and factors could be identified that possibly hinders the design and implementation of ICT continuity in local government. This subsequently provided the basis for the development of a set of unique criteria which would ultimately guide the development of an approach to address the set problem.

The third and final secondary objective required that an approach be articulated to assist municipalities, within the local government sphere, to design, implement and manage IRBC. Towards this end, a method towards IRBC (M-IRBC) was established, consisting of a theoretical foundation and a supporting tool-set, which targets the planning of IRBC within the unique municipal environment. M-IRBC was developed by following the research process discussed in Chapter 4 and the unique criteria defined in Chapter 3. The adherence to these criteria was subsequently validated in Chapter 6, confirming M-IRBC's suitability to the unique municipal environment.

Collectively, by achieving these secondary objectives, a method towards IRBC (M-IRBC) in local government was delivered, and the primary objective consequently met.

## 7.4 Summary of Contributions

This study produced three research outputs that collectively constitute the research contribution. Each of these research outputs are discussed below.

### 7.4.1 Research Contribution as an Artefact

The primary contribution of this study that pertains to the primary research objective is an artefact in the form of a method. The method towards IRBC in local government, titled M-IRBC, is extensively discussed in Chapter 5. As illustrated in Figure 7.1, M-IRBC consists of both a theoretical foundation and a supporting tool-set.

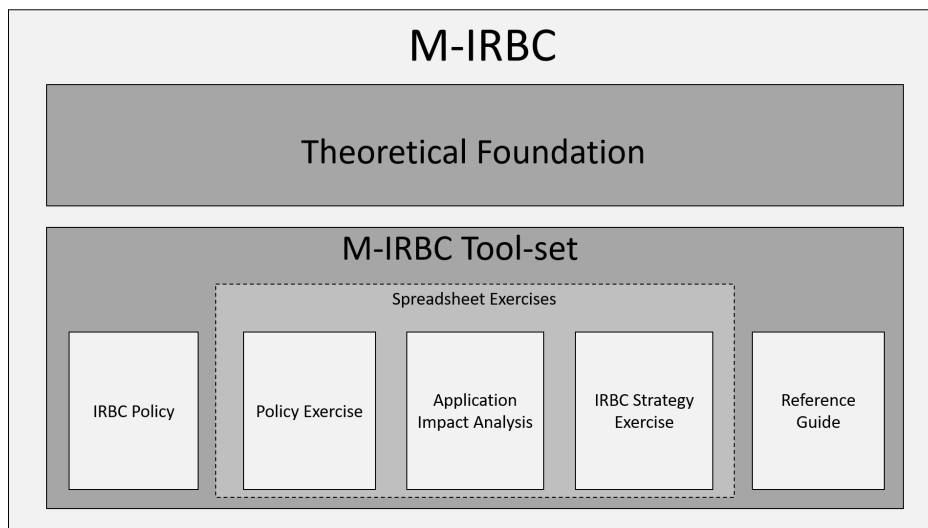


Figure 7.1: Summary of M-IRBC Components

The theoretical foundation, illustrated as a model in Figure 5.4 and discussed in Section 5.3.1, provides the basis of the entire IRBC system. The requirements of M-IRBC is illustrated and explained and includes the Plan-Do-Check-Act iterative cycle and various components such as the IRBC policy, strategy and plan. It also provides guidance pertaining to external components like the ISMS and BCMS.

The tool-set, illustrated in a process model in Figure 5.5 and discussed in Section 5.3.2, supports the theoretical foundation by providing a set of spreadsheet-based exercises to help plan the municipal IRBC and essentially give municipalities guidance on *HOW* to do so. The supporting tool-set



specifically caters for the Plan-phase of the theoretical foundation and is aimed at tailoring the IRBC system to the unique municipal size and capability. As seen in Figure 7.1, the supporting tool-set delivers outputs which include an IRBC policy, a completed AIA, an IRBC strategy, as well as a reference guide to point the user to the necessary information for the rest of the implementation process.

Holistically, M-IRBC addressed the primary objective of the study, whilst also adhering to the unique criteria of *Scalable*, *Simplistic*, *Comprehensible* and *Usable*. Adhering to these criteria ensured that M-IRBC is appropriate for the municipal environment and caters to their unique challenges. As mentioned previously, Chapter 4 provided the research process which guided the development of M-IRBC. This research process was conducted within the scope of the design-oriented IS research paradigm. For this study to be regarded as true design-oriented IS research, the resulting artefact (M-IRBC), had to adhere to the prescribed principles of the paradigm.

### **Adherence to Research Paradigm Principles**

As discussed in Chapter 4, Österle et al. (2011) explain that in order for a research study to be regarded as design-oriented IS research it has to adhere to four principles. These principles, as explained in Section 4.2, include *Abstraction*, *Originality*, *Justification* and *Benefit*.

The principle of *Abstraction* requires that, “*Each artefact must be applicable to a class of problems*”. This principle, in essence, speaks to the fact that the artefact has to be ‘general’ in nature, and not problem specific as one would find for example during consultation with a specific business problem. In this case, M-IRBC is applicable to the district and local municipalities in South Africa and address the problem of ICT continuity in municipalities throughout the country. Furthermore, due to the use of international standards, M-IRBC can be extrapolated to a large extent beyond the scope of local government.

With regard to the principle of *Originality*, “*Each artefact must substantially contribute to the advancement of the body of knowledge*”. The adherence to this principle is two-fold. Firstly, M-IRBC has been publicised in several academic publications, and as a result contribute to the body of knowledge. Secondly, M-IRBC addresses a gap in knowledge currently experienced by

‘poor resource and low-capacity’ category municipalities. As discussed in Chapter 3, these municipalities are given directive on *WHAT* they should do, but lack the information and guidance on *HOW* they should do it.

The principle of *Justification* requires, “*Each artefact to be justified in a comprehensible manner and to allow for its validation*”. With regard to this principle, M-IRBC finds its justification in the fact that it addresses a real-world problem in local government, as reported by the AGSA. M-IRBC caters for a definite need. Furthermore, by designing M-IRBC around the unique criteria defined in Chapter 3, M-IRBC allows for its validation. This validation against the set criteria of *Scalable, Simplistic, Comprehensible* and *Usable*, was done successfully during a workshop with municipal ICT representatives, as discussed in Chapter 6.

Lastly, is the principle of *Benefit*. This principle requires that, “*Each artefact yield benefit to the respective stakeholders, either immediately or in the future*”. The diffusion of M-IRBC through academic publications and distribution to the stakeholder provides the foundation for immediate benefit. Municipalities are able to use M-IRBC towards planning and implementing IRBC, a project that will run continuously and ultimately address the concerns of the Auditor-General. Subsequently, as seen in Chapter 6, the feedback regarding M-IRBC is predominantly positive, with one attendee noting that: “The M-IRBC would benefit municipalities and help with their ICT continuity challenges”.

## 7.4.2 Methodological Contribution

In addition to M-IRBC, this study also delivered a methodological-oriented contribution. As discussed in Chapter 4, the research process associated with the design-oriented IS research paradigm lacks comprehensive guidance and detail regarding each of the phases. Österle et al. (2011) however, state that design-oriented IS research provides academic freedom as long as the artefact adheres to the given principles (as discussed in the previous subsection). Consequently, due to having a similar goal, that of producing an artefact, this study combined the research approaches of design-oriented IS research and design-based research by Reeves (2006).

This resulting unique integrated research approach, illustrated in Figure 4.3, provided a detailed platform at a per-phase level, from which M-IRBC

could be developed. The elements within each of the research phases provided by Herrington et al. (2007) guided M-IRBC towards its completion and ultimate adherence to set criteria. Therefore, the integrated research process discussed in Section 4.3 and illustrated in Figure 4.3, provides an alternative approach for developing an artefact. The methodological contribution exists in the fact that this approach can be utilised in similar projects where an artefact is required to address a real-world problem and yield benefit to a particular stakeholder.

### 7.4.3 Academic Publications

The final contribution of this study included two published academic conference papers as well as an academic journal paper that is currently under review. These can be found in Appendix A. The first publication is a conference paper, presented at an international conference in Lilongwe, Malawi and published in the conference proceedings of the IST-Africa conference (See Appendix A.1). This paper discussed the results of the preliminary literature review which formed part of Phase 1 of the integrated research process.

The second publication was presented at the same conference the following year, this time in Durban, South Africa, and published in the IST-Africa conference proceedings (See Appendix A.2). This paper presented the initial draft of M-IRBC during Phase 3 of the integrated research process. Lastly, a paper was submitted to the Journal of Public Administration and is currently under review. This paper reported on the study as a whole and proposed the final M-IRBC (See Appendix A.3). The two published conference papers are referenced below:

- Koen, R., Von Solms, R., & Gerber, M. (2015). Improved Service Continuity in municipalities. In *IST-Africa Conference, 2015* (pp. 1-10). IEEE
- Koen, R., Von Solms, R., & Gerber, M. (2016). ICT Readiness for Business Continuity in local government. In *IST-Africa Week Conference, 2016* (pp. 1-11). IIMC

The three above mentioned contributions (artefact, methodological contribution, academic publications) collectively serve as the contribution of this research study.

## 7.5 Future Research

Future research is required to expand on the BCM aspect within local government. Currently, the Auditor-General reports only on the lack of ICT continuity controls in the majority of municipalities. Many of the municipalities that experience challenges with ICT continuity design and implementation are expected to experience even greater challenges with implementing BCM. However, if municipalities were provided with a practical approach to implement a BCMS, which is tailored to their needs and specific challenges, it will hopefully lead to a resilient municipality as a whole, and not only a resilient ICT environment through IRBC.

## 7.6 Epilogue

As a final word, the field of business and ICT continuity has evolved throughout the information age. Changes in technology and the increase in threats to ICT which store, transmit and process important enterprise information, have resulted in an increase in the strategic importance of not only ICT itself but in the availability of the ICT systems.

Ensuring the availability of ICT is a daunting task. Many enterprises and in this case specifically the ‘poor resource and low-capacity’ category municipalities, struggle to implement effective controls to enhance this availability. This is mostly due to limited resources and unique ICT operating environments. An approach that could circumvent some of these challenges could prove to be highly beneficial.

This study proposed such an approach in the form of a method (M-IRBC), which assists municipalities in planning and implementing IRBC according to their resource capabilities. M-IRBC adheres to specific criteria that ensure its usability in any municipality in order to plan a scalable IRBC system, that is both comprehensible and simplistic to implement and therefore suitable for use in local government.

# References

- Andersen, N. E., Kensing, F., Lundin, J., Mathiassen, L., Munk-Madsen, A., Rasbech, M., & Sørgaard, P. (1990). *Professional systems development: experience, ideas and action*. Prentice-Hall, Inc.
- Auditor-General of South Africa. (2014). *Consolidated general report on the audit outcomes of local government 2012-13*.
- Auditor-General of South Africa. (2015). *Consolidated general report on the audit outcomes of local government 2013-14*.
- Barab, S., & Squire, K. (2004). Design-based research: Putting a stake in the ground. *Journal of the Learning Sciences*, *13*(1), 1-14.
- Barab, S. A., & Kirshner, D. (2001). Guest editors' introduction: Rethinking methodology in the learning sciences. *Journal of the Learning Sciences*, *10*(1-2), 5-15.
- Belanger, F., & van Slyke, C. (2012). *Information Systems for Business: An Experiential Approach*. John Wiley and Sons, Inc.
- Botha, J., & von Solms, R. (2004). A cyclic approach to business continuity planning. *Information Management & Computer Security*, *12*, 328–337.
- British Standards Institute. (2008). *Information and communications technology continuity management Code of practice BS 25777*. BSI.
- Brynard, P., & De Coning, C. (2006). Policy implementation. In *Improving public policy* (2nd Editio ed.). Pretoria: Van Schaik Publishers.
- BSI. (2008). *BS 25777:2008*. <http://shop.bsigroup.com/ProductDetail/?pid=000000000030166966>. (Accessed: 24 July 2016)

- Cameron, R. (2001). The Upliftment of South African Local Government? *Local Government Studies*, 27(13), 97–118.
- Carr, N. G. (2003). IT doesn't matter. *Harvard Business Review*, 81(5), 41–49.
- Cerullo, V., & Cerullo, M. J. (2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management*, 21, 70–78.
- Coertze, J., & von Solms, R. (2012). A model for information security governance in developing countries. *e-Infrastructure and e-Services for Developing Countries*, 279–288.
- Constitution of South Africa. (1996). The Bill of Rights of the Constitution of the Republic of South Africa. *Government Gazette*(17678).
- Department: Public Service and Administration. (2012). Corporate Governance of Information and Communication Technology Policy Framework.
- Department: Western Cape Local Government. (2015a). Local Government Circular: C5 of 2015.
- Department: Western Cape Local Government. (2015b). *Municipal Corporate Governance of Information and Communication Technology Policy*.
- Epstein, B., & Khan, D. C. (2014). Application impact analysis: A risk-based approach to business continuity and disaster recovery. *Journal of business continuity & emergency planning*, 7(3), 230–237.
- Evans, B. (2003). *IT is a must, no matter how you view it*. <http://www.informationweek.com/business-technology-it-is-a-must-no-matter-how-you-view-it/d/d-id/1018120>. (Accessed: 17 July 2016)
- Franklin, B. J., & Osborne, H. W. (1971). *Research methods: Issues and insights*. Wadsworth Publishing Company.

- Hamidovic, H. (2011). An Introduction to ICT Continuity Based on BS 25777. *ISACA Journal*, 2(45), 1–5.
- Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, 52(6), 978–1002.
- Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business Continuity Management: Time for a strategic role? *Long Range Planning*, 37(5), 435–457.
- Herrington, J., McKenney, S., Reeves, T., & Oliver, R. (2007). Design-based research and doctoral students: Guidelines for preparing a dissertation proposal. In *World conference on educational multimedia, hypermedia and telecommunications (edmedia) 2007* (pp. 4089–4097). (Appears In: Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2007)
- IBM. (2009). *Business resilience: The best defense is a good offense*. <https://www.ibm.com/smarterplanet/global/files/us-en-us-security-resiliency-buw03008usen.pdf>.
- IoDSA. (2009). *The King Report on Corporate Governance for South Africa*. Johannesburg: Institute of Directors for Southern Africa.
- IoDSA. (n.d.). *King Report on Corporate Governance in SA*. <http://www.iodsa.co.za/?page=KingIII>. (Accessed: 24 July 2016)
- ISO 22301. (2012). *Societal security – Business continuity management systems – Requirements*. Geneva: International Standards Organization.
- ISO/IEC 27000. (2012). *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. Geneva: ISO/IEC.
- ISO/IEC 27002. (2013). *Information technology – Security techniques – Code of practice for information security controls*. Geneva: ISO/IEC.
- ISO/IEC 27005. (2011). *Information technology – Security techniques – Information security management*. Geneva: ISO/IEC.

- ISO/IEC 27031. (2011). *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*. Geneva: ISO/IEC.
- ISO/IEC 38500. (2008). *Corporate governance of information technology – ISO/IEC 38500*. Geneva: ISO/IEC.
- IT Governance Institute. (2008). *Unlocking value: An Executive Primer on the Critical Role of IT Governance*. Rolling Meadows, IL: IT Governance Institute.
- Jackson, C. (2002). The Changing Face of Continuity Planning. *Information Systems Security*, 10(6), 18–21.
- Kanyane, M. (2006). Municipal Skills challenges for accelerated service delivery in South Africa. *Journal of Public Administration*, 41(3), 112 – 118.
- Longhurst, R. (2003). Semi-structured interviews and focus groups. *Key methods in geography*, 117–132.
- Lyytinen, K. (1987). A taxonomic perspective of information systems development: theoretical constructs and recommendations. In *Critical issues in information systems research* (pp. 3–41).
- Madsen, S., Kautz, K., & Vidgen, R. (2006). A framework for understanding how a unique and local is development method emerges in practice. *European Journal of Information Systems*, 15(2), 225–238.
- Marbais, G. (2012). *Using ISO 27031 to Guide IT Disaster Recovery Alignment with ISO 22301*.
- Mathiassen, L. (1998). Reflective systems development. *Scandinavian Journal of Information Systems*, 10(1), 12.
- Ministry of CoGTA. (2016). *About Cooperative Governance and Traditional Affairs*. <http://www.cogta.gov.za/?page-id=253>. (Accessed: 11 October 2016)



- Nickson, C. (2015). *Technology & The Way We Work*. <http://www.atechnologysociety.co.uk/technology-way-we-work.html>. (Accessed: 19 July 2016)
- NIST SP800–30. (2002). *Risk Management Guide for Information Technology Systems – Special publication 800–30*. Washington: USA: National Institute of Standards and Technology.
- Nolan, R., & McFarlan, F. (2005). Information technology and the board of directors. *Harvard business review*, 83(10), 96.
- Ogu, E. C., & Oyerinde, O. D. (2014). ICT And National Security in Developing and Underdeveloped Countries The Good , The Bad and The Ugly : A Case Study of Nigeria ’ s Cyberspace. *International Journal of Computer Science and Information Technologies*, 5(4), 5625–5633.
- Olivier, M. S. (2009). *Information technology research: A practical guide for computer science and informatics*. Van Schaik.
- Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A., & Sinz, J. E. (2011). Memorandum on design-oriented information systems research. *European Journal of Information Systems*, 20(1), 7–10.
- Posthumus, S., von Solms, R., & King, M. (2010). The board and IT governance : The what , who and how. *South African Journal of Business Management*, 41(3), 23–33.
- Presidential Commissioners. (1998). *Report of the Presidential Review Commission on the Reform and Transformation of the Public Service in South Africa*.
- PriceWaterhouseCoopers. (n.d.). *Corporate Governance – King III report – Introduction and overview*. <http://www.pwc.co.za/en/king3.html>. (Accessed: 24 July 2016)
- Protiviti Inc. (2013). *Guide to Business Continuity Management*. <http://www.protiviti.com/en-US/Documents/Resource-Guides/Guide-to-BCM-Third-Edition-Protiviti.pdf>.

- Reeves, T. C. (2006). Design Research from a Technology Perspective. In J. Van den Akker, K. Gravemeijer, S. McKenney, & N. Nieveen (Eds.), *Educational design research* (pp. 86–109). Routledge.
- Sahebjamnia, N., Torabi, S., & Mansouri, S. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, *242*(1), 261–273.
- Saleh, Z., Refai, H., & Mashour, A. (2011). Proposed Framework for Security Risk Assessment. *Journal of Information Security*, *02*(02), 85–90.
- SALGA. (2012). A Municipal Guide / Roadmap To Successful ICT Governance.
- Sarbanes-Oxley Act. (2002). *Sarbanes-Oxley Act*. Washington DC.
- Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security*, *57*, 14–30.
- Stanton, R. (2005). Beyond disaster recovery: The benefits of business continuity. *Computer Fraud and Security*, *2005*(7), 18–19.
- von Solms, R., & von Solms, S. H. (2006). Information Security Governance: A model based on the Direct-Control Cycle. *Computers and Security*, *25*(6), 408–412.
- Wang, F., & Hannafin, M. J. (2005). Design-based research and technology-enhanced learning environments. *Educational Technology Research and Development*, *53*(4), 5–23.
- Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security*. Course Technology.

# Appendix A

## Academic Publications

Appendix A includes the academic papers that were written throughout the duration of the study. These papers include two published international conference papers, as well as a journal paper that has been submitted but not yet reviewed.

These include the following:

1. IST-Africa 2015
2. IST-Africa 2016
3. Journal of Public Administration

### A.1 IST-Africa 2015

*This paper, titled ‘Improved Service Continuity in Municipalities’ was presented at the 2015 IST-Africa international conference. The conference was hosted in Lilongwe, Malawi. The paper was subsequently published in IEEE-Xplore.*



IST-Africa 2015 Conference Proceedings  
Paul Cunningham and Miriam Cunningham (Eds)  
IIMC International Information Management Corporation, 2015  
ISBN: 978-1-905824-50-2

## Improved Service Continuity in Municipalities

Ruan KOEN<sup>1</sup>, Rossouw VON SOLMS<sup>2</sup>, Mariana GERBER<sup>3</sup>

*Nelson Mandela Metropolitan University,  
University Way, Port Elizabeth, 6001, South Africa*

<sup>1</sup>Tel: +27605072141, Email: [s211062790@nmmu.ac.za](mailto:s211062790@nmmu.ac.za)

<sup>2</sup>Tel: +27415043607, Email: [rossouw@nmmu.ac.za](mailto:rossouw@nmmu.ac.za)

<sup>3</sup>Tel: +27415043705, Email: [mariana.gerber@nmmu.ac.za](mailto:mariana.gerber@nmmu.ac.za)

**Abstract:** Information Technology acts as an enabler for municipalities to provide services to its citizens. It is therefore important for these services to continuously be available. An effective Service Continuity Management System enables these services to continue during IT disasters by combining good Contingency - and Disaster Recovery - Plans. The problem is that municipalities lack proper Service Continuity Management. This lack is emphasized by the Auditor General's findings in South Africa. It is thus the objective of this paper, through an initial literature survey, leading to an ongoing case study, to propose a model for guiding the process towards improved service continuity in municipalities, not only within South Africa, but throughout Africa.

**Keywords:** Municipalities; Service Continuity (SC); Service Continuity Management (SCM); IT Continuity

### 1. Introduction

Information Technology (IT) service continuity is a critical aspect within government institutions. IT plays an important role as an enabler in government service delivery across the continent of Africa, and throughout the world. According to Cameron [5], South Africa has one of the most advanced local government systems in the world. In order to move away from a hierarchical intergovernmental system, the Constitution of South Africa drafted in 1996, introduced a three-sphere system. Chapter 3 of the Constitution introduces the sphere system, which promotes a co-operative government. In the Republic, government is constituted as national, provincial and local spheres of government, which are distinctive, interdependent and interrelated [19]. This allows each sphere of government to function on its own, but rely on each other in working towards the greater goal.

The Constitution of South Africa [19] states that local government consists of municipalities, which must be established throughout the country. Each municipality has the right to govern, on its own initiative, the local government affairs of its community, subject to conformance to national and provincial legislation, as provided in the Constitution [19]. The Municipal Council has the executive and legislative authority of the municipality; and national or provincial government may not compromise a municipality's ability or right to exercise its powers or perform its functions [19]. Municipalities have several objectives. These objectives, as declared in the Constitution, include – among others – to promote a safe and healthy environment, and to ensure the provision of services to communities in a sustainable manner [19]. In modern societies, IT enables local governments to achieve these objectives and to fulfil their duties.

Using IT in government holds many advantages, if used effectively and to its full potential. IT saves on cost, increases productivity and eases citizen interaction with

government; but along with all these benefits come certain drawbacks. Ndou [14] states: “ICT, in general, is referred to as an ‘enabler’; but on the other hand, it should also be regarded as a challenge and a peril in itself.” Using IT on a large scale, such as on a governmental level, requires effective governance to ensure the safety of information transgressing the IT systems and service continuity in the event of system interruptions. The term service continuity is used in this paper interchangeably with business continuity; as this paper deals with municipalities, which are not seen as business functions, but rather as service providers.

IT systems are used to store, transmit and process important information. It is reasonable to argue that, with regard to governmental institutions, ensuring the protection of the information is critical. This is normally conducted via a process of effective information security management. Information security management involves the preservation of the confidentiality, integrity and availability of information [13]. Botha and von Solms [3] state that although ensuring confidentiality and integrity is important, the availability component of information security is of greater significance with respect to Business Continuity Planning (BCP). BCP involves developing a collection of procedures for the various business units that would ensure the continuance of critical business processes – while the IT data centre is recovering from some related incident or disaster [21]. Such an incident or disaster usually gives rise to some disruption in IT services; and normally associated business services are influenced in one or other matter. “The potential causes of business interruption are not only from natural disasters; but [they] are multifaceted, including interruptions caused by human error, utility disruptions (such as power outages), and malicious threats from outsiders” [6]. Service continuity thus aims to have all business functions, whether they are those of the finance department or HR department, function normally during a disastrous event.

The Auditor General (AG) of South Africa conducts annual audits of, among others, local government. The AG has identified Information Technology as a key risk area. In the Consolidated General Report on the audit outcomes of local governments in 2012-13 [2], the AG reiterates what was highlighted above that IT, if used properly, ensure the confidentiality, integrity and availability of state information, enable service delivery, and promote national security. The AG says that it is thus essential for good IT governance, effective IT management, and a secure IT infrastructure to be in place [2]. The AG audit of local government assessed the IT controls, and highlighted four major shortcomings: those of IT governance, security management, user access management and IT service continuity [2]. Thus, IT service continuity is seen as one of the four critical IT control areas that require special attention within municipalities.

The AG explains that IT service continuity controls enable institutions to recover critical business operations and application systems that would be affected by disasters or major system disruptions within reasonable time frames [2]. Proper service continuity planning (within the IT domain) should enable a municipality to continue with critical service delivery processes in all departments; whilst disaster recovery of IT systems take place behind the scenes. From the audit, the AG found that 30% of the auditees had IT service continuity controls that were embedded and functioning; 62% continued to experience challenges with design; and 8% experienced challenges with implementation [2]. These results are illustrated in Figure 1, as seen in the AG’s Consolidated General Report [2].

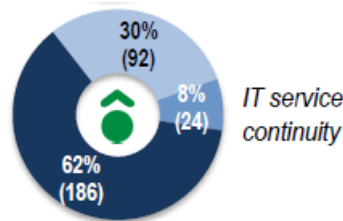


Figure 1: IT Service Continuity Audit Results

Some of the most common findings by the AG included: firstly, that most municipalities experienced challenges with the design and implementation of appropriate business continuity plans and disaster recovery plans [2]. The finding that 62% of municipalities had not designed a continuity plan, which is an alarming figure, supports this contention. Secondly, the AG found that the management of back-ups remained a challenge as most of the municipalities did not test their back-ups to ensure that they could be restored when required [2]. These back-ups were also not stored at secure off-site facilities, to ensure that they could easily be retrieved in the event of an onsite disaster; but not damaged or destroyed in the same disaster.

From the above, it is clear that the overall management of business and IT continuity planning is generally not addressed properly in most South African municipalities. This is a concerning situation, because municipalities process valuable information on a daily basis; the loss of confidentiality, integrity, and the availability of that information, can have dire consequences. Thus, the problem is that there exists a lack of proper IT service continuity structures in South African municipalities.

The objective of this paper is, therefore, to study and assess the reasons for this situation, and to propose a model for improving IT service continuity in municipalities. The paper commences with a discussion of the research approach, followed by an in-depth investigation of relevant municipal documents, as well as best practices and standards relating to business continuity management. Finally, a model for improved service continuity in municipalities will be presented.

## 2. Research Approach

In order to address the problem, as described in the previous section, this paper focuses on a detailed literature review, leading to an ongoing case study. According to Olivier [15], a literature review is an iterative process of obtaining information sources relevant to one's study. For the purpose of this paper, these sources include a variety of documents, ranging from legislation, audit reports, standards and best practices.

Qualitative document analysis was conducted to study the identified documents. Qualitative research is defined as being about exploring issues, understanding phenomena, and answering questions – by analysing and making sense of unstructured data [17]. The documents should thus be analysed and interpreted, in order to gain an understanding of the bigger issue. Document analysis, according to Bowen [4], is a systematic procedure for reviewing or evaluating documents. The above mentioned author then goes on to explain that the process involves skimming, reading and interpreting the documents. With this in mind, thorough analysis of the relevant documents should illustrate the problem, with legislation and standards providing acceptable concrete information to argue the case for better service continuity.

Argumentation involves producing and comparing arguments – using a variety of types of reasoning [1]. It was thus the approach of this study to use the information gathered through analysing relevant documentation to reason towards a reiterative approach to improve the situation of service continuity in municipalities. This reiterative process was presented as a model. Tomhave [20] defines a model as: “An abstract, conceptual construct

that represents processes, variables, and relationships, without providing specific guidance on, or practices, for implementation". The following section will explore the most relevant documents relating to service continuity in local government. The aim is to structure the documents and extract important aspects for improving service continuity.

### **3. Service Continuity and Related Best Practices and Standards**

In order to address the problem identified in section 1, it is important to gather information relevant to the problem; thus making use of documents, which are known to be best practices or international standards, and to place them in context in the topical area. The most important aspects regarding the improvement of service continuity should be identified, and their significance supported by the documents. This section will look at the most relevant documents relating to the improvement of service continuity; and highlight important aspects necessary to address the problem. The relationship between what was found in these documents and the problem will then be put in context. The next sub-section will discuss some of the relevant standards and best practices in this regard.

#### *3.1 Relevant Standards and Best Practices*

Documents, such as best practices and standards, allow society to gather amongst other, sound information, guidelines or requirements, from a consensus of experts. It is thus beneficial to any entity, private or public, to make use of such documents and follow its guidance and recommendations.

The King Report on Governance was formally introduced by the Institute of Directors in Southern Africa. The most recent report, namely KING III, came into effect in March of 2010; and it falls in line with the South African Companies Act no. 71 of 2008 [10]. KING III, in contrast to previous revisions, applies to all entities – regardless of the form of incorporation and establishment [16]. In essence, KING III is thus applicable to private and public entities – regardless of size or type of incorporation. KING III consists of several principles on corporate governance.

IT, as an enabler for any business, requires proper governance to function effectively. Chapter 5 of KING III includes seven principles for good IT governance. One of these principles applies to service continuity. Principle six states that the board should ensure that information assets are managed effectively [9]. Within principle six, it is stated that the board is responsible for establishing a business continuity programme addressing the company's information and recovery requirements, and ensuring that the programme is aligned with the successful execution of the business' activities [9]. Principle 6 also makes reference to the CIA of information, where ensuring the availability of information and information systems in a timely manner, is specified [9].

From this, it is reasonable to argue that IT is regarded as an important business function requiring the board's attention. Thus, service continuity is part of good governance; and sound oversight from the board or municipal council is core to its effective functioning.

Implementing service continuity is a small step towards good IT governance. The next consideration should be having a good service continuity system. International standards are critical to businesses when implementing any form of IT systems [11]. ISO standards draw on international expertise and experience; and they are, therefore, a vital resource for governments when developing regulations [11]. Using ISO standards for implementing service continuity is thus beneficial to any enterprise, including municipalities. ISO 22301:2012 [12] stipulates all the requirements of a business continuity management system. From here on, this will be referred to as a service continuity management system (SCMS).

Table 1: PDCA Mapping to Clauses

ISO22301 Clause	PDCA Phase	Explanation of Clause Content
Clause 4 – Context of the organisation	Plan	Introduces requirements necessary to establish the context of the SCMS as it applies to the organisation, as well as needs, requirements and scope.
Clause 5 – Leadership	Plan	Summarizes the requirements specific to top management’s role in the SCMS, and how leadership articulates its expectations to the organization via a policy statement.
Clause 6 – Planning	Plan	Describes requirements as they relate to establishing strategic objectives and guidance for the SCMS as a whole.
Clause 7 – Support	Plan	Supports SCMS operations, as they relate to establishing competence and communication on a recurring basis with interested parties, while documenting, controlling, maintaining and retaining such required documentation.
Clause 8 – Operation	Do	Defines service continuity requirements; and it determines how to address them and develops the procedures to manage a disruptive incident.
Clause 9 – Performance evaluation	Check	Summarizes requirements necessary to measure service continuity management performances, SCMS compliance with ISO22301 and management’s expectations, and seeks feedback from management regarding expectations.
Clause 10 – Improvement	Act	Identifies and acts on SCMS non-conformance through corrective action.

ISO22301:2012 [12] specifies requirements for setting up and managing an effective SCMS. ISO22301 applies the “Plan-Do-Check-Act” (PDCA) to improve the effectiveness of an organisation’s SCMS. Seven of the clauses contained in ISO22301 are requirements for an effective SCMS. Each of the requirement clauses within the ISO22301 standard is mapped to a specific phase with the PDCA model [12]. This mapping is illustrated in Table 1, together with a brief explanation of what each clause entails. Adhering to these requirements should enable the implementation of a sound SCMS in any organisation, including government. Governmental entities should, however, adhere to internal practices and frameworks.

The Department of Public Service in South Africa drafted the Corporate Governance of Information and Communication Technology Policy Framework (CGICTPF), in order to institutionalise the corporate governance of ICT, as an integral part of corporate governance within departments [7]. The CGICTPF is applicable to all spheres of government [7], including municipalities. A three-phase approach is set out to enable departments or entities to implement the CGICTPF.

Service continuity is briefly addressed in the CGICTPF, as part of Phase 1. Phase 1 includes establishing the corporate governance of and governance of ICT environments [7]. The CGICTPF requires policies, frameworks and plans for enabling a departmental service continuity plan [7]. This, in turn, should be informed by a service continuity strategy, service continuity policy, and an IT continuity plan [7]. The CGICTPF is, however, a rather high-level document, and therefore a more detailed document specifically for local government was drafted.

The South African Local Government Association (SALGA) drafted a Municipal Guide to Successful ICT Governance aligned with the CGICTPF [18]. Guidelines towards service continuity in municipalities are given as short-term goals. These guidelines are illustrated in Table 2 [18]. These guidelines are, however, rather vague; and they hinder implementation at a municipal level. The next sub-section will discuss the relationship of these documents with the problem of this study, in order to put them in context.



Table 2: SALGA SC Guidelines

Incorporate the ICT continuity and disaster recovery plans into the organisational business continuity plan.
Distribute, update and test the ICT continuity plan and DRP, and store at an offsite location.
Implement an ICT back-up and retention strategy.
Perform back-up procedures for data and programs, according to the above strategy.
Store back-ups in a secure offsite storage facility.
Implement physical access and environmental controls over offsite storage facilities.

### 3.2 Relationship with Problem

The previous sub-section discussed documents relevant to IT governance and service continuity applicable to any organisation. The aim of this sub-section is to relate the most important aspects of those documents with the problem area of this study. This will place the relevant documents in the context of municipalities, to indicate what is required by municipalities with regard to the problem.

The problem for this study was identified as being a lack of proper IT service continuity in municipalities. The root of this issue, as identified by the AG, was that no IT service continuity plan design has taken place in a large majority of municipalities [2]. Municipalities must adhere to KING III, as stated in section 3.1., KING III clearly directs the municipal council to establish a service continuity plan, which should address the information and recovery requirements, ensuring that this is aligned with the successful execution of business activities [9]. Principle six also requires that the availability of information and information systems in a timely manner needs to be addressed [9]. Implementing designed service continuity plans is also a problem.

As seen in section 1, along with the 62% that have not designed any service continuity plans, the AG identified 8% of municipalities which have designed service continuity plans, but have not yet implemented them. The ISO22301 standard for implementing and managing an effective SCMS was discussed in section 3.1. It sets out specific requirements for implementing and maintaining a service continuity system. The ISO22301 standard is universal; and thus it is applicable to all municipalities [12]. Proper guidance should thus be given to these municipalities – based on the requirements of this standard. In South Africa, documents, such as the CGICTPF and SALGA guidelines, were drafted for IT governance in government – and the latter was exclusively designed for municipalities.

The CGICTPF is in line with KING III with regard to IT governance. Both state that IT governance should be a top-level management directive and also require compliance. Again, as with KING III, the CGICTPF requires government institutions to have policies, frameworks and plans for enabling a service continuity plan. This, however, is not becoming a reality; since most municipalities lack guidance from higher levels in implementing service continuity plans. The SALGA guidelines for service continuity in municipalities are vague and rather high level. It thus hinders design and implementation of service continuity. In essence, it states *what* needs to be done; but it does not give any direction as to *how*.

This sub-section discussed how the documents relevant to service continuity, relate to the lack of proper service continuity within municipalities. It also highlighted that adherence to what is stated in these documents is critical for successful service continuity.

This section has identified and discussed documents relevant to service continuity. These include both best practices and standards; and they have been placed in context with the problem of this study. Important requirements for service continuity were identified and the need for proper guidance in service continuity was highlighted. The next section will aim to address the problem by arguing the need for a model to implement and maintain a

service continuity plan – specifically for municipalities – not just within South Africa, but throughout Africa.

#### 4. Towards Improved Service Continuity in Municipalities

The previous section allowed for a better idea of where municipalities are in reference to standards and best practices with respect to the problems at hand. This section aims to address the problem identified by this study, by using the ISO22301 standard as a guide, to propose and formulate a model for a service continuity management process.

In essence, a model should enable one to understand the different aspects and inter-relationships without any in-depth explanation. The Municipal Service Continuity Management Model is illustrated in Figure 2. The model is based on the “Plan-Do-Check-Act” model, as seen in ISO22301:2012 [12]. It incorporates service continuity management (SCM), contingency planning (CP), and disaster recovery (DR) in a spiral – to illustrate their relationship – and then the applicability of the PDCA process to each entity.

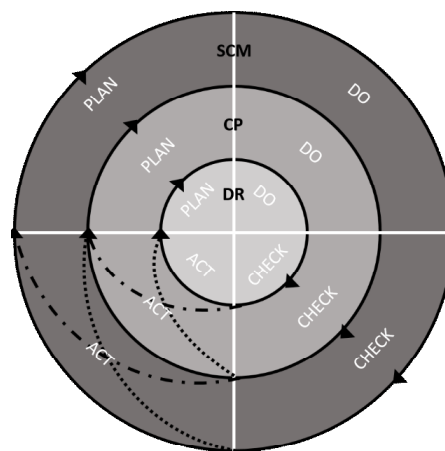


Figure 2: Municipal Service Continuity Management Model

The ‘circles’ within the spiral are an indication of how each entity relates to the others. The focus of this study is on service continuity, and how to manage it properly. In order to do this, all of the aspects, referred to as entities, involved within proper service continuity should form part of it. For this paper, these entities will only be mentioned, and their role briefly explained. The first of these aspects is disaster recovery (DR). Starting from the centre, DR is core to SCM. DR aims to recover the municipal IT systems and their related functions as quickly as possible after a disaster event. Disaster events could include natural disasters or man-made disasters, anything that might cause IT failure, whether a tornado or a Denial-of-Service attack on the network. IT, as stated earlier in this study, is an enabler and therefore, if the IT fails, so do the business services that rely on it.

Contingency planning (CP) aims to make provision for continuing business processes in a disaster situation, while recovery is taking place [8]. DR is thus a component of CP, as illustrated in the model. With regard to municipalities, CP is critical to the overall SCM. The business processes that rely on IT need to continue, whether that entails residents paying utility fees, or merely the HR department doing staff information updates. CP could involve the use of back-up systems, or an off-site facility, whilst the recovery of core IT takes place. It should be noted that the CP should function in such a way that when IT recovers from the disaster, normal business can seamlessly continue, with the work done

during the disaster being available on the recovered systems. CP, in line with its DR activities, forms part of service continuity; and this, in turn, needs to be managed.

Just like any other management system, according to ISO22301:2012 [12], a SCMS includes key components. These components include: (1) A policy; (2) people with defined responsibilities; (3) certain management processes like planning, assessment and improvement; (4) documentation providing auditable evidence; and (5) SCM processes relevant to the organisation [12]. Running an effective SCMS, together with its underlying CP and DR plans, requires an iterative process; because disaster threats change regularly. To enable this iteration, the model makes use of the PDCA process, and therefore the spiral effect in the model.

In order to better understand the PDCA process, each step has to be defined. Table 3 gives an overview of what each step involves. The PDCA steps need to be implemented on all three entities. The first of these is DR. The DR plans need to continuously go through the PDCA steps, in order to improve their reliability; as is the case with the CP that has to be reviewed, and the back-up systems tested for effectiveness in the event of a disaster. Lastly, the SCMS will go through the same iterative process, in order to keep the SCMS in line with other management systems in the business, and to adequately fulfil the requirements of a proper SCMS. The requirements of these are given by ISO22301, as shown in Section 3, Table1. Improving any of the SCMS requires one to 'Act'.

Table 3: PDCA Process Definition

<b>Plan</b>	Establish the necessary policies, objectives and procedures.
<b>Do</b>	Implement and operate the policies and procedures.
<b>Check</b>	Monitor and review its effectiveness against the stated objectives.
<b>Act</b>	Maintain and improve by taking corrective action, based on the review.

The process of 'Act' is initiated after a proper review of the system during the 'Check' process. The 'Check' process may lead to two actions, as illustrated by the model. A clean check of the DR system can allow one to shift over to the PDCA for CP; it would be the same for CP shifting over to PDCA processes for SCM. Alternatively, if a check of the SCMS requires one to act and improve the system, the process shifts back to the PDCA processes for CP. The reason is that CP is an important aspect for a proper SCMS. The same applies to improving CP, which requires an improvement of DR, thus resulting in a shift back to the PDCA processes of DR.

As a whole, the Municipal Service Continuity Management Model takes SCM and its underlying components into account; it illustrates their relationships; and applies the PDCA process cycle on each of the three entities. The model also illustrates that acting on an entity might require shifting either up or down; i.e. developing the next entity or improving the previous entity. Using this model, together with the requirements of the ISO22301 standard, should enable the implementation and maintenance of an effective SCMS in municipalities.

Although a number of best practices, standards and governmental documents have provided a lot of relevant information as to *what* needs to be done to improve service continuity, the Municipal Service Continuity Management Model does provide some guidance on *how* it can be done.

This section has introduced the Municipal Service Continuity Management Model as three spiralling circles, each indicating entities of a SCMS. These entities and their relation were explained, giving a brief overview of each; after which looking at applying the PDCA process to these entities to allow for an effective SCMS.

## 5. Conclusion

Information Technology plays a vital role as an enabler in the delivery of services in municipalities. The hardware and its information systems are critical components requiring

constant up-time. It is thus extremely important that when IT fails, normal business processes can continue seamlessly; while primary IT systems recover from the disaster event. The problem identified by this study was a lack of service continuity in municipalities. This hinders a municipality's ability to deliver services. The objective of this study was thus to propose a model for improving IT service continuity.

This objective was met through the development of a Municipal Service Continuity Management Model. The model proposes an iterative process for planning, implementing, monitoring and improving each underlying entity of service continuity management through continuous review and maintenance. Using the model as a guide, in conjunction with the requirements set out in relevant standards, should enable municipalities to implement a sound continuity system. Although this study has focused on South Africa, it is applicable to any municipality in Africa; as the solution is based on international standards.

Municipalities should thus not hesitate to ensure that adequate SCM takes place. This model currently only provides a process, and more detailed guidance is needed to oversee the implementation and maintenance of each entity.

Further research will thus be done, to examine the requirements for each of the entities of SCM, namely CP and DR, to provide an overarching tool for implementing a SCMS. This tool should answer 'HOW' effective SCM should be implemented, and not only 'WHAT' should be implemented. Such a tool should include all the requirements for every entity, in order to fully incorporate each entity into SCM in an effective and consistent manner. Such a tool should give municipalities the ability to effectively implement sound IT continuity, and thus deliver continuous service. This study will continue and further results will follow in due course.

## References

- [1] Andriessen, J. B. (2003). Argumentation, computer support, and the educational context of confronting cognitions. *Arguing to Learn*, 1-25.
- [2] Auditor - General of South Africa. (2013). *Consolidated general report on the audit outcomes of local government*. Auditor - General South Africa.
- [3] Botha, J., & von Solms, R. (2004). A cyclic approach to business continuity planning. *Information Management & Computer Security*, 12(4), 328-337.
- [4] Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*, 9(2), 27-40.
- [5] Cameron, R. (2001). The upliftment of South African local government? *Local Government Studies*, 27(3), 97-118.
- [6] Cerullo, V. &. (2004). Business continuity planning: a comprehensive approach. *Information Systems Management*, 21(3), 70-78.
- [7] Department: Public Service and Administration. (2012, December). Public Service Corporate Governance of Information and Communication Technology Policy Framework. South Africa: the dpsa.
- [8] Glenn, J. (2002). What is business continuity planning? How does it differ from disaster recovery planning? *Disaster Recovery Journal*, 15(1).
- [9] IoDSA. (2009). *KING REPORT ON GOVERNANCE FOR SOUTH AFRICA*. Johannesburg: IoDSA.
- [10] IoDSA. (n.d.). *King Report on Corporate Governance in SA*. Retrieved 11 30, 2014, from Institute of Directors Southern Africa: <http://www.iodsa.co.za/?kingIII>
- [11] ISO. (n.d.). *Benefits of International Standards*. Retrieved 11 30, 2014, from International Standards Organisation: <http://www.iso.org/iso/home/standards/benefitsofstandards.htm>
- [12] ISO/IEC. (2012). ISO 22301:2012 Societal security — Business continuity management systems — Requirements. Geneva, Switzerland: ISO/IEC.
- [13] ISO/IEC. (2014). ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva, Switzerland: ISO/IEC.
- [14] Ndou, V. (2004). E-government for developing countries: opportunities and challenges. *The Electronic Journal of Information Systems in Developing Countries*, 1-24.
- [15] Olivier, M. S. (2009). *Information Technology Research - A Practical Guide for Computer Science and Informatics* (3rd ed.). Pretoria: Van Schaik.
- [16] PWC. (n.d.). *Corporate Governance - King III report - Introduction and overview*. Retrieved 11 30, 2014, from PricewaterhouseCoopers: <http://www.pwc.co.za/en/king3/>

- [17] QSR International. (n.d.). *What is Qualitative Research*. Retrieved 11 29, 2014, from QSR International: <http://www.qsrinternational.com/what-is-qualitative-research.aspx>
- [18] South African Local Government Association. (2012, June). *A Municipal Guide / Roadmap To Successful ICT Governance*. South Africa: SALGA.
- [19] The Bill of Rights of the Constitution of the Republic of South African. (1996). *Government Gazette*. (No. 17678).
- [20] Tomhave, B. L. (2005). Retrieved December 4, 2014, from [www.secureconsulting.net/Papers/Alphabet\\_Soup.pdf](http://www.secureconsulting.net/Papers/Alphabet_Soup.pdf)
- [21] Wilson, B. (2000). Business Continuity Planning: A Necessity In The New E-Commerce Era. *Disaster Recovery Journal*, 13(4), 24-26.

## A.2 IST-Africa 2016

*This paper, titled ‘**ICT Readiness for Business Continuity in Local Government**’ was presented at the 2016 IST-Africa international conference. The conference was hosted in Durban, South Africa. The paper was subsequently published in IEEE-Xplore.*



IST-Africa 2016 Conference Proceedings  
Paul Cunningham and Miriam Cunningham (Eds)  
IIMC International Information Management Corporation, 2016  
ISBN: 978-1-905824-54-0

# ICT Readiness for Business Continuity in Local Government

Ruan KOEN<sup>1</sup>, Rossouw VON SOLMS<sup>2</sup>, Mariana GERBER<sup>3</sup>

*Nelson Mandela Metropolitan University,*

*University Way, Port Elizabeth, 6001, South Africa*

<sup>1</sup>Tel: +27605072141, Email: [s211062790@nmmu.ac.za](mailto:s211062790@nmmu.ac.za)

<sup>2</sup>Tel: +27415043604, Email: [rossouw.vonsolms@nmmu.ac.za](mailto:rossouw.vonsolms@nmmu.ac.za)

<sup>3</sup>Tel: +27415043705, Email: [mariana.gerber@nmmu.ac.za](mailto:mariana.gerber@nmmu.ac.za)

**Abstract:** Information and Communication Technology is a critical enabler for service delivery in local government. The importance of adequate business and ICT continuity should therefore not be understated. Effective ICT Readiness, as part of the wider Business Continuity system, enables ICT to be more resilient and able to recover should an incident or disaster occur. However, within South African local government, ICT continuity controls are found to be ineffective. This is an ongoing problem reported by the Auditor-General of South Africa. The objective of this paper is therefore to propose a model, based on literature and a design-oriented research approach, for the implementation and operation of ICT readiness in local government – applicable throughout the continent of Africa.

**Keywords:** Local Government; Business Continuity (BC); Information and Communication Technology (ICT); ICT Readiness for Business Continuity (IRBC)-

## 1. Introduction

Information and Communication Technology (ICT) has become a pervasive commodity in modern day organisations. ICT is used to store, transmit and process important information. ICT has developed from initial adoption as a technical instrument, to a business function core to achieving organisational objectives. This is also the norm within government institutions, where ICT has become a key enabler to achieve governmental objectives.

In South Africa, government operates at national, provincial and local levels [1]. Local government includes municipalities which are divided into three categories namely: metropolitan-, district- and local municipalities [1]. Local government is mandated by the Constitution of South Africa to deliver basic services to its community [1]. Local government relies on ICT to deliver these services. Therefore, it is essential that local government has effective ICT systems in place to enable service delivery. Critically, these ICT systems have to be continuously available; however, this is not always the case.

The Auditor-General of South Africa conducts annual audits of, amongst others, local government. The Auditor-General has identified ICT as a key risk area within local government; furthermore, the Auditor-General highlighted four critical control areas within ICT, which includes ICT continuity. The Auditor-General emphasized that ICT should ensure the confidentiality, integrity and availability of information [2]. Botha and von Solms [3] support this contention, but highlights that the availability aspect is particularly important to business continuity. In general, the Auditor-General has found that ICT continuity, which is an important element of business continuity, is generally not well addressed within local government.

The consolidated audit reports from 2012-13 [2], and 2013-14 [4] published by the Auditor-General of South Africa have highlighted major concerns with regard to the design and implementation of ICT continuity controls in local government. Referring to Figure 1, which illustrates the consolidated audit findings, it is evident that ICT continuity is insufficiently addressed within local government, with the majority of local governments failing to have embedded and functioning ICT continuity controls [2], [4]. When comparing the results from both audit years, Figure 1 illustrates a slight improvement in the amount of local governments which have designed their ICT continuity controls; however, the fact that there was a slight decline in local governments which possess embedded and functioning controls, is concerning.

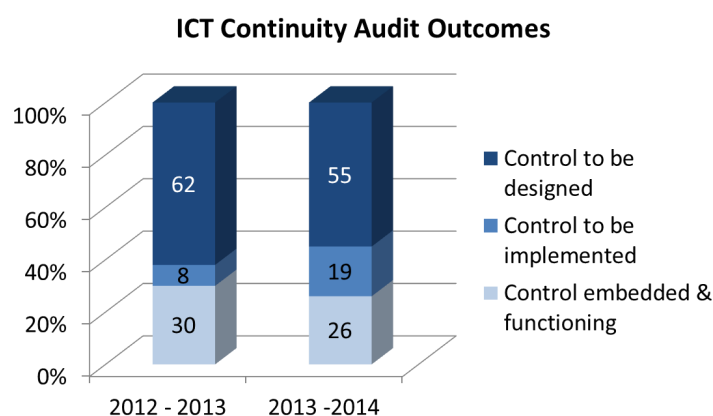


Figure 1: Auditor General Consolidated Findings

Taking into account what has been stated above, it is clear that the ICT component, within the business continuity domain, is generally not addressed satisfactorily within the majority of South African local governments. It is therefore the objective of this paper to address this issue by proposing a model for the operation of ICT Readiness for Business Continuity in South African local government, and similarly, where applicable throughout Africa. Furthermore, a process for the implementation thereof will be suggested – discussing research that is currently still ongoing and in the process of being developed. Critically, best practices and international standards guide towards perfect world implementations, which due to the lack in capacity in most of these local governments, are unattainable. The combined approach proposed in this paper is therefore tailored to address ICT continuity, whilst considering the unique challenges faced in local government.

This paper commences with a discussion about the research approach, followed by an in-depth look at the business- and ICT continuity landscape as well as the concept of ICT Readiness for Business Continuity. Finally, a model for ICT Readiness will be proposed, followed by a suggested implementation process, whereupon the paper will be concluded. The next section will look at the research approach.

## 2. Research Approach

In order to address the problem of ICT continuity in local government, this paper – which forms part of an ongoing research study – proposes a model and process for the operation and implementation of ICT Readiness for Business Continuity in local government. The aforementioned model will form the foundation upon which a tangible artefact will be developed to aid local government in fulfilling their ICT Readiness objectives. Keeping in



mind the primary research goal of yielding a useable artefact, the approach for the study is design-oriented in nature.

For the purpose of this paper, and the larger study, the design-oriented research followed an iterative method with the goal of refining the contribution of the research through various testing cycles. According to Olivier [5], a literature study is an iterative process of obtaining information sources relevant to one's study. To get to the initial draft of the model and process, a detailed literature study was conducted. Upon completion, the initial draft underwent various cycles of refinement through semi-structured interviews.

Semi-structured interviews can be described as: "*a qualitative method of inquiry that combines a pre-determined set of open questions (questions that prompt discussion) with the opportunity for the interviewer to explore particular themes or responses further*" [6]. To tailor the contribution as a scaled-down approach for lesser capacity municipalities, the input from municipalities was critical for the refinement process. These interviews were conducted with members of the ICT department at a district municipality in the Western Cape Province. This local government was best suited for the refinement cycle due to the clean audit of its ICT department.

Finally, the refined model was presented and verified through open and formal discussions. Tomhave [7] defines a model as: "*An abstract, conceptual construct that represents processes, variables, and relationships, without providing specific guidance on, or practices, for implementation*". The following section will explore the continuity landscape, bridging the gap between ICT and Business Continuity, and lastly introduce the concept of ICT Readiness.

### **3. ICT and Business Continuity: Bridging the Gap**

Business continuity and its related activities have become synonymous with daily operations in the majority of modern day organisations. Business continuity is defined as the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident [13]. Herbane, Elliott and Swartz [8] state that organisations have not only recognised the need for an approach toward continuity beyond mere ICT disaster recovery, but have linked business continuity management to strategically important dimensions of their operations. However, confusion still exists about the differences between disaster recovery and business continuity, where the terms are used interchangeably – whilst a clear difference in function exists [9]. This section will explore different concepts within continuity and briefly look at the evolution of business continuity as it is known today. Finally, the concept of ICT Readiness for Business Continuity will be discussed.

#### *3.1 From Recovery to Resilience: The Road to Business Continuity Management*

Since the advent of ICTs, organisations regardless of type or incorporation, operate in a networked – interconnected – world. ICT has changed the way modern organisations conduct their daily operations. This change has allowed organisations to streamline their operations, thus increasing productivity and ultimately – profit. The transformation toward ICT has not only emphasized the importance of protecting the information traversing these systems, but critically, the importance of ensuring the availability of the information and the systems it resides on.

The unavailability of ICT through some type of disaster or event can hold significant consequences for an organisation, not only from a fiscal perspective, but also from a reputation perspective. Herbane, Elliott, and Swartz [8] state that the effects on the reputation of the organisation may outlast the direct effects of the actual crisis if they are unable to recover ICT quickly or effectively. It is therefore critical for organisations to take

the necessary steps toward achieving some type of plan to ensure their ICT systems are available subsequently enabling the organisation to continue with daily operations.

It is fair to argue that ICT and its incumbent technologies have drastically advanced within the information age. The way organisations prepare for the continuity of these technologies also had to change. Herbane [10] says that the development of what is known today as business continuity management can most notably be attributed to the technological revolution of the 1970's. Organisations wanted to protect their data processing systems and the focus was very much with the technologies itself. Herbane [10] goes on to say that during this infancy period, the focus was very much with standby systems and critical data backups, rather than actions to prevent a failure from occurring. This period presented the advent of what came to be known as disaster recovery planning.

Disaster recovery is defined as the recovery and resumption of critical technology assets in the event of a disaster and may include resuming individual systems or all critical aspects of the ICT environment [11]. The emphasis here is two-fold, the first being on ICT systems instead of the business as a whole and secondly, that of recovery, implying a post-incident response approach. The concern with disaster recovery resides in the lack of continuity of business operations whilst ICT is recovering in the background. Partly due to this issue, the limitations of a computer centre focused disaster recovery planning approach were called into question in the mid-1980s [10].

Herbane [10] states that recognition grew throughout major world events, which included terrorist attacks among others, that an organisation-wide approach was needed to take precedence over ICT focused disaster recovery. This recognition would later see the realisation of business continuity management. Business continuity management enabled an industry focus-shift, away from data centre recovery planning, to one where organisational functionality and processes are considered as the start and end points for proper organisation-wide availability [12]. Simply put, business continuity management could be described as the activity that takes place before an incident occurs, and disaster recovery which happens afterwards [9].

The International Standards Organisation [13] defines business continuity management in its standard as: "*a holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realized, might cause and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities*". The main notion within the definition is that of organisation-wide resilience which holds many benefits if implemented.

According to Herbane, Elliott and Swartz [8], business continuity management has evolved into a process that identifies an organisation's exposure to internal and external threats and synthesises hard and soft assets to provide effective prevention and recovery. In essence, business continuity management has brought about the ability for an organisation to be prepared for incidents or disaster events alongside its recovery capabilities. It allows not only for the recovery of ICT and information systems, but for the continuance of normal business operations whilst ICT recovers. However, it is important that business continuity management not be confused with contingency planning.

As a type of 'Plan-B', contingency planning refers to tactical solutions addressing a core resource or process [11]. In contrast to business continuity management, contingency planning is typically an isolated action and does not resemble a program or series of actions for continuity [11]. In essence, contingency planning can thus be described as a workaround that might be instigated if ICT systems were disrupted. Contingency planning is, rather, an element of business continuity management, which accompanied by disaster recovery and other elements such as: risk assessment, business impact analysis and risk mitigation, brings business continuity into one cohesive and comprehensive unit [9].

It is evident – starting from a computer-oriented disaster recovery approach during the technological revolution, up until the mature business continuity management activities we see in modern day organisations – that there has been a shift from post-incident recovery, to pre-incident resilience. Many different terms and concepts have been used to describe recovery and continuity activities in the past, but owing to the realisation of its importance, organisations now operate in an age where standardisation has eliminated confusion and promoted worldwide collaboration to enhance business continuity holistically. However, with this in mind it is critical, that the importance of ICT within an organisation’s business continuity activities not be devalued. Therefore, we have seen the advent of the concept of ICT Readiness for Business Continuity. This concept and its context will be discussed next.

### 3.2 *ICT Readiness in the Modern Organisation*

ICT, as detailed before, remains a critical enabler for organisational activities. The shift from disaster recovery to business continuity management should therefore not disregard the importance of having available ICT systems. Should a misalignment between the organisation’s business continuity and its ICT disaster recovery exist, it could have damaging consequences if a disruption were to occur. Aligning the ICT disaster recovery to business continuity is unfortunately not as simple as one would think, partly due to a different focus. In essence, as mentioned earlier, disaster recovery plans are written with post-incident recovery in mind, whereas business continuity focuses on prevention [14].

To address this misalignment, the British Standards Institution published the British Standard 25777 in 2008 as a code of practice for ICT Continuity Management, to help organisations plan and implement an ICT continuity strategy [14]. The aim of this standard was to align ICT continuity within the framework of business continuity management, which were provided by the 25999 British Standard published in 2006 [14]. The BS 25777 standard promotes ICT continuity as a holistic program-management activity, and helps the user gain a thorough understanding of the ICT requirements for business continuity [15].

The shift toward ICT continuity, which supports the overall business continuity management in the organisation, has allowed the required ICT services to be resilient and able to recover to the predetermined timeframes as required by top management [14]. The effectiveness of this approach has resulted in its adoption by the International Standards Organisation (ISO). The ISO/IEC 27031 [16] standard, which was officially published in 2011, officially replaces and supersedes the BS 25777 [15]. However, the ISO/IEC 27031 standard has introduced the concept of ICT Readiness for Business Continuity, thus effectively moving away from ICT continuity terminology. Much of the content of ICT continuity management remains the same in ICT Readiness for Business Continuity.

ICT Readiness for Business Continuity (IRBC), as the name suggests, involves readying or preparing the ICT environment for the business continuity management activities and its related objectives, in the organisation. The official definition of IRBC is: “*the capability of an organisation to support its business operations by prevention, detection and response to disruption and recovery of ICT services*” [16]. This directly translates to the objective of implementing strategies that will reduce the risk of disruption to ICT services as well as respond to and recover from a disruption [17].

This approach toward resilience through risk reduction, prevention and effective response is clearly documented within the ISO/IEC 27031 standard. ISO/IEC 27031 centres itself upon five key principles [16]. These principles are listed in Table 1 and clearly outline the core of IRBC. It is evident that the principles of IRBC supports the notion of an all-inclusive approach, from preventing ICT incidents, right through to continually improving and learning from incidents that have already occurred. Crucial to the effectiveness of the ISO/IEC 27031 standard, is the introduction of a management system to address IRBC,

which aligns to the broader business continuity management system defined in the ISO/IEC 22301 standard for business continuity management [17].

*Table 1: Principles of IRBC [16]*

Principle	Description
<b>Incident Prevention</b>	Protecting ICT services from threats, such as environmental and hardware failures, operational errors, malicious attack, and natural disasters, is critical to maintaining the desired levels of systems availability for an organization.
<b>Incident Detection</b>	Detecting incidents at the earliest opportunity will minimize the impact to services, reduce the recovery effort, and preserve the quality of service.
<b>Response</b>	Responding to an incident in the most appropriate manner will lead to a more efficient recovery and minimize any downtime. Reacting poorly can result in a minor incident escalating into something more serious.
<b>Recovery</b>	Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data. Understanding the recovery priorities allows the most critical services to be reinstated first. Services of a less critical nature may be reinstated at a later time or, in some circumstances, not at all.
<b>Improvement</b>	Lessons learned from small and large incidents should be documented, analysed and reviewed. Understanding these lessons will allow the organization to better prepare, control and avoid incidents and disruption.

The ISO/IEC 22301 standard, published in 2012, is a standard for business continuity management and defines a management system approach which is also adopted by ISO/IEC 27031 for IRBC. This approach, namely the Plan-Do-Check-Act management system, creates a continual lifecycle for implementing IRBC, starting from a planning phase and continually reviewing IRBC through monitoring and improvement activities. It is this management system which ultimately aligns IRBC to business continuity management. If implemented effectively alongside business continuity, the result may be an ICT environment that is as resilient as the organisation itself, effectively bridging the gap between ICT and business continuity.

This subsection has discussed the inception of ICT continuity and its eventual development into what is now referred to as IRBC. It has furthermore elaborated on the most important aspects of IRBC.

As a whole, Section 3 has explored the origins and evolution of ICT and business continuity and highlighted important differences between several continuity concepts. Finally, IRBC was discussed. The following section will look at an approach toward enhancing ICT readiness in local government.

#### **4. Enhancing ICT Readiness for Business Continuity in Local Government**

The previous section has captured the ICT continuity landscape, from disaster recovery to business continuity, and toward the end introduced the concept of IRBC. This section will aim to address the lack of ICT continuity in local government, as identified by the Auditor-General of South Africa, by proposing a model for the operation of IRBC. Finally, a process for the implementation of IRBC will be suggested to ultimately assist local government to prepare their ICT environment for business continuity.

##### *4.1 Municipal ICT Readiness for Business Continuity Model*

A brief explanation of the proposed model and each underlying element will follow. A model should in essence, as supported by Tomhave [7] in Section 2, enable comprehension of different elements and inter-relationships without any exhaustive explanation. Figure 2 depicts the proposed Municipal ICT Readiness for Business Continuity Model. This model

illustrates the internal and external elements to consider when implementing IRBC in local governments in South Africa, and throughout Africa. It also depicts the use of the Plan-Do-Check-Act management system, to plan, implement and continually improve IRBC.

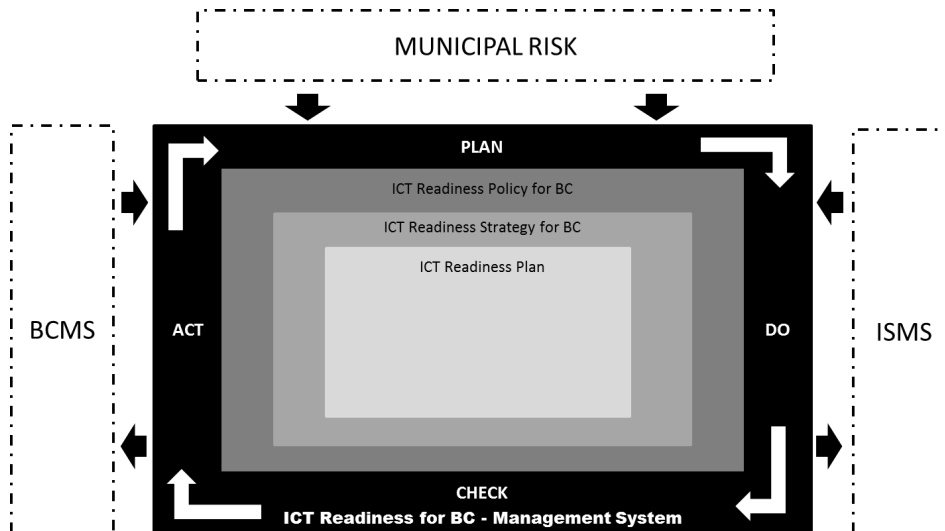


Figure 2: Municipal ICT Readiness for Business Continuity Model

Starting with the external elements of IRBC, the first major element is that of ‘Municipal Risk’. ICT is vulnerable to a multitude of different threats which, if realised, can cause harm to systems and organisational reputation through rendering ICT unavailable. ISO/IEC 27031 supports this notion in stating that IRBC should enable the organisation to respond to the constantly changing risk environment [16]. Therefore, ‘Municipal Risk’ should be considered as a vital input in the operation of IRBC.

The second external element which provides both input and output to IRBC is that of the local government’s ‘Business Continuity Management System (BCMS)’. Section 3 emphasized the relationship between IRBC and business continuity management and indicated the interdependence existing between them. ISO/IEC 27031 also states that IRBC supports and ultimately complements the BCMS, as well as the Information Security Management System (ISMS) [16]. From an implementation perspective, IRBC is also dependent on the outcome of a business impact analysis, conducted as part of the BCMS [16]. This will be discussed further in subsection 4.2.

The final external element for IRBC in local government is the relationship with the local government’s ‘ISMS’. An ISMS aims to safeguard the confidentiality, integrity and availability of organisational data [3]. This organisational data resides on the ICT systems of every local government. Thus, it is critical to ensure collaboration between the IRBC and ISMS activities to not only allow the availability of data, but support its confidentiality and integrity.

Element	Description
<b>Skill &amp; Knowledge</b>	Includes consideration regarding the specialized technical skills and knowledge needed to operate ICT services before, during and after a disruption. Strategies that include skill and knowledge considerations focus on ensuring no single individual holds specialized skills or knowledge that would be needed to operate the organization's ICT systems.
<b>Facilities</b>	Includes mitigating risk associated with operating ICT systems based in a single facility. Strategies that include facility considerations ensure ICT systems can be operated even if a primary facility is rendered inoperable.
<b>Technology</b>	Includes consideration of the technical requirements needed to meet the organization's recovery requirements, specifically Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Strategies that include technology considerations involve ensuring hardware and applications are able to be recovered within the time and data recovery required by the organization. These considerations must include support systems such as power, cooling, staffing, vendor support and WAN connectivity.
<b>Data</b>	Includes consideration of how to protect the data required by the organization. Strategies that include data considerations include security, validity and availability of the data required by end users.
<b>Processes</b>	Includes consideration of how to sustain the processes necessary to monitor, operate and recover ICT systems in order to meet business requirements. Strategies that consider processes identify the ICT processes necessary prior to, during and after a disruption to ICT systems.
<b>Suppliers</b>	Includes consideration of how to inform and engage suppliers who are needed to recover and operate ICT systems. Strategies that include supplier considerations identify what suppliers are engaged in the operation and recovery of ICT systems before, during and after a disruption has occurred.

Table 2: Strategy Elements for IRBC [17]

Core to this model is the IRBC management system, which contains three internal elements to consider for operation of IRBC. The same Plan-Do-Check-Act approach used for BCMS in ISO/IEC 22301 is used in ISO/IEC 27031 but is adapted to fit the technical nature of IRBC [17]. Plan-Do-Check-Act is a simple approach which basically allows each element in the IRBC management system, to be implemented holistically and continually monitored and improved. This is an iterative process for the complete IRBC lifecycle.

The first internal element of IRBC is the IRBC policy. This is a strategic policy and should provide the local government with documented principles to which it will aspire, and against which its IRBC effectiveness can be measured [16]. The objectives, scope and responsibilities, among others, should be delineated within the policy. Through the policy, senior management should drive, endorse and promote IRBC in order for it to be effective [16]. Taking the aforementioned into account, we can argue that the acceptance of an IRBC policy at senior level is critical, especially in the infancy phase of IRBC.

The second internal element of IRBC is the IRBC strategy. The IRBC strategy should define the approaches to implement the required resilience so that the principles of IRBC, as mentioned in Section 3, are put in place [16]. The strategy options selected, should be evaluated to ensure it is capable of supporting the business continuity requirements of the local government, as well as take note of resource requirements to keep it in line with the financial and administrative capacity of the local government [16]. The strategy options that are selected, need to incorporate six components termed 'strategy elements', into monitoring for, responding to and recovering from disruptions to ICT [17]. These strategy elements as described by Marbais [17] are listed in Table 2.

The final element of IRBC is the ICT readiness plan. ISO/IEC 27031 [16] states that the local government should have documentation to manage potential disruption and thereby enable continuity of ICT services and the recovery of critical activities. They further explain that small local governments may have a single document that encompasses all recovery activities [16]. In contrast, the ICT readiness plan in large local governments would include a comprehensive set of documents addressing, among other things, an awareness - and training program, ICT response and recovery plans like the incident

response and disaster recovery plan, strategy implementation plan and specific IRBC processes [16]. All the elements in the Municipal ICT Readiness for Business Continuity Model, both internal and external, represent the operation of IRBC within local government.

#### 4.2 A Process for the Implementation of IRBC in Local Government

As mentioned in Section 2, this paper forms part of a larger ongoing research study. The ultimate goal of the study is to yield a useable artefact to assist local government to implement ICT Readiness for Business Continuity. With this in mind, this subsection suggests a process, based on the Municipal ICT Readiness for Business Continuity Model, depicted in Figure 2. The initial proposal is an automated application that runs within Microsoft Excel. The use of Excel is mainly to eliminate application incompatibility issues. Using the model proposed in Section 4.1 as the foundation, supported by the requirements of the ISO/IEC 27031 standard, the application content and ultimate output should comply with international best practices. Figure 3 illustrates the process for the application.

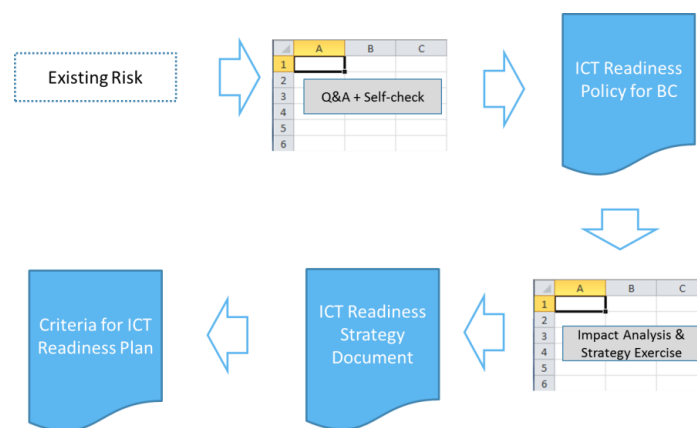


Figure 3: Process for the Implementation of IRBC in Local Government

The Excel application should yield three documents upon completion. These include: (1) an IRBC policy; (2) an IRBC strategy; and (3) a criteria document for the IRBC plan. Firstly, the responsible party takes into account the existing risk to ICT and does a ‘question and answer’-based exercise that is designed using requirements for the IRBC policy given by the ISO/IEC 27031 standard. Answering ‘yes’ to questions will reverse engineer the specific question into a policy statement. Should the answer be ‘no’, a self-check flag will appear to indicate possible consequences, to which the responsible party must agree to accept accountability for.

Once the IRBC policy is generated the application is taken over by the person indicated in the policy as responsible for IRBC. The application has to take into account the possibility that not all local governments have a BCMS implemented, and subsequently, no business impact analysis (BIA) activities have therefore taken place. The main requirement of the BIA for IRBC is to identify the critical ICT services and define recovery objectives for each. Marbais [17] suggests an alternative to the BIA, and states that an easy way to develop recovery requirements is to conduct a more focused application impact analysis (AIA).

The AIA focuses on the use of ICT services and measures the impact on the organisation that a disruption might hold [17]. The AIA in a local government should

effectively identify key ICT systems, the level of impact of a disruption to ICT and define recovery objectives for those ICT systems. The person responsible for IRBC implementation will therefore conduct an AIA, followed by a strategy exercise.

The strategy exercise will ultimately allow the user to select IRBC strategy options based on the six strategy elements of IRBC, as seen in Table 2. These options are directly derived from the ISO/IEC 27031 standard. A strategy document will be generated upon completion of the exercise.

Lastly, a final document will be generated, detailing criteria for the IRBC plan based on the options chosen during the strategy exercise. The main reason for the criteria document is the fact that each local government's ICT environment differs, and with recovery plans being very technically specific, it is unfeasible to produce such a plan generically. Therefore, criteria for an IRBC plan will be suggested to assist the user with designing an IRBC plan based on the selected strategies.

A process for the functioning of an Excel-based application to aid local government in implementing IRBC has been argued and proposed above. Section 4, above, proposed the Municipal ICT Readiness for Business Continuity Model illustrating the operation of IRBC in local government.

## 5. Conclusion

Local government has the responsibility of providing sustainable services to its communities. ICT functions as a critical enabler within local government to assist in this regard. It is therefore essential that these ICT services are resilient and able to recover within acceptable timeframes. However, the problem identified within this paper, is a lack of adequate ICT continuity controls in the majority of South African local governments. The objective of this paper was therefore to propose a model to address this problem.

The Municipal ICT Readiness for Business Continuity Model, proposed in this paper, proposes a scaled-down approach for the operation of an IRBC management system in local government. The model illustrates external and internal elements that should be considered for IRBC as well as the Plan-Do-Check-Act management system lifecycle to operate and continually improve IRBC. The paper also suggested an implementation process through the development of a usable artefact, which form part of a larger research study, and briefly discussed each proposed process stage. Using the model as a basis in parallel with the requirements set out in relevant standards, should enable even lesser capacity local governments to implement sound IRBC structures. Although this study is based on a problem in South Africa, the proposed model is applicable to similar local government structures throughout the continent of Africa.

Further research is currently being done to automate the implementation of IRBC in local government. This automation, in the form of an application, should help local government to have the correct structures in place, based on international standards, for their ICT to be as resilient as possible. The approach should allow for a generic IRBC implementation that fits the financial and administrative capacity of each local government. Further results of the study will follow in due time.

## Acknowledgement

The authors hereby acknowledge the financial assistance of the National Research Foundation (NRF) and Nelson Mandela Metropolitan University (NMMU) towards this research. Opinions expressed and conclusions arrived at, are those of the authors and not necessarily that of the NRF or NMMU.



## References

- [1] The Bill of Rights of the Constitution of the Republic of South Africa. (1996). *Government Gazette (No. 17678)*.
- [2] Auditor-General of South Africa. (2014). *Consolidated general report on the audit outcomes of local government 2012-13*. AGSA.
- [3] Botha, J., & von Solms, R. (2004). A cyclic approach to business continuity planning. *Information Management & Computer Security*, 12(4), 328-337.
- [4] Auditor-General of South Africa. (2015). *Consolidated general report on the audit outcomes of local government 2013-14*. AGSA.
- [5] Olivier, M. S. (2009). *Information Technology Research - A Practical Guide for Computer Science and Informatics* (3rd ed.). Pretoria: Van Schaik.
- [6] Pacific Research and Evaluation Associates. (2010). *Semi-structured Interview*. Retrieved November 23, 2015, from Evaluation Toolbox: [http://evaluationtoolbox.net.au/index.php?option=com\\_content&view=article&id=31&Itemid=137](http://evaluationtoolbox.net.au/index.php?option=com_content&view=article&id=31&Itemid=137)
- [7] Tomhave, B. L. (2005). *Alphabet Soup: Making Sense of Models, Frameworks, and Methodologies*. Retrieved November 23, 2015, from [www.secureconsulting.net/Papers/Alphabet\\_Soup.pdf](http://www.secureconsulting.net/Papers/Alphabet_Soup.pdf)
- [8] Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business continuity management: time for a strategic role? *Long Range Planning*, 37(5), 435-457.
- [9] Stanton, R. (2005). Beyond disaster recovery: the benefits of business continuity. *Computer Fraud & Security*, 18-19.
- [10] Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, 52(6), 978-1002.
- [11] Protivity Inc. (2013). *Resource Guides*. Retrieved November 25, 2015, from Protivity: <http://www.protiviti.com/en-US/Documents/Resource-Guides/Guide-to-BCM-Third-Edition-Protiviti.pdf>
- [12] Jackson, C. B. (2002). The changing face of continuity planning. *Information Systems Security*, 10(6), 18-21.
- [13] ISO/IEC. (2012). ISO 22301:2012 Societal security — Business continuity management systems — Requirements. Geneva, Switzerland: ISO/IEC.
- [14] Hamidovic, H. (2011). An Introduction to ICT Continuity Based on BS 25777. *ISACA Journal*, 2(45).
- [15] British Standards Institute. (2008). *BS 25777:2008*. Retrieved December 26, 2015, from BSI Group: <http://shop.bsigroup.com/ProductDetail/?pid=000000000030166966>
- [16] ISO/IEC. (2011). Information technology — Security — Guidelines for information and communication technology readiness for business continuity. *ISO/IEC 27031:2011*. Geneva, Switzerland: ISO/IEC.
- [17] Marbais, G. (2012, November 9). *Using ISO 27031 to Guide IT Disaster Recovery Alignment with ISO 22301*. Retrieved from Avaluation's Perspective on Business Continuity & Disaster Recovery: <http://perspectives.avalution.com/2012/using-iso-27031-to-guide-it-disaster-recovery-alignment-with-iso-22301/>

### **A.3 Journal of Public Administration (Submitted)**

*This paper, titled ‘An Approach towards ICT Readiness for Business Continuity in Local Government’ was submitted to the South African Journal of Public Administration. This paper was written upon completion of the study to present the final M-IRBC. It is currently (November 2016) under review.*

# An Approach towards ICT Readiness for Business Continuity in Local Government

## Abstract

ICT enables enterprises, regardless of sector, to fulfil their strategic objectives. Similarly, ICT is critical in enabling municipalities within South Africa to deliver sustainable services to their communities. This dependence on ICT therefore necessitates a resilient ICT environment where minimal disruption is the primary focus. Unfortunately, as reported by the Auditor-General, the majority of South African municipalities are neglecting to adequately address the continuity of their ICT services. This restricts these municipalities to achieve their strategic goals and to fulfil the constitutional mandate of service delivery. It is therefore the objective of this paper to propose an approach, founded on a theoretical foundation, to assist municipalities in addressing a real-life ICT continuity problem. The theoretical foundation, derived from best practice and standards, will introduce the concept of ICT readiness for business continuity. Furthermore, by taking into account various challenges within local government, a tailored approach will ultimately help municipalities to help themselves in this regard. In order to achieve this objective, this paper has followed a cyclical research approach, in which the outcome was refined with multiple cycles of surveys conducted with municipalities. This cyclical process has resulted in a tailored self-help approach, in order for municipalities to plan and implement ICT readiness for business continuity.

**Keywords:** ICT, Recovery, Resilience, Continuity, ICT Readiness for Business Continuity (IRBC), Business Continuity (BC), Local Government, Municipalities

## 1. Introduction

Information and Communication Technology (ICT) has developed into a pervasive commodity within all sectors of business, both locally and throughout the world (IODSA, 2010). As Coertze and Von Solms (2012) state, ICT is essential in managing the information and knowledge required in the daily operation of organizations, and thereby significantly contribute to their success. ICT is, therefore, a major driver for enterprises within these sectors to achieve their strategic objectives. This holds true within the South African government as well, particularly local government, where ICT has become a critical enabler for service delivery (Auditor-General of South Africa, 2014).

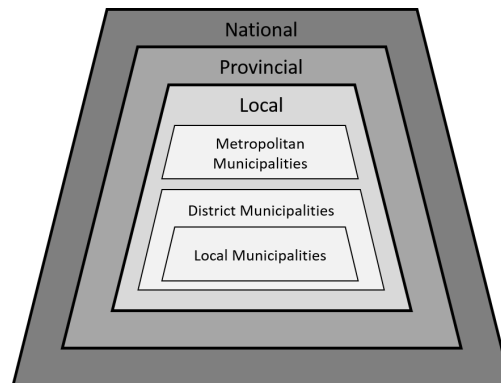


Figure 1: South African Government Structure

According to Cameron (2001), South Africa has one of the most advanced local government systems in the world. As illustrated in Figure 1, the structure of South African government consists of three spheres of government, namely: The national-, provincial- and local spheres of government (*Constitution of the Republic of South Africa, 1996*). Importantly, this notion makes each sphere of government distinctive, interdependent and interrelated (Cameron, 2001). Local government is further divided into three categories of municipalities, referred to as metropolitan-, district- and local municipalities; whereas district municipalities consist of multiple local municipalities within their geographical location (*Constitution of the Republic of South Africa, 1996*).

The primary focus of this study is vested in district municipalities and their local municipalities, henceforth referred to as municipalities, which in most cases lack adequate resource capacity.

The Constitution of South Africa (1996) mandates local government, to deliver sustainable services to its communities. It is, therefore, critical for municipalities to have proper ICT systems in place. More importantly, these ICT systems have to be available continuously. Cerullo and Cerullo (2004) explain that the dependence on ICT systems has broadened the potential causes of ICT disruptions; and it is therefore critical that enterprises quickly respond. Hence, priority should be given to proper ICT continuity practices, promoting resilient and recoverable ICT systems within municipalities. Unfortunately, the Auditor-General of South Africa has reported that this is not the case.

The Auditor-General of South Africa conducts annual audits of, amongst others, local government. In the audit reports from the 2011/12 financial year up to the latest 2013/14 financial year, the Auditor-General identified ICT as a key risk area within local government

(Auditor-General of South Africa, 2013, 2014, 2015). ICT continuity is subsequently highlighted in these reports, as one of four major shortcomings within the ICT function in local government. The Auditor-General emphasizes that ICT should not only ensure the confidentiality, integrity and availability of State information; but it should enable service delivery, and promote national security (Auditor-General of South Africa, 2015). It is therefore critical that ICT is resilient, and be able to recover, should any disruptions occur. This does not seem to be the case; since the state of ICT continuity controls in local government is questionable.

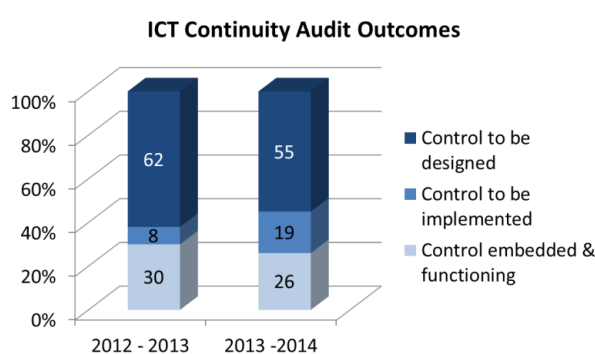


Figure 2: Comparison of Latest Local Government Audits

Reports from the local government audit of the last two financial years indicate that a majority of municipalities have failed to implement adequate ICT continuity controls. As seen in Figure 2, during the 2012/13 financial year, 62% of municipalities failed to design any ICT continuity controls – rendering those municipalities vulnerable to prolonged ICT downtime – should any disruptions occur (Auditor-General of South Africa, 2014). The more concerning finding, however, is that between the two audit years, there has been a decline of 4% in the number of municipalities that have embedded and functioning ICT continuity controls; whilst the majority still do not have any controls designed (Auditor-General of South Africa, 2015).

This is a significant finding, because even though government has tried to address these concerns through various initiatives since the 2012/13 audit, the number of embedded controls has declined.

It is evident that ICT continuity is not being effectively addressed in the majority of municipalities, if addressed at all. It is also noteworthy that attempts by national and provincial government at addressing the root causes of these findings have been fruitless (Auditor-General of South Africa, 2015). The objective of this paper is, therefore, to propose a tailored approach,

founded on a sound theoretical foundation, to provide local government with a self-help method, supported by relevant practical tools, to plan and implement ICT Readiness for Business Continuity. Critically, it must be stressed that this approach comprises not just extractions from best practices; but it shapes itself around the unique challenges of local government.

This paper commences by briefly discussing the research approach, leading to an exploration into the previous attempts by government to address the shortfalls of ICT, specifically continuity, and trying to gauge what the challenges are that hamper current attempts. This is followed by a brief look at the current business- and ICT-continuity environment, and specifically discussing the concept of ICT Readiness for Business Continuity – as a more structured method – to address the continuity aspect of ICT.

An approach for ICT Readiness for Business Continuity, supported by practical tools that are tailored to the challenges of municipalities, will be proposed. Finally, validation results will be reported on, whereupon the paper will be concluded.

## **2. Research Design**

To address the inadequacies of ICT continuity controls, as reported by the Auditor-General, and to achieve its objective, this paper, as part of an ongoing research project, has followed a design-oriented research approach – with the goal of producing a practical artefact. In essence, a real-life industry problem has been identified; and the goal is to provide an approach towards this problem situation.

Due to the complexity of local government and how it functions, paired with its limitations, this research has adopted a cyclical approach. In order to start addressing the problem, a theoretical foundation was drafted through the literature, as part of the first research cycle. However, this theoretical foundation still required various practical cycles of refinement, before developing a prototype, which fits the unique environment of local government.

To refine the approach, a district municipality that has had multiple clean audits in past years, was approached to assist in this regard. The main aim was not to mould this approach to this municipality, but to rather tailor it to municipalities in general. During each cycle, through the use of semi-structured interviews, the approach was fine-tuned and adapted to the needs of local government in general, taking into account the different challenges faced in this government sphere, until an acceptable approach had been developed; and both parties were satisfied with the outcome. This approach was validated by using a workshop, which 22

municipal representatives attended. The following section will explore the different attempts by government to address the poor state of ICT controls in municipalities, and attempt to reason towards principles for the approach to pursue.

### 3. ICT Continuity in Local Government

ICT continuity promotes an available ICT environment, without which, many enterprises would struggle to reach their objectives. It is evident, based on the audit findings of local government, that ICT continuity is not suitably addressed in the various municipalities. Before addressing this issue, it is essential to explore the attempts already made, as well as to identify the challenges preventing the successful implementation of ICT continuity. This section will elaborate on these matters.

#### 3.1 Government Attempts at Addressing Continuity and Related ICT

Modern-day enterprises cannot deny the strategic importance of ICT. The world-wide introduction of laws, standards and best practices, like the King Code on Corporate Governance for South Africa (IODSA, 2010), the American Sarbanes-Oxley Act (Act, 2002), as well as the ISO/IEC 38500 standard (ISO/IEC, 2008), to name only a few, ratifies this notion. It would be naïve to think, noting the identified issues of ICT continuity in municipalities, that government in South Africa has not realised the strategic importance of ICT. In fact, this realisation came as early as 1998. The Presidential Review Commission (PRC) Report of 1998 (Presidential Commissioners, 1998), which emphasized the importance of ICT, stated that important ICT decisions should not be delegated to the technologists; but they should stem from senior political and managerial leadership (Presidential Commissioners, 1998).

Figure 3 illustrates the progression of government initiatives to address ICT, since the release of the PRC Report.

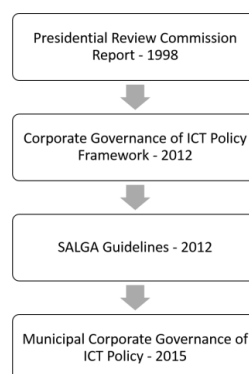


Figure 3: Timeline of Government ICT Initiatives

The PRC Report emphasized the need for ICT to be aligned to government business goals (Presidential Commissioners, 1998). Sadly, ten years after the publication of the PRC Report, the Auditor-General reported that little has happened with regard to ICT governance, which directly affects ICT continuity. The Auditor-General subsequently recommended that a government-wide governance of ICT framework be implemented to address any ICT risks, which would, in turn, address the continuity of ICT (Department: Public Service and Administration, 2012).

The governance framework recommended by the Auditor-General in the 2008/09 report materialised during 2012, addressing both the corporate governance- and governance of ICT, with all its inherent risks, including ICT continuity. This framework, namely the Corporate Governance of ICT Policy Framework (CGICTPF), aims to institutionalise ICT, as an integral part of corporate governance within government departments; and it was to be implemented in three-phases (Department: Public Service and Administration, 2012).

Importantly, the CGICTPF is applicable to all spheres of government (Department: Public Service and Administration, 2012), which made this the guiding ICT document at that time for municipalities.

The CGICTPF requires, as part of the implementation of Phase 1, a Business Continuity Plan, which in turn, informs a Business Continuity Strategy, a Business Continuity Policy and an ICT Continuity Plan (Department: Public Service and Administration, 2012). Being a governance framework, one would not expect the CGICTPF to provide much detail. The CGICTPF is, however, a very high-level and complex document; and municipalities with resource-capacity limitations have struggled to implement it within the timeframes set out for each of the implementation phases (Department: Western Cape Local Government, 2015a). In support, the South African Local Government Association (SALGA) has drafted a guidance document to assist municipalities in this regard.

The SALGA guidelines are aligned with the CGICTPF; and they provide municipalities with more guidance on the governance of ICT (SALGA, 2012). However, on the issue of ICT continuity, the SALGA guidelines do not provide much more detail than the CGICTPF itself. Instead, it provides guidelines in the form of short-term goals, without further explanation, which might hinder the implementation at municipalities with resource deficiencies. In essence, both the CGICTPF and the SALGA guidelines only address WHAT has to be done; and they do not provide any detail on HOW it should be done. The lack of implementation guidance has become evident in the subsequent audits of local government.



As seen in Section 1, the Auditor-General reports a decline in municipalities with embedded ICT continuity controls (Auditor-General of South Africa, 2015). This finding comes two years after the publication of the CGICTPF and the SALGA guidelines, resulting in municipalities exceeding the deadline for ICT continuity implementation, as required by Phase 1 of the CGICTPF (Department: Public Service and Administration, 2012), by one year.

In the 2013/14 audit report, the Auditor-General in response notified that the CGICTPF had been customized specifically for local government and the Municipal Corporate Governance of ICT Policy (MCGICTP) (Department: Western Cape Local Government, 2015b), was drafted for that purpose (Auditor-General of South Africa, 2015).

The MCGICTP aims to address the inadequacies of the CGICTPF and to cater for local government specifically (Department: Western Cape Local Government, 2015b). However, although this new policy is set to be implemented in the 2015/16 financial year, little has changed. A critical analysis of the draft MCGICTP, against the CGICTPF, indicates that it is predominantly the same. The MCGICTP again addresses WHAT must be done, with very little guidance as to HOW it should be done. It can be argued that the MCGICTP will not be of much help, when taking into account the unique challenges faced by municipalities.

The following subsection will aim to identify some of the main challenges that are hindering municipal attempts at implementing proper ICT controls.

### **3.2 The Capacity Challenge in Local Government**

The concerning findings from the Auditor-General reports in the past several years have given little, or no reason, for municipalities to ignore the major inadequacies of their ICT controls, and in this case of ICT continuity. Municipalities require proper ICT continuity; but as seen in the previous subsection, past and present initiatives have proven fruitless in overcoming what seems to be an overwhelming number of challenges. To address this real-life problem, it is essential to consider the challenges in municipalities. These challenges predominantly revolve around capacity.

Capacity, in a municipal sense, refers to the availability of and access to tangible resources which include human-, financial-, material-, or technological resources, and furthermore to have the knowledge to implement policies and deliver public services (Brynard & De Coning, 2006). Capacity also refers to intangible resources, for instance commitment to, and leadership for, the implementation and delivery of public services (Brynard & De Coning, 2006).

It is fair to argue, that the lack of capacity in municipalities, both in terms of tangible and intangible resources, will ultimately nullify their efforts of implementing effective ICT continuity controls.

In the case of local government, unfortunately, one size does not fit all. In their guidelines, SALGA states that cognisance must be taken that low, medium and higher capacity municipalities, across all classes of the local government sphere, exist (SALGA, 2012). Furthermore, SALGA deduces five distinct categories of municipalities, based on their fiscal capacity and resource availability; and subsequently, they have found that about 30% of municipalities fall into the ‘poor resources and low-capacity’ category (SALGA, 2012). The Auditor-General also points out budget constraints, limiting the development of ICT policies and procedures (Auditor-General of South Africa, 2014, 2015). Therefore, it is essential that municipalities, and especially those who fall into the ‘poor resources and low-capacity’ category, be facilitated by a *SCALABLE* approach, which is appropriate to their capacity.

Human-resource capacity, including skills and knowledge, are critical to the success of any ICT undertaking. Kanyane (2006) notes that amongst others, weak leadership in strategic management, including corporate governance, the misplacement of skills within municipalities, and the political considerations in appointments of senior managers, without the requisite qualifications, has tremendously weakened the performance of municipalities.

Specifically, with regard to ICT, SALGA stated that because of a large skill shortage, ICT staff in many municipalities are made up of underqualified professionals with watered-down skills that are not capable of handling real-life ICT challenges (SALGA, 2012). This is supported by the Auditor-General, who reports a lack of skills to appropriately design and implement ICT controls (Auditor-General of South Africa, 2014, 2015). Thus, it is clear that there is a knowledge and skills shortage in municipalities; and essentially, this requires a *SIMPLISTIC* and *COMPREHENSIBLE* approach to the problem.

In many cases, laws that have good intentions may also be a thorn in the path of progress. Municipalities in South Africa are self-governing entities, subject to conformance with provincial and national legislation; and with regard to ICT therefore operate in a very isolated non-uniform manner (*Constitution of the Republic of South Africa*, 1996; SALGA, 2012). Consequently, the different municipal ICT environments might differ, from both a topological and a technological perspective; and therefore also, their software and hardware resources might differ. Therefore, any approach using practical tools to help local government, should be *USABLE* in any environment, enabling functionality within the greater majority of municipalities, irrespective of their technological capabilities or differences.

Table 1: Principles for ICT Continuity in Local Government

Principle 1: <b>Scalable</b>
Principle 2: <b>Simplistic</b>
Principle 3: <b>Comprehensible</b>
Principle 4: <b>Usable</b>

Government has attempted via various initiatives to address the inadequacies of ICT in local government; but it has fallen short in most cases. Table 1 lists the principles identified by taking into account the resource-capacity challenges in municipalities. The approach for the municipal ICT continuity problem, which is proposed in this study, should aim to adhere to these principles, in order to make it more suitable and acceptable to the municipal environment. Therefore, through using such an approach, municipalities should benefit by being able to help themselves, in addressing their ICT continuity problems.

In essence, this section has specifically explored the current government attempts to address various ICT inadequacies, including ICT continuity; but unfortunately, only addressing WHAT should be done. Furthermore, to aid in the development of a tailored approach to address the ICT continuity problem, this section has identified various principles, arrived at by taking into account the different capacity constraints and the challenges in municipalities. The following section will briefly explore continuity and the progression from recovery to resilience, looking at different components, and ultimately introducing ICT Readiness for Business Continuity.

#### **4. Continuity: The Shift from Recovery to Resilience**

If ICT were to become unavailable beyond the durability of the enterprise, it might hold irreparable consequences. Herbane, Elliot and Swartz (2004) state that the effects on the reputation of the enterprise might outlast the direct effects of the actual disruption – should the enterprise be unable to recover ICT quickly or effectively. Efforts toward continuity have consequently seen a shift from recovery, to resilience.

The progression from recovery to resilience of ICT has not only evolved – due to the innovation of new technologies, but because of its strategic business importance. As Herbane, Elliot and Swartz (2004) stated, enterprises have not only recognised the need for an approach towards continuity beyond mere ICT disaster recovery, but have linked business continuity

management to strategically important dimensions of their operations. There is, however, still some confusion about the differences between disaster recovery and business continuity; where terms are used interchangeably – whilst a clear difference in function exists (Stanton, 2005).

The focus of disaster recovery is two-fold, firstly the notion of recovery, which indicates a post-incident response approach, and secondly a focus on ICT, instead of the business as a whole. This aspect is clear from the fact that disaster recovery is defined as the recovery and resumption of critical technology assets – in the event of a disaster – and this may include resuming individual systems, or all critical aspects of the ICT environment (Protiviti Inc, 2013). Although disaster recovery still has a role to play, this approach in isolation has become rather dated, and the limitations of such an approach have been called into question (Herbane, 2010).

Over the years, following numerous incidents and disasters, it has become apparent that an enterprise-wide approach was needed; ultimately taking precedence over ICT-focused disaster recovery (Herbane, 2010). This enterprise-wide approach was needed to ensure that business continues as normal, following some incident or disaster. The result was business continuity, defined as the capability of an enterprise to continue with the delivery of products or services at acceptable predefined levels following some disruptive incident (ISO 22301, 2012).

Granted, disaster recovery would still play a major role as part of business continuity. This approach to continuity, rather than recovery, has enabled the shift towards resilience, focusing rather on the prevention of disruptions to business. As part of a management system, business continuity management considers functionality and processes as core to proper enterprise-wide availability (Jackson, 2002). In essence, business continuity management could be described as the activity taking place before an incident; whilst disaster recovery happens afterwards (Stanton, 2005).

It is important, however, that the emergence of business continuity, as the primary continuity approach, should not devalue the important role of ICT. Aligning ICT disaster recovery to business continuity is not a simple task, mainly because of the difference in focus. Disaster recovery plans are written with post-incident ICT recovery in mind; whereas business continuity rather focuses on the resilience of the business as a whole, in order to withstand any possible future disasters (Hamidovic, 2011). To address this misalignment, the BS 25777 British Standard was published – with the objective of aligning ICT continuity within the framework of business continuity (Hamidovic, 2011).

The BS 25777 standard promotes ICT continuity as a holistic programme-management activity; and it helps the user to gain a thorough understanding of the ICT requirements for

business continuity (BSI, 2008). Hamidovic (2011) states that the shift towards ICT continuity, and thereby supporting business continuity management, has allowed the ICT services to be resilient and to be able to recover to predetermined timeframes, as required by top management. The effectiveness of this approach has resulted in the international adoption and the ultimate replacement of the BS 25777 British Standard, by the ISO/IEC 27031 international standard (BSI, 2008).

The ISO/IEC 27031 (2011) standard, which is similar to the BS 25777 British Standard, has introduced the concept of ICT Readiness for Business Continuity (IRBC), thereby effectively moving away from the ICT continuity terminology. The content and goals of both standards, do however remain largely similar.

As the name suggests, IRBC involves preparing the ICT environment to be ready and in line with business continuity management and its incumbent activities and objectives. IRBC is officially defined as: “the capability of an organisation to support its business operations by prevention, detection and response to disruption and recovery of ICT services” (ISO/IEC 27031, 2011). This involves implementing strategies that would reduce the risk of disruption, as well as respond to and recover from disruption to ICT services (Marbais, 2012). The ISO/IEC 27031 standard centres itself around 5 key principles, namely: incident prevention; incident detection; response; recovery; and improvement (ISO/IEC 27031, 2011). These principles form the essence of what IRBC strives to achieve, and what an enterprise would get from adopting IRBC. Thus, as the more modern approach, IRBC should provide an ICT environment that is more resilient and able to recover effectively.

From the point of view of this study, it cannot be assumed that municipalities have business continuity management in place; but it is beyond the scope of this study to provide municipalities with business continuity. Rather, this study aims to provide an approach that can enable a resilient ICT environment within municipalities through sound IRBC planning, but additionally to have the ability to latch on to any existing business continuity management system, should one exist. The ability of IRBC to function in isolation, which will also be emphasized in the following section, allows this study to follow this approach, and ultimately to address the concerns of the Auditor-General.

This section has briefly discussed the evolution from recovery to resilience and introduced the origin and importance of IRBC. Considering its unique challenges, such as the lack of skills, budget-constraints and diverse operational environments, planning and implementing IRBC within local government could become a nearly impossible undertaking.

The following section will, therefore, propose a tailored approach for planning and implementing IRBC, with the aim of helping municipalities to help themselves.

## **5 A Self-Help Approach for IRBC Planning in Local Government**

As stated in Section 2, a real-life problem exists because many municipalities do not have ICT continuity controls in place; and therefore, it is the objective of this study to provide an approach to address this problem. Critically, the proposed approach should be guided by best practice, but be tailored to the unique municipal environment. Thus, the approach should address the challenges acknowledged in Section 3, by aligning itself with the identified principles listed in Table 1. This section will propose an approach to address this problem, based on a sound theoretical foundation and supported by practical tools, to assist resource-restricted municipalities to help themselves in this regard.

### **5.1 A Theoretical Foundation for IRBC in Local Government**

The theoretical foundation for IRBC in municipalities, is illustrated in Figure 4. It is adapted from the ISO/IEC 27031 standard, taking into account the unique municipal environment. It consists of the IRBC management system, based on the Plan-Do-Check-Act system lifecycle. Furthermore, external elements having both input and receiving output from the IRBC system are shown; and these comprise municipal risk, information security management activities, as well as business continuity management activities. Finally, each Plan-Do-Check-Act phase has specific outcomes.

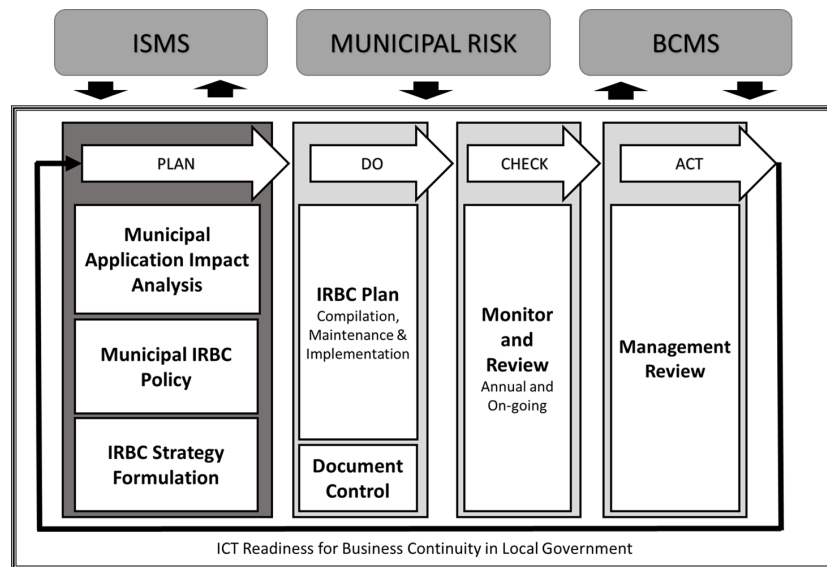


Figure 4: Theoretical Foundation for IRBC in Local Government

Although IRBC supports the enterprise business continuity management system (BCMS), it is capable of functioning on its own. Marbais (2012) states that frequently enterprises want to implement mitigation, response and recovery measures in advance of a broader business continuity management programme. This would be the case in most of the smaller municipalities, which do not have the capacity to implement a proper BCMS, but which essentially require a resilient ICT environment. IRBC, as an internationally recognised ICT continuity approach, is therefore suited to this capacity concern, because it can function within an island environment, either in isolation, or as part of an existing business continuity system. The resulting outcome is therefore a scalable approach to ICT continuity.

The ISO/IEC 27031 standard delineates the same Plan-Do-Check-Act management approach, as seen in the ISO 22301 BCMS standard; but it is, however, adapted due to the technical nature of IRBC (Marbais, 2012). Plan-Do-Check-Act is an iterative process for the entire lifecycle of IRBC. It allows each element of IRBC to be implemented holistically in the scope of the municipality, and to be continually monitored and improved.

Each step within Plan-Do-Check-Act has certain obligations and outcomes. These are illustrated in Figure 4, where the most important deliverables and actions, suited to municipalities, have been listed. These include: Firstly, the conducting of a Municipal Application Impact Analysis, which will be further discussed in subsection 5.2. Secondly, an IRBC policy, which should provide the municipality with documented principles, to which it

will aim, and against which the effectiveness of IRBC can be measured. Thirdly, an IRBC strategy, which defines different approaches to achieve resilience and to adhere to the principles of IRBC, as mentioned in Section 4 (ISO/IEC 27031, 2011). Lastly, further requirements include an IRBC plan, as well as monitoring and reviewing activities for the purpose of refining IRBC.

Having explained the theoretical basis of the municipal IRBC, the practical implementation component becomes apparent. To avoid being a copy-and-paste best-practice solution, and therefore effectively help address the problem in local government, as highlighted by the Auditor-General, further help is required. Providing municipalities with this theoretical foundation would only go half-way in achieving the goal of addressing the ICT continuity issues. As part of the overall approach, municipalities should also be provided with practical tools, to help them with the planning of IRBC, which ultimately conforms to the principles, as stipulated in Table 1.

Unfortunately, due to the technical nature of IRBC, such tools would only be able to assist with the Plan-phase of IRBC implementation, highlighted in a darker shade within Figure 4. Thus, practical tool exercises can only be made available for the Plan-phase, with some output resulting as input into the subsequent Do-phase (IRBC Plan). The rest of the requirements of the Do-, Check-, and Act-phases will remain the responsibility of the municipality. The following subsection will propose such a practical tool for the Plan-phase of IRBC.

### **5.2 A Practical Tool for Planning IRBC in Local Government**

Following is a short description of a practical tool that assists the municipal ICT personnel to perform the Plan-phase in a very scalable, comprehensible, simplistic and usable manner. The major goal of this study is to provide a practical approach for the ICT continuity problem. It is critical for this approach to meet certain principles, which are derived from the resource-capacity challenges faced by most municipalities. Due to the mentioned capacity constraints, and possibly others that are not identified within this paper, municipalities would barely be able to undertake the implementation of IRBC merely from best practices and the ISO/IEC 27031 alone. It is fair to argue that the standard delineates a perfect world scenario, which is unattainable in local government. Also, the literature studied and associated best practices focus on WHAT should be done, but provide little guidance as to HOW it should be done. Figure 5, therefore, illustrates a proposed process for a spreadsheet-based tool, to help plan the implementation of IRBC in any municipality.



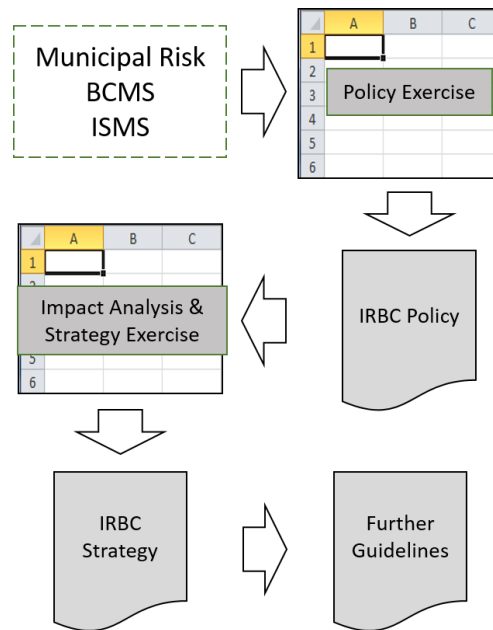


Figure 5: Spreadsheet-based Tool for IRBC Planning

This spreadsheet-based tool, is based on the theoretical foundation, which is adapted from the ISO/IEC 27031 standard and tailored to the challenges within municipalities. This tool should upon completion, yield an IRBC policy, a completed application impact analysis, and a strategy towards drafting an IRBC Plan. Further guidelines assisting with the remaining ‘Do-Check-Act’ are subsequently provided. The process is initiated by acknowledging and accounting for various municipal risks that threaten ICT, as well as requirements from both the ISMS and BCMS.

The first exercise will produce a high-level IRBC policy. The policy exercise consists of a list of statements, engineered from the policy requirements of the ISO/IEC 27031 standard. The responsible person, preferably from senior- or top management, should either ‘agree’, or ‘disagree’ with the given statements. These options would determine which policy statements would eventually be omitted or included in the policy. If there is a disagreement with a statement, a self-check flag is raised, with the relevant information as to why the given statement is applicable or important. The person can either change the decision, or accept accountability for its omission, when the policy is eventually generated.

If a BCMS exists within the municipality, it is assumed that a proper business impact analysis has been completed and that it can provide the recovery requirements to IRBC.

However, to cater for municipalities, which are developing IRBC in isolation, the spreadsheet-tool provides an alternative to the business impact analysis. Marbais (2012) states that a simple way to develop recovery requirements is to conduct a more focused application impact analysis (AIA). The AIA focuses on ICT systems that specifically cater for municipal business activities, and measures the impact on the enterprise that a disruption might impose (Marbais, 2012). The AIA will produce the relevant recovery objectives, which IRBC must address.

Once the recovery objectives and most critical ICT systems are identified, a strategy exercise is completed. This will provide the municipality with a high-level ICT strategy to ensure resilience and continuity of critical ICT systems, in line with the requirements of the enterprise set in the AIA. The responsible person will select the relevant strategies within six elements, as defined in the ISO/IEC 27031, and which ultimately allows for a tailored-to-capacity approach. Upon generating the IRBC strategy, the Plan-phase of IRBC is concluded. As mentioned, due to the technical and contextual nature of IRBC, the municipality has to continue by itself from this stage. However, relevant guidance will be provided to assist with the drafting of relevant IRBC plans, and procedures.

This approach as a whole, addresses the ICT continuity problem in local government, from both a theoretical foundation and by factoring in resource-capacity challenges. Firstly, the principle of *SCALABILITY* is addressed, as a result of the flexibility of the output from the different tool exercises, as well as the ability for IRBC to function in isolation. Secondly, this approach is *SIMPLISTIC* in nature, identifying the most critical aspects needed for IRBC in municipalities and combining these in a self-help spreadsheet-based tool, which anyone with basic computer literacy should be able to use. Furthermore, the principle of *COMPREHENSIBILITY* is addressed through simplification, as well as the adequate guidance provided throughout the entire process: a process, which would normally require help from consultants. Furthermore, due to municipalities functioning in diverse environments, this approach is *USABLE* within any municipality, provided the responsible person has access to a spreadsheet application, such as Microsoft Excel.

Therefore, based on a theoretical foundation from best practices and standards, IRBC can be developed in a municipality, whilst taking into account their resource-capacity limitations. As explained earlier, only the Plan-phase can be addressed generically, due to the context-specific nature of municipalities. Should a municipality make use of this approach and initiate the implementation of IRBC, and then follow through with the entire process, the concerns of the Auditor-General, with regard to ICT continuity, should be addressed

satisfactorily. The following section will briefly discuss the validation of the IRBC spreadsheet-based tool.

## **6. Validation**

### **6.1 Data Collection**

A workshop was hosted for the purpose of validating the proposed approach for IRBC in municipalities. In total, 22 representatives, primarily from the ICT department of different municipalities, attended the workshop. The workshop spanned two days; and each day consisted of a theoretical background session, followed by a practical session. Each municipal representative received a functioning prototype of the IRBC spreadsheet-based tool. During the practical session, each attendee had the opportunity to use the spreadsheet-based tool and to work through the different exercises, as illustrated in Figure 5.

Upon completion of the practical session, as part of a survey, each representative completed a questionnaire. The objective of the questionnaire was to test whether the IRBC spreadsheet-based tool met the principles identified in Section 3.1, in order to be suitable for the municipal environment. The questionnaire consisted of various statements, each testing a different principle; and the representative had to indicate whether they ‘strongly disagree’, ‘disagree’, ‘agree’ or ‘strongly agree’ with the given statement. In conjunction with the statements, the questionnaire also included some open-ended questions, where representatives could indicate whether the tool lacked anything, needed improvement in some areas, as well as anything positive that they had identified.

### **6.2 Results**

The questionnaire results indicated that all of the principles, including – scalability, simplicity, comprehensibility and usability – tested positive, with the overwhelming majority of the respondents either agreeing or strongly agreeing that the tool satisfies each principle. Both scalability and usability received a 100% agree or strongly agree response; whilst comprehensibility received 91%. With regard to the principle of simplicity, 16% disagreed that the tool was simplistic, whilst the majority agreed.

Feedback from the open-ended questions was primarily good, with most respondents giving positive feedback. The respondents indicated that the IRBC spreadsheet-based tool would benefit municipalities and help with their ICT continuity challenges. When asked where the IRBC spreadsheet-based tool was lacking, a respondent said that it was complex for someone with no knowledge about ICT and disaster recovery. Some respondents said that the

technical aspects of IRBC had to be included in the tool. Another respondent indicated that clarity was needed on how district municipalities and local municipalities can interact, due to many local municipalities relying on district municipalities for their continuity. It should be noted that some of the municipal representatives were from municipal functions, like finance and internal audit; and they would, therefore, not be familiar with ICT continuity and recovery.

Taking into account the results as a whole, the overall feedback is very positive; and it indicates that the principles have largely been satisfied, and that especially low-capacity municipalities would greatly benefit from using the tool.

## **7. Conclusion**

Municipalities within the South African local government sphere have the constitutional mandate to deliver sustainable services to their communities. ICT is a critical enabler within municipalities to assist in this regard; but it must be resilient and able to recover effectively. This study has determined that the majority of municipalities within South African local government are not designing, nor implementing adequate ICT continuity controls. Furthermore, challenges with regard to capacity in municipalities have been identified. It has been argued that these challenges predominantly hinder municipalities from addressing any ICT controls, even though multiple government attempts have been made to address the situation.

This study, with the help from a district municipality, has aimed to address this real-life problem by proposing an approach for planning IRBC in municipalities, that is tailored to the challenges faced in local government, but founded on best practices and standards. The practical spreadsheet-based tool forming part of this approach, would assist municipalities to plan IRBC, according to their needs; and further guidelines would help the municipality to effectively implement what has been planned. This approach should enable municipalities to overcome their challenges, and thereby result in a resilient ICT environment through sound IRBC structures.

A prototype of the IRBC spreadsheet-based tool was developed and tested at a workshop with representatives from various municipalities. The survey conducted at the workshop validated the tool against the identified principles required in low-capacity municipalities. The results reported on were positive in the majority of cases.

## Reference List

- Act, S. O. Sarbanes-Oxley Act (2002). Washington DC.
- Auditor-General of South Africa. (2013). *Consolidated general report on the audit outcomes of local government 2011-12*.
- Auditor-General of South Africa. (2014). *Consolidated general report on the audit outcomes of local government 2012-13*.
- Auditor-General of South Africa. (2015). *Consolidated general report on the audit outcomes of local government 2013-14*.
- Brynard, P., & De Coning, C. (2006). Policy implementation. In *Improving Public Policy* (2nd Edition). Pretoria: Van Schaik Publishers.
- BSI. (2008). BS 25777:2008. Retrieved December 26, 2015, from <http://shop.bsigroup.com/ProductDetail/?pid=000000000030166966>
- Cameron, R. (2001). The Upliftment of South African Local Government? *Local Government Studies*, 27(13), 97–118.
- Cerullo, V., & Cerullo, M. J. (2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management*, 21, 70–78.
- Coertze, J., & von Solms, R. (2012). A model for information security governance in developing countries. *E-Infrastructure and E-Services for Developing Countries*, 279–288.
- Constitution of the Republic of South Africa, Government Gazette No. 17678 (1996).
- Department: Public Service and Administration. (2012). Public Service Corporate Governance of Information and Communication Technology Policy Framework.
- Department: Western Cape Local Government. (2015a). Local Government Circular: C5 of 2015.
- Department: Western Cape Local Government. (2015b). Municipal Corporate Governance of Information and Communication Technology Policy.
- Hamidovic, H. (2011). An Introduction to ICT Continuity Based on BS 25777. *ISACA Journal*, 2(45), 1–5.
- Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, 52(6), 978–1002.
- Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business Continuity Management: Time for a strategic role? *Long Range Planning*, 37(5), 435–457.
- IODSA. (2010). *King Report on Corporate Governance in South Africa*. Retrieved from <http://www.iodsa.co.za/?kingIII>
- ISO 22301. (2012). Societal security — Business continuity management systems — Requirements ISO 22301. Geneva: ISO.
- ISO/IEC. (2008). Corporate governance of information technology ISO/IEC 38500, 1–25.

- ISO/IEC 27031. (2011). Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity ISO/IEC 27031. Geneva: ISO/IEC.
- Jackson, C. B. (2002). The Changing Face of Continuity Planning. *Information Systems Security*, 10(6), 18–21.
- Kanyane, M. H. (2006). Municipal Skills challenges for accelerated service delivery in South Africa. *Journal of Public Administration*, 41(3), 112 – 118.
- Marbais, G. (2012). Using ISO 27031 to Guide IT Disaster Recovery Alignment with ISO 22301. Retrieved January 12, 2016, from <http://perspectives.avalution.com/2012/using-iso-27031-to-guide-it-disaster-recovery-alignment-with-iso-22301/>
- Presidential Commissioners. (1998). *Report of the Presidential Review Commission on the Reform and Transformation of the Public Service in South Africa*. Retrieved from <http://www.gov.za/documents/report-presidential-review-commission-reform-and-transformation-public-service-south>
- Protiviti Inc. (2013). *Guide to Business Continuity Management*. Protiviti. Retrieved from <http://www.protiviti.com/en-US/Documents/Resource-Guides/Guide-to-BCM-Third-Edition-Protiviti.pdf>
- SALGA. (2012). A Municipal Guide / Roadmap To Successful ICT Governance, (June), 93.
- Stanton, R. (2005). Beyond disaster recovery: The benefits of business continuity. *Computer Fraud and Security*, 2005(7), 18–19.

# Appendix B

## Questionnaires

Appendix B includes the questionnaires that were used during study. These questionnaires were used both for initial data collection, as well as validation of the M-IRBC.

These include the following:

1. Semi-structured Interview Topics/Questions
2. Validation Workshop Questionnaire

### B.1 Semi-structured Interview Topics/Questions

*The semi-structured interview topics/questions was used during Phase 1 of the integrated research process. The aim of these questions were to get a general overview of the municipal ICT environment. It also aimed to get an idea of what is needed within municipalities.*

**Municipal Stakeholder Semi-Structured****Interview: Topics/Questions:**

1. What legislation/standards/best practices is the main driver for what you from an IT governance/IT systems/IT security perspective?
2. Which of your municipal manager and/or executive mayors' key performance indicators is directly related to your IT governance challenges?
3. To what extent is IT/IT governance a regular agenda point on municipal council meetings?
4. Do you have an audit and/or risk committee?
5. To what extent does the audit and/or risk committee address IT/IT governance as an agenda point at council meetings?
6. To what extent do you escalate IT/IT governance aspects to the council, possibly via the audit/risk committee? How easy is it to do?
7. Do you have a CIO, or somebody, fulfilling the role of a CIO?
8. Is this person serving on the municipal council, audit or risk committees?
9. What is the typical process followed by the Auditor General during an audit of your municipalities IT?
10. Does the AG use some sort of checklist or compliance list?
11. What relationship exists between district and local municipality regarding IT governance?
12. Are you confident that you know what is required for proper IT systems/IT governance?
13. What type of guidance/tools will be able to assist you towards a better audit report?
14. What skills do you feel is missing or required within the municipality?
15. What courses/training will assist you towards improving?



## B.2 Validation Workshop Questionnaire

*The Validation Workshop Questionnaire was used during Phase 4 of the integrated research process. The aim of this questionnaire was to validate the M-IRBC against the criteria of Scalable, Simplistic, Comprehensible and Usable to deem its appropriateness for local government.*































**Nelson Mandela  
Metropolitan  
University**  
*for tomorrow*

## ICT Readiness for Business Continuity in Local Government

Thank you for participating in the workshop session for ICT Readiness for Business Continuity (IRBC). Please be so kind as to complete the following questions, so we can further improve on the exercises you have completed today.

*Mark with - X*

<b>1. The M-IRBC and its exercises would be compatible to function in any municipality.</b>			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
<b>2. In general, the concept of IRBC becomes clear and understandable throughout the M-IRBC process.</b>			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
<b>3. It is possible to complete the exercises in this M-IRBC without extensive guidance or knowledge about the subject area.</b>			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
<b>4. The M-IRBC allows IRBC to scale to the size and resource capacity of a municipality.</b>			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
<b>5. A person with limited technical ability would be able to successfully complete the tool-set exercises.</b>			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
<b>6. The M-IRBC can be equally successful in both larger and smaller municipalities.</b>			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
<b>7. A person without prior knowledge about IRBC would be able to comprehend the goals and objectives of what IRBC strives to achieve upon completing the M-IRBC exercises.</b>			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 

**8. What have you found to be particularly good and/or useful about M-IRBC?**

---

---

---

---

---

---

---

---

**9. In what aspects, in your opinion, is the M-IRBC lacking?**

---

---

---

---

---

---

---

---

**10. In your opinion, what aspects about the M-IRBC can be improved?**

---

---

---

---

---

---

---

---

# Appendix C

## M-IRBC Tool-set

Appendix C provides excerpts from the M-IRBC Tool-set that were provided to representatives from local government during the validation workshop. Although these excerpts cannot illustrate the functionality of the actual application functionality, the screen captures provide a good overview of how the various exercises look, and one can see how it works to a certain extent. The complete IRBC policy and reference guide is also included.

Appendix C includes the following:

1. IRBC Policy Exercise
2. IRBC Policy
3. Application Impact Analysis Exercise
4. IRBC Strategy Exercise
5. Reference Guide

## C.1 IRBC Policy Exercise

*The IRBC Policy Exercise includes two parts. The first part is the ‘**Principles Exercise for the IRBC Policy**’. Within this part, the user will agree or disagree with certain statements to determine which statements will remain within the policy. Part two is the ‘**Policy Omissions**’. Here, the user must provide justification for any policy statements that have been excluded from the policy. The user will gain access to the IRBC Policy only once justification has been provided for all omitted policy statements.*

Principles Exercise for the ICT Readiness for Business Continuity Policy				
The following exercise serves as a precursor to the Municipal ICT Readiness for Business Continuity Policy. The following statements represent important principles or criteria that are included in the Policy. Should you definitely disagree with any of the following statements, the "Policy Omissions" worksheet will provide instructions as to which policy statements or sections to omit from the policy. You will however be required to give relevant accountability for each omission. Read through the given statements and indicate in Column C whether you agree. Should you disagree a relevance message will appear in the adjacent cell within Column D. You may change your decision or subsequently agree to omit the statement using the option in Column E. (Note: by agreeing with the statement, it will automatically be included in the policy - indicated by a NO in Column E).				
#	Statements:	Do you agree with this statement:	Why is this important?	Do you wish to omit the resulting policy statement or section regarding this principle/criteria?
1	Disruptions to ICT can constitute strategic risks to the reputation of the municipality and its ability to operate.			NO
2	It is critical to develop and implement a readiness plan for the continuity of ICT systems, to ensure that the municipality has a resilient ICT environment which also support the municipal ISMS, BCMs and Risk mitigating activities.			NO
3	The municipality acknowledges the benefit of being compliant with international best practice with regard to its ICT Readiness objectives			NO
4	In order for the municipality to achieve ICT Readiness for Business Continuity (IRBC), it needs to put in place a systematic process to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services.			NO
5	To be effective, the IRBC program should be a process fully integrated with the municipality's management activities, driven from the top of the municipality, endorsed and promoted by top management.			NO
6	The objectives of the IRBC program should lean toward the resiliency of municipal ICT systems, rather than recovery of such systems - post disaster.			NO
7	The municipality should carefully consider resource requirements throughout the IRBC program lifetime and take into account and address internal constraints such as budget, technological constraints and regulatory obligations etc. within its resource capability.			NO
8	The scope for the IRBC program must be clearly defined including possible limitations and exclusions.			NO
9	The roles and responsibilities of the people and teams having authority (both in terms of decision-making and authority to spend) before, during and following a disruptive incident should be clearly documented.			NO
10	Important terms should be adequately defined as to promote universal understanding of components within the IRBC program.			NO
11	IRBC is critical for ensuring the municipality's ability to operate and therefore adequate document and record control have to be established for all the relevant policies and plans within the IRBC program in order to be readily available in any event.			NO
12	The IRBC plans should be maintained on a continual basis through planned monitor, testing and audit activities.			NO
13	It is important that the IRBC management system should be reviewed by top management at regular intervals, taking input from audits or self-assessments, to identify opportunities for improvement or the need for changes to IRBC management, including the policy and objectives.			NO
14	Top management should appoint or nominate a person with appropriate seniority and authority to be accountable for IRBC policy and implementation			NO
15	It is important that the necessary processes are in place to regularly promote IRBC awareness in general within the municipality as well as suppliers, and also assess and enhance competency of all relevant personnel key to the successful implementation of IRBC.			NO

Policy Omissions			
This worksheet lists any IRBC policy statements with its corresponding section in the IRBC policy, of statements you chose to omit. Any statement/s you chose to omit from the IRBC policy, should be erased and replaced with a statement of applicability, within the policy, confirming that the municipality accepts the omission.			
#	Omitted?	Please provide a statement of applicability:	Remove the following statement in the policy: Section:
1	DEFAULT		
2	DEFAULT		
3	NO		
4	NO		
5	NO		
6	NO		
7	NO		
8	DEFAULT		
9	NO		
10	DEFAULT		
11	NO		
12	NO		
13	NO		
14	NO		
15	NO		

<u>Criteria to gain access the Municipal IRBC Policy:</u>
1. You must agree with all the statements in the IRBC Policy Exercise
OR
2. Provide accountability statements for every omitted statement within this Policy Omissions Exercise
Failure to do this will result in access to the Municipal IRBC Policy being withheld.
Have you completed the IRBC Policy Exercise and Omissions table?

Access Rights Status: ACCESS DENIED

## C.2 IRBC Policy

*The IRBC policy attached in this appendix is the complete IRBC policy. The user will gain access to this policy after completing the IRBC Policy Exercise. The Policy Omissions worksheet will indicate which policy statements should be replaced with statements of applicability.*





---

# MUNICIPAL ICT READINESS FOR BUSINESS CONTINUITY POLICY

---

Draft 1.3



APRIL 26, 2016  
XXX MUNICIPALITY

Contents

- 1. Introduction ..... 2
- 2. Terms and Definitions ..... 3
- 3. IRBC Management Objectives ..... 4
  - 3.1 Goal of IRBC Policy in the Municipality ..... 4
  - 3.2 Goal for IRBC Implementation ..... 4
- 4. Scope ..... 4
- 5. ICT Readiness for Business Continuity ..... 5
  - 5.1 Management Commitment ..... 5
  - 5.2 Policy Communication ..... 5
  - 5.3 Roles and Responsibilities ..... 5
  - 5.4 Management Review and Compliance ..... 5
  - 5.5 IRBC Requirements ..... 5
  - 5.6 Audit, Testing and Maintenance of IRBC Plans ..... 6
  - 5.7 Document Management ..... 6
  - 5.8 Awareness and Training ..... 6
- Sign-off ..... 6

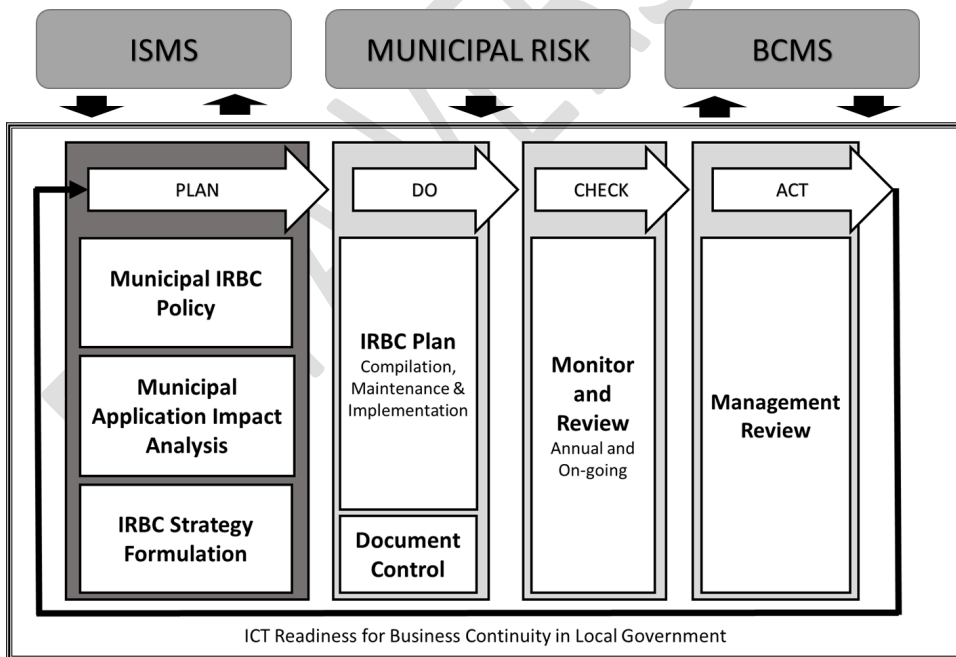
BETA VERSION

### 1. Introduction

Failures of ICT services, including the occurrence of security issues such as systems intrusion and malware infections, will impact the continuity of business operations. Thus, managing ICT and related continuity and other security aspects form a key part of business continuity requirements. Furthermore, in the majority of cases, the critical business functions that require business continuity are usually dependent upon ICT. This dependence means that disruptions to ICT can constitute strategic risks to the reputation of the organization and its ability to operate.

ICT readiness is an essential component for many organizations in the implementation of business continuity management and information security management. As part of the implementation and operation of an information security management system (ISMS) and business continuity management system (BCMS) respectively, it is critical to develop and implement a readiness plan for the ICT services to help ensure business continuity. In order for an organization to achieve ICT Readiness for Business Continuity (IRBC), it needs to put in place a systematic process to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services to ultimately achieve a resilient ICT environment.

Due to the limitations and resource capacity constraints in many municipalities, these municipalities do not have existing BCMS which IRBC can form part of. However, IRBC can function in isolation to achieve a resilient ICT environment, separate from the non-existing municipal BCMS, to have at a minimum, an ICT environment that is ready to face disruptions. The following figure illustrates an IRBC system adapted for municipalities. Only the most vital components are illustrated.



## 2. Terms and Definitions

### **Business continuity management (BCM)**

A holistic management process that identifies potential threats to an organization and the impacts to business operations whose threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

### **ICT readiness for business continuity (IRBC)**

The capability of an organization to support its business operations by prevention, detection and response to disruption and recovery of ICT services.

### **Minimum business continuity objective (MBCO)**

The minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption.

### **Recovery point objective (RPO)**

The point in time to which data must be recovered after a disruption has occurred.

### **Recovery time objective (RTO)**

Period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions must be recovered after a disruption has occurred.

### **Resilience**

The ability of an organization to resist being affected by disruptions.

BETA VERSION

### 3. IRBC Management Objectives

#### 3.1 Goal of IRBC Policy in the Municipality

This policy provides the necessary directives for the planning, implementation, continual evaluation and improvement of an ICT Readiness for Business Continuity (IRBC) management system within the municipality. The IRBC management system can be best achieved through the application of the PLAN-DO-CHECK-ACT (PDCA) cyclical step approach for its entire lifecycle. In doing so working toward ICT services that are resilient and can be recovered to pre-determined levels within timescales required and agreed by the municipality. This policy in its entirety aims to be compliant with international best practice.

#### 3.2 Goal for IRBC Implementation

In order for the municipality to achieve ICT Readiness for Business Continuity, it needs to put in place a systematic process to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services. Ultimately, the municipality aims to control a resilient ICT environment. To achieve this, the municipal IRBC must aim to:

- a) Improve the incident detection capabilities;
- b) Prevent a sudden or drastic failure at best effort;
- c) Enable an acceptable degradation of operational status should the failure be unstoppable;
- d) Further shorten recovery time; and
- e) Minimize impact upon eventual occurrence of the incident.

### 4. Scope

This policy applies to Municipal site offices, facilities and IT systems at all locations. The Municipality will be prepared for and develop effective ICT readiness for scenarios including, but not limited to, natural disasters, power outages, loss of premises, criminal activity, fires, civil and industrial unrest etc. that might impede the ability of the municipality to continue with normal daily functions.

Municipal sites include:

[Addresses]

## **5. ICT Readiness for Business Continuity**

### **5.1 Management Commitment**

Management hereby declares that all elements of IRBC will be supported with adequate resources within the municipality's resource capability in order to achieve all goals and objectives set within this policy, as well as satisfy all identified requirements.

Furthermore, municipal management acknowledges that the IRBC program should be a process fully integrated with the municipalities' management activities, driven from the top of the municipality, endorsed and promoted by municipal management.

### **5.2 Policy Communication**

Management has to ensure that all employees of the municipality, as well as suppliers and outsourcing partners who have a role in IRBC are familiar with this policy.

### **5.3 Roles and Responsibilities**

Management should appoint or nominate a person with appropriate seniority and authority to be responsible for the IRBC policy and its implementation, but accept that ultimate accountability rests with municipal management.

The roles and responsibilities of the people and teams having authority (both in terms of decision-making and authority to spend) before, during and following a disruptive incident should be clearly documented within the relevant recovery plans.

The municipality should furthermore carefully consider resource requirements throughout the IRBC program lifetime and take into account and address internal constraints such as budget, technological constraints and regulatory obligations etc.

### **5.4 Management Review and Compliance**

Ownership of this Policy shall be vested with the Manager who will review the document on an annual basis (at minimum), or when significant changes, such as environmental changes or organizational changes, occur.

### **5.5 IRBC Requirements**

Requirements should be defined, based on the results of an Application Impact Analysis, to have documented Recovery Time Objectives and Recovery Point Objectives for the relevant ICT services, which aligns to the recovery objectives of the municipality.

An IRBC Strategy should be formulated, based on the results of an Application Impact Analysis, and the necessary IRBC processes and response plans developed and documented (IRBC Plan) in line with best practice, to fulfil the requirements and objectives of this policy.

The IRBC Strategy should outline different options to address the resilience and recovery of specific municipal ICT's which might impact important business functions. Related response and recovery plans (IRBC Plan) should adhere to the set objectives for recovery of the various systems.

Performance criteria should be defined and documented to measure the effectiveness of its IRBC.

### 5.6 Audit, Testing and Maintenance of IRBC Plans

The IRBC plans should be maintained through planned monitor, testing and audit activities. These activities, as well as the processes and persons involved, must be well documented as part of the IRBC Plan. These activities should at a minimum be carried out annually.

### 5.7 Document Management

Adequate document and record control have to be established for all the relevant policies and plans within the IRBC management system in order to be readily available in any event.

### 5.8 Awareness and Training

The necessary processes should be put in place to regularly promote IRBC awareness in general, as well as assess and enhance competency of all relevant personnel key to the successful implementation of IRBC.

### Sign-off

This policy has been approved by the Manager, [NAME].

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

BETA VERSION

### C.3 Application Impact Analysis

*The AIA exercise provides the user with a platform from which to determine the municipal business functions and the ICT systems these functions depend on. The importance of the various ICT systems can be determined and the RTO and RPO of each system defined based on its impact rating.*



Municipal Application Impact Analysis for the Readiness of Critical ICT Systems							
The following Municipal Application Impact Analysis is a scaled down BIA, which would normally be conducted as part of the municipal BCMS. Taking into account that many municipalities do not have BCMS implemented this exercise aims to establish recovery objectives for the ICT systems supporting critical municipal business functions. It is important that due care be taken, and that all relevant parties be consulted, so that recovery time requirements of the municipality align to the capability of the ICT department to provide such timeframes. Adapt this exercise to your municipality, and feel free to remove any of the generic examples.							
#	Municipal Business Function reliant on ICT	Do you regard this business function critical to the daily operation of your municipality?	On a scale between 1 (None) and 6 (Severe), what impact would the unavailability of this function have on your municipality?	Related ICT System (Hardware/Software)	Impact Rating	Recovery Time Objective - RTO	Recovery Point Objective - RPO
	Identify activities or functions that support the delivery of key services that should be included in the municipal IRRC.	Information regarding the criticalness of a certain business function can come from interviews, questionnaires and workshops etc. with the relevant stakeholders.	The municipality should address impacts relating to its aims and objectives, and interested parties. These may include: Adverse effects on staff or public well-being; Breach of regulations or SAs; Damage to reputation; Financial loss; Deterioration of service quality; and environmental damage.	Fill in the related systems applicable to your municipality. Utilities such as electricity and telecommunications should also be taken into account and relevant strategies implemented for these utilities.		The RTO for the ICT systems upon which the business function relies should be included in the RTO required by the municipality for the function to resume. This could include the recovery times required by a BCMS.	RPO is the point in time to which data must be recovered after a disaster. The RPO should be directly influenced by the backup strategy, e.g., if the RPO is 4 Hours Data must be backed-up every 4 hours.
1	Vehicle Registration			e-NATIS; LAN; WAN			
2	Personnel Management / HR			CAPWAN; PROMUN; ORGPLUS; LAN; WAN			
3	Finance Management			PROMUN; Excel; LAN; WAN			
4	Research (Legal)			LexisNexis; LAN; WAN			
5	Contract Management			Collaborator; LAN			
6	Library Services			PALS; LAN; WAN			
7	Customer Service			PROMUN; LAN; WAN			
8	Reporting			Microsoft Office Suite; LAN			
9	Research (General)			Internet browser; LAN; WAN			
10	Traffic Administration			TCS; LAN; WAN			
11	Water Care			Adroit Telemetry system; LAN; WAN			
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							

## C.4 IRBC Strategy Exercise

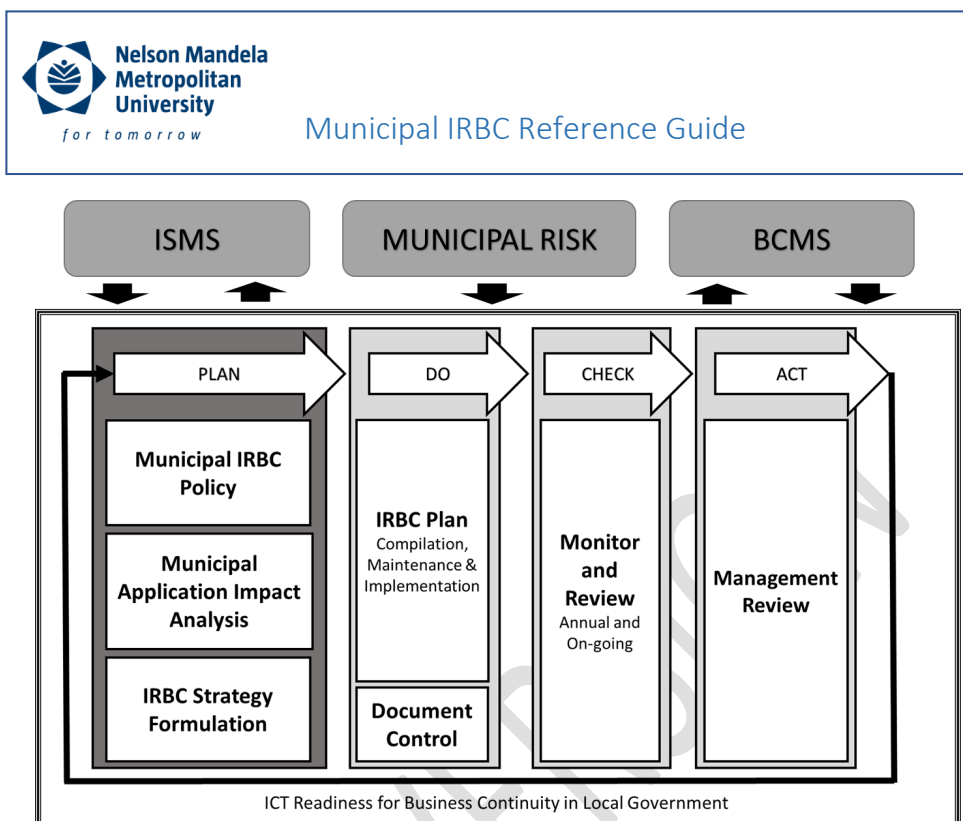
*The IRBC Strategy Exercise enables the user to select the relevant IRBC strategies within each of the IRBC elements. The selected strategies should be able to fulfil the RTO and RPO requirements determined during the AIA and align to the resources provided for the IRBC project. The selected strategies are subsequently collated within the following worksheet where it can be printed.*

ICT Readiness for Business Continuity Strategy Exercise									
The following exercise is divided into 6 elements, defined within IRBC, with each element containing various strategy options. The IRBC strategy should be flexible and cater to the resource capacity of the municipality whilst defining approaches toward ICT resilience so that the principles of incident prevention, incident detection, response, recovery and improvement are put in place. Any strategy options that requires funding will have to go through the relevant municipal budget allocation and procurement procedures. The selected options within each element should directly address the critical ICT systems identified in the municipal Application Impact Analysis (or BOMS BIA), and satisfy the RTO and RPO requirements.									
Strategy Description:	People, Skills & Knowledge	Facilities	Technology	Data	Processes	Suppliers	Strategy:	Considerations:	Selection:
<p>The municipality should identify appropriate strategies for the recovery of critical ICT services. This should be done beyond employees to contractors and other stakeholders who possess extensive ICT specialist skills and knowledge.</p>	<p>The specialist with appropriate skills and knowledge, and competent backup personnel.</p>	<p>The physical environment in which ICT resources are located.</p>	<p>1) hardware (including racks, servers, storage arrays, tape drives, switches and routers); and 2) network (including data connectivity and voice services); 3) software, including operating system and application software, links or interfaces between applications and batch processing routines;</p>	<p>Application data, voice data and other types of data</p>	<p>Supporting documentation to describe the configuration of ICT resources and enable the effective operation, recovery and maintenance of ICT services.</p>	<p>Other components of the risk to be addressed where ICT service provision is dependent upon an external service provider or another organization within the supply chain, e.g. a power utility provider, telecoms carrier or internet service provider.</p>	<p>Documentation of the way in which critical ICT services are performed</p>	<p>IRBC processes should be documented clearly and in sufficient detail to enable competent staff to execute them (some of these processes may differ from the daily operation).</p>	<p>Specialist of additional equipment and software copies at another location</p>
	<p>Multi-skill training of ICT staff and contractors to enhance skill redundancy</p>	<p>Alternative facilities provided by other organizations</p>	<p>Hot standby, where ICT infrastructure is replicated across two sites</p>	<p>The ICT services upon which critical business activities depend should be available in advance of their resumption of their dependent critical business activities. Technology platforms and application software should be put in place within timescales demanded by the municipality as a whole.</p>	<p>Critical business activities may depend on the provision of up-to-date or near-up-to-date data. Solutions should meet the RPO of each critical business activity of the municipality. The selected IRBC options should ensure the ongoing confidentiality, integrity and availability of critical data.</p>	<p>In selecting its IRBC strategy, the municipality should consider the processes necessary to ensure the viability of that strategy, including those necessary in the incident prevention, incident detection, incident response and disaster recovery predetermined and agreed timetables.</p>	<p>Arrangements with suppliers for the delivery of replacement equipment at short notice</p>	<p>RPO requirements</p>	<p>IRBC processes should be documented clearly and in sufficient detail to enable competent staff to execute them (some of these processes may differ from the daily operation).</p>
	<p>Separation of core skills to reduce the concentration of risk</p>	<p>Alternative facilities provided by third-party specialists</p>	<p>Warm standby, where recovery takes place at a secondary site where ICT infrastructure is partially prepared</p>	<p>How data are securely stored, e.g. disk, tape or optical media; appropriate backup and restoration mechanisms should be in place to ensure the data are secure and in a safe environment</p>	<p>Where information is stored, transported or transmitted, the RBC procedure may need to be adapted in light of the application (e.g. the operational priorities and the stakeholders demands).</p>	<p>IRBC procedures may be dependent on the situation that unfolds and in practice may need to be adapted in light of the application (e.g. the operational priorities and the stakeholders demands).</p>	<p>Read repair and/or replacement of faulty parts in the event of an equipment malfunction</p>	<p>Where information is stored, transported or transmitted, the RBC procedure may need to be adapted in light of the application (e.g. the operational priorities and the stakeholders demands).</p>	<p>IRBC procedures may be dependent on the situation that unfolds and in practice may need to be adapted in light of the application (e.g. the operational priorities and the stakeholders demands).</p>
	<p>Knowledge retention and management</p>	<p>Workshop from home or at other rented sites</p>	<p>Cold standby, where infrastructure is built or configured from scratch in an alternative location</p>	<p>Where information is stored, transported or transmitted, the RBC procedure may need to be adapted in light of the application (e.g. the operational priorities and the stakeholders demands).</p>	<p>Restore timescales, driven by the volume of data, how they are stored and the complexity of the technical restore process, along with the requirements of the service user and the needs of municipal continuity</p>	<p>Restore timescales, driven by the volume of data, how they are stored and the complexity of the technical restore process, along with the requirements of the service user and the needs of municipal continuity</p>	<p>Def. supply of utilities such as power and telecoms</p>	<p>Emergency generating equipment</p>	<p>Emergency generating equipment</p>
		<p>Other agreed suitable working facilities</p>	<p>Ship-in arrangements, under which external service providers provide hardware</p>	<p>Ship-in arrangements, under which external service providers provide hardware</p>					
		<p>Use of an alternative workforce in an established site</p>							
	<p>Alternative facilities that can be arranged to be used to provide direct replacement of some of the physical assets involved</p>								

<b>The following strategies have been selected:</b>	
<p>This worksheet aims to place all the selected IRBC strategies together. This worksheet can be printed and the selected strategies used as the foundation for an expanded IRBC Strategy, or usage within a municipal Master Systems Plan, all depending on the processes of the municipality</p>	
<b>People: Skills &amp; Knowledge</b>	
<b>Facilities</b>	
<b>Technology</b>	
<b>Data Consideration</b>	
1	RPO requirements
2	How data are securely stored, e.g. disk, tape or optical media; appropriate backup and restoration mechanisms should be in place to ensure the data are secure and in a safe environment
3	Where information is stored, transported or transmitted, distance, location, network links, etc. (onsite, offsite or third party) and expected timescales for the retrieval of backup media
4	Restore timescales, driven by the volume of data, how they are stored and the complexity of the technical restore process, along with the requirements of the service user and the needs of municipal continuity
<b>Processes</b>	
1	IRBC processes should be documented clearly and in sufficient detail to enable competent staff to execute them (some of these processes may differ from the daily operation).
2	IRBC procedures may be dependent on the situation that unfolds and in practice may need to be adapted in light of the disruption (e.g. the degree of loss or damage), the organization's operational priorities and the stakeholders demands.
<b>Suppliers</b>	

## C.5 Reference Guide

*Due to the technical nature of IRBC, and the aim of making the tool-set scalable and usable, the tool-set only provides help with the Plan-phase of IRBC. This reference guide therefore provide the user with reference to where information and guidance can be found for the rest of the implementation process.*



The municipal IRBC spreadsheet-based tool has automated the most critical components of the IRBC Plan-phase. Unfortunately, due to the technical and municipality-specific nature of the subsequent DO-CHECK-ACT-phases, no generic solution can be provided to assist in that regard. This document therefore aims to provide reference to relevant information within various standards which can be consulted to make the implementation requirements of IRBC more clear.

**IRBC Requirements:**

Understanding critical ICT services	ISO/IEC 27031 – Section 6.3.2
Implementing the IRBC Strategy Elements	ISO/IEC 27031 – Section 7.2
Incident Response guidance	ISO/IEC 27031 – Section 7.3; ISO/IEC 27035
IRBC Plan: Including its Content & Response and Recovery Plan documentation	ISO/IEC 27031 – Section 7.4; ISO/IEC 24762
Awareness, competency & training	ISO/IEC 27031 – Section 7.2.1 + 7.5
Document Control requirements	ISO/IEC 27031 – Section 7.6
IRBC Maintenance and Audit	ISO/IEC 27031 – Section 8.1 + 8.2 + 8.4
Management Review requirements	ISO/IEC 27031 – Section 8.3 + 8.4
IRBC Improvement	ISO/IEC 27031 – Section 9



You Write. **We Edit.** You Love it.

24 November 2016

TO WHOM IT MAY CONCERN

**REF: CONFIRMATION OF LANGUAGE EDITING SERVICES: RUAN KOEN**

I confirm that I have done Language Editing for Ruan Koen's Dissertation titled:

**ICT READINESS FOR BUSINESS CONTINUITY IN LOCAL GOVERNMENT.**

The Dissertation now conforms to Nelson Mandela Metropolitan University's language editing standards.

Yours sincerely

A handwritten signature in black ink that reads "Lynn N Sibanda". The signature is written in a cursive style.

Lynn N Sibanda

Tel: 011 050 0376

Mobile: 071 989 0983

Email: [lynn@lovetoedit.co.za](mailto:lynn@lovetoedit.co.za)

Member of the [Professional Editors Guild](#)

Professional  
**EDITORS**  
Guild



## Glory be to Jesus Christ the Son of God

*<sup>30</sup> Even the youths shall faint and be weary,  
And the young men shall utterly fall,  
<sup>31</sup> But those who wait on the LORD  
Shall renew their strength;  
They shall mount up with wings like eagles,  
They shall run and not be weary,  
They shall walk and not faint.*

Isaiah 40:30-31

*<sup>13</sup> I can do all things through Christ who strengthens me.*

Philippians 4:13