Business continuity in the public sector: a case study of the Western Cape Government, South Africa

Gillian Lutz*, Michael Twum-Darko and
Andre Slabbert

Cape Peninsula University of Technology,
Cape Town, South Africa
Email: Gillian.Lutz@westerncape.gov.za
Email: darkom@cput.ac.za
Email: slabbert.andre311@gmail.com
*Corresponding author

Abstract: This paper explored the management of risks and the continuation of business in the public sector more specifically, the Western Cape Government of South Africa. It is argued that the current environment is continuously evolving, organisations are therefore not immune to change and disruption. The inability of an organisation such as government to manage business continuity would compromise service delivery to the citizens. The study adopted an interpretivist philosophy that allowed for the exploration of the theory and to obtain rich in-depth data from the participants. A qualitative approach utilising semi structured interviews and focus groups among 6 of the 13 Western Cape Government departments were used. From the findings, it is argued that the risk and business continuity management processes were not fully understood. It is recommended that business continuity be adopted as a holistic approach with business continuity embedded within the existing government processes to manage disruptions appropriately.

Keywords: business continuity; risk management; governance; public service.

Reference to this paper should be made as follows: Lutz, G., Twum-Darko, M. and Slabbert, A. (2021) 'Business continuity in the public sector: a case study of the Western Cape Government, South Africa', *Int. J. Business Continuity and Risk Management*, Vol. 11, No. 4, pp.277–294.

Biographical notes: Gillian Lutz is the Deputy Director: Security Information and Knowledge Management, Department of Community Safety, Western Cape Government, South Africa. She holds a Master's in Business Administration. Her expertise and work is focused on business process improvement, identifying process failures and developing improvement processes to ensuring the organisation remains relevant and archives its objectives. She is a competent administrator developing and implementing key policies to empower line function managers. She has gained vast experience within various disciplines within government and is a key influencer with regards to the development of departmental strategy.

Michael Twum-Darko is the Head: Centre for Business Innovation and Incubation, Cape Peninsula University of Technology, South Africa. His research work and projects focused on digital transformation of organisations particularly; business process innovation, enterprise architecture strategies the last 16 years and recently, the implications of the 4th Industrial Revolution. A NRF C3 rated researcher in South Africa, he viewed the digital transformation processes using disruptive technologies as a discipline that seeks to reinvent business, government and community services using enterprise architecture principles to extract and optimise value from limited resources to benefit society. He investigated using qualitative and/or mixed methods, guided by social theories and applied these research interests in Africa businesses, state-owned enterprises, municipalities, and provincial governments.

Andre Slabbert spent nearly 30 years in academia after obtaining his Doctorate in 1981. The last 15 years of his tenure was as the Head of Research for the Business Faculty at the Cape Peninsula University of Technology. During this period, he successfully supervised 58 Master's and Doctoral students, examined approximately 300 Master's and Doctoral dissertations from other universities, local and abroad. He presented 40 papers at local and international conferences, published 38 papers in local and international journals, and received several research awards. His primary research interests were structural unemployment (effect on societies), poverty, societal change, and organisational effectiveness.

1 Introduction and background of the study

With the current environment continuously evolving, organisations were required to adapt to change and disturbance, and government as an organisation was therefore not immune. The Constitution of the Republic of South Africa, 1996 stipulated how government worked. The three areas of government were: national government, provincial government and local (municipal) government. The spheres were distinctive, interrelated and interdependent. The Western Cape Government is the provincial government of the Western Cape Province in South Africa. The Southern Business School (2013, p.6) explained that government has a range of institutions that render services to the citizens. These institutions are generally referred to as the public sector. According to Bakar et al. (2019), the primary business of the public sector is service delivery. The public service is therefore tasked to render services to the citizen on behalf of government. It is therefore understood that government has an obligation to provide services to the citizens of the country. An interruption to business functions could have widespread effects on the ability of government to render services to the citizens. The aim of the study was to explore how the public sector, more specifically the Western Cape Government, would continue to provide services to the citizens as a result of a disruption by managing risks.

Venter (2014, pp.138–139) explained that organisations ought to be considered open systems in relation to their environment and competitors. The boundaries and interfaces that existed between organisations and the external environment were relatively fluid and could not be easily or clearly defined. The external environment from time to time would spring surprises on organisations and managers needed to be prepared to react. Timely and accurate information about the environment proved to be critical for strategic decision making and planning. According to Denyer (2017, p.5), to be responsive to the ever changing external environment required organisations to predict, plan for, react and adjust to change and rapid events of disruption to continue and flourish. Simply put, it required organisations to become resilient. Drawing from Viljoen (2015, p.50), resilience is the ability of a functional organisation to encounter change and disruption without disastrous transformations. Naden (2017) further argues that resilience was the key for any business wanting to thrive in an ever-changing world. Fiksel (2015) maintained that managers were confronted with change and were paying greater consideration towards becoming a resilient organisation, one that had the ability to survive, adjust, and thrive in the face of erratic change. For an institution to be resilient it must be able to achieve its core objectives under all conditions.

According to the Australian Institute of Company Directors (2017), good governance was at the heart of any successful business. It maintained that a well-governed organisation was one that had systems and processes under control, strategy mapped out and risk monitored. Well governed organisations generally achieved much better outcomes than those that were not. The leadership were the determents of how well governed an organisation was. In the public sector good governance meant the responsible handling of public funds. According to CQI (2016) poor governance exposed organisations to increased financial, reputational and operational risk. The Institute of Directors, South Africa (2016, p.20) further maintained that in South Africa the King IV report served as the benchmark for corporate governance. Corporate governance therefore facilitated the effective management of government departments to deliver services to the citizens. It is therefore assumed that for government as an organisation to achieve its core objectives it has to be well run.

2 Literature review

In order to action the expectation of government to provide services to the citizens and/or its stakeholders it is crucial that adequate controls are in place to ensure that risks which governments face are appropriately managed. To achieve this requires the assurance that government as an organisation is well run, not only were they adequately prepared but they had systems and processes in place that enabled continuity. This assured that well run government organisations were those that were able to achieve strategic objectives, had the commitment of leadership, were able to manage risks, had the ability to continue to provide critical services, manage disruptions to have limited impact and downtimes. To pursue business continuity as a key process, it required the exploration of how risks were managed and the identification of the processes currently being used by the Western Cape Government to manage business continuity. The literature reviewed provided extensive references to related research and theory in the field of business continuity. The literature studied was not solely limited to the field of business continuity but also explored how the public sector managed risks to ensure the continuation of business.

2.1 Managing risk in the public sector

2.1.1 Public sector and managing risk

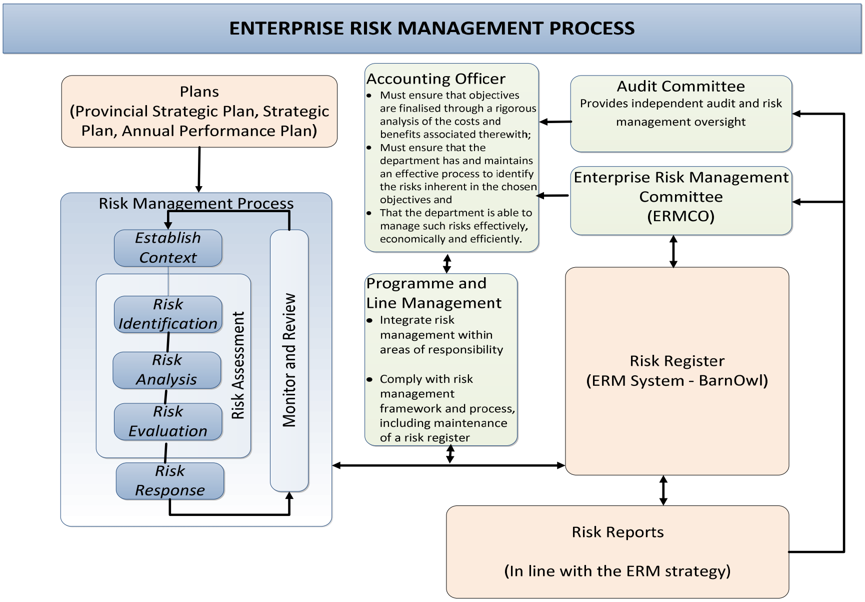
The Southern Business School (2013) provided that the public sector around the globe was undergoing change and renewal. It involved rethinking government's "business" with the intent to improve service delivery towards the achievement of government objectives. Government had been viewed as bureaucratic, slow to respond, not efficient and not creative. In South Africa, the intention was to bring about a shift to become more client-orientated and innovative in the delivery of public services. This sentiment was supported by the Western Cape Government, Western Cape (South Africa) (2018, p.1, p.3) to enable a shift from governance for compliance to governance aimed at improving service delivery. The Institute of Directors, South Africa (2016, pp.3, 41, 61) in the King IV Report on Corporate Governance for South Africa acknowledged that the times we were currently living in were characterised by changes essentially in society as well as business. It also noted that risk needed to be governed in such a manner that provided support to the organisation in determining and the achievement of strategic objectives. Therefore, effective risk management should be delegated to management to implement and execute. The Institute of Directors, South Africa (2016, p.61) also recommended that the management of risks should be integrated and embedded in the business activities and culture of the organisation. Venter (2014, p.146) argued that the classic risk management strategies limited to financial analysis were no longer acceptable. Risk management strategies needed to be expanded to include destabilising events arising from other external forces. According to Coetzee and Lubbe (2013) it was becoming difficult for both privately owned and the public sector to achieve goals and manage risks effectively. The reasons range from fewer resources, continuously changing business environment and the inability to identify and manage risks effectively. The Institute of Directors, South Africa (2016, p.61) recommended that the management of risks should be integrated and embedded in the business activities and culture of the organisation.

2.1.2 South Africa public sector and managing risk

The provincial governments legal foundation for risk management was established in terms of Section 45 of the Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999). In terms of Section 38(1)(a) of the Public Finance Management Act (Act 1 of 1999), heads of departments as accounting officers in their respective departments were mandated to "ensure and maintain effective, efficient and transparent risk management systems." The Public Finance Management Act [South Africa, (1999b), p.47] maintained that heads of departments in the public service were therefore mandated with the management of all risks resultant from threats which could hamper their ability to deliver services and achievement of stated objectives. Furthermore, National Treasury, South Africa (2010, p.67) assigned provincial treasuries to monitor and assess the implementation of risk management for provincial governments in terms of the Public Sector Risk Management Framework. National Treasury, South Africa (2016) specified that in the public sector, risk management was focused on having frameworks and systems in place for the management of risk. The efforts from stakeholders had gone unnoticed which ensured that the results of the management of risk had added value. Risk management in the public sector was largely still regarded as a burden. This sentiment was echoed by Moloi (2016) as it was found that national government departments had poor risk management practices affecting their ability to identify threats which in turn impact on the achievement of government objectives.

National Treasury, South Africa (2010, p.28) used the term 'enterprise risk management' to describe how the management of risks were applied throughout the organisation opposed to selected areas or disciplines of the organisation. Enterprise wide risk management was defined as a holistic approach to manage risks in all major responsibilities and operations. Western Cape (South Africa) (2018, p.3) maintained that Western Cape Government departments adopted the enterprise risk management policy in 2016. The policy articulated the risk management philosophy and captured on a high level the obligations of the different role players and provided the basis for the risk management processes in departments. The process for risk management was illustrated in Figure 1 (Department of Community Safety, South Africa, 2018).

Figure 1 The enterprise risk management process (see online version for colours)


ENTERPRISE RISK MANAGEMENT PROCESS
Plans
(Provincial Strategic Plan, Strategic Plan, Annual Performance Plan)
Risk Management Process
Establish Context
Risk Identification
Risk Analysis
Risk Evaluation
Risk Assessment
Risk Response
Monitor and Review
Accounting Officer
• Must ensure that objectives are finalised through a rigorous analysis of the costs and benefits associated therewith;
• Must ensure that the department has and maintains an effective process to identify the risks inherent in the chosen objectives and
• That the department is able to manage such risks effectively, economically and efficiently.
Programme and Line Management
• Integrate risk management within areas of responsibility
• Comply with risk management framework and process, including maintenance of a risk register
Audit Committee
Provides independent audit and risk management oversight
Enterprise Risk Management Committee
(ERMCO)
Risk Register
(ERM System - BarnOwl)
Risk Reports
(In line with the ERM strategy)

Source: Department of Community Safety, South Africa (2018)

The risk identification process for the government of the Western Cape as explained in Western Cape (South Africa) (2018, p.5), was the identification, recognition and description of risk. Risks were identified as follows:

a Strategic risks (the ability of the department to meet strategic goals). Strategic risks were dealt with by senior management, including risks that have a transversal impact and which could impact the vision/goals of the departments as recorded in the five-year strategic plan.

b Program risks: these arose at program level. These risks required specific and detailed responses and monitoring regimes, were short-term and linked to annual performance plan indicators. Departments could be faced with major adverse consequences if operational risks were not monitored and dealt with. The Western Cape Government (South Africa) (2016) registered the ability of the Western Cape Government to plan for disruptive events, to continue and restore business after such events as a provincial risk.

2.2 *Managing business continuity in the public sector*

2.2.1 *Public sector and business continuity*

Smith (2012, p.2) viewed the management of business continuity as the holistic management process that identified possible threats and the effects to the operations of the business should they be realised, may cause. It provided a guide to developing organisational resilience as an effective response that safeguarded the interests of stakeholders.

Wong and Shi (2015, p.8) further provided that business continuity management was essential in the organisation's overall approach to governance. It underpinned the oversight capabilities that ensured controls were established to safeguard key assets, capacity to earn and reputation of the organisation. Hela (2017) also inferred that business continuity had become a governance issue. The Institute of Directors, South Africa (2016, pp.61, 62, 68) in the King IV report provided guidelines for how to apply its principles to public sector entities. Principles 11, 12 and 15 specifically dealt with how risk, information and technology were governed. Taking this into consideration accounting officers within the public sector therefore needed to start placing more emphasis not only on what their business continuity plans looked like, but who would be responsible for them. The Institute of Directors, South Africa (2016, p.61) further provided that the King IV report made provision for the creation and implementation of business continuity measures that allowed the organisation to continue to function during instances of instability, to resist and recover from disturbances.

Drawing from Smith (2012, p.10) it is agreeable that in order to embed or integrate business continuity management, a change in mind-set from that of the proven practice 'tick box' approach which was seen to deliver quick gains was required. This approach was convinced that all that was needed was a structure and strategy.

2.2.2 South Africa public sector and business continuity

National Treasury, South Africa (2018) presented that government in South Africa was in the process of growing business continuity management in the public sector. National Treasury, South Africa (2018, p.8) based its draft government resilience and continuity strategy on the ISO 22301: 2012 – requirements of a business continuity management system. This implied that the ISO 22301: 2012 would become the guiding principle to be used by the public service. National Treasury, South Africa (n.d., p.5) provided that the objective of the draft government continuity and resilience guideline was to ensure that government was prepared for and could recover from disruption thereby building government resilience. The aim was therefore to build high level resilience in all government departments in the delivery of services when facing major adverse events. An enabling environment needed to be created whereby government would be able to continue to deliver services and achieve its performance objectives.

National Treasury, South Africa (n.d., p.5) in the draft government continuity and resilience guideline confirmed government's commitment to empowering government officials to plan, implement, operate, test and maintain state continuity capability; developing continuity practices that were relevant and appropriate to build, operate and maintain government continuity capability. According to National Treasury, South Africa (n.d., p.3) effective and efficient service delivery by government when disruptive or a disaster happened remained a challenge. Government therefore had to improve planning for government continuity and resilience management in the public sector. According to the Department of Planning, Monitoring and Evaluation, South Africa (2013, p.29) it is agreeable that governance and accountability comprised the operations that linked the structures of management, ethics and being accountable to improve service delivery. To minimise maladministration and strengthen efficiencies for service delivery required effective governance and accountability.

Selowa (2016) presented that although the public sector had not reached the relevant maturity levels in business continuity, it did however have the potential to lead business continuity in South Africa, setting up resilient structures, to withstand both man-made and natural disasters. Ferguson (2018) stated that in South Africa, not many departments of the public service understood the theory and requirements of the management of business continuity. Very few departments understood the reasons for developing and maintaining systems resistant to events. Pheea (2020) examined government's response to the COVID-19 crisis and lockdown where business continuity was still viewed as an IT problem, it was not embedded within the government, non-commitment by the leadership and there is no common policy framework.

2.2.3 Public sector and ISO 22301: 2012

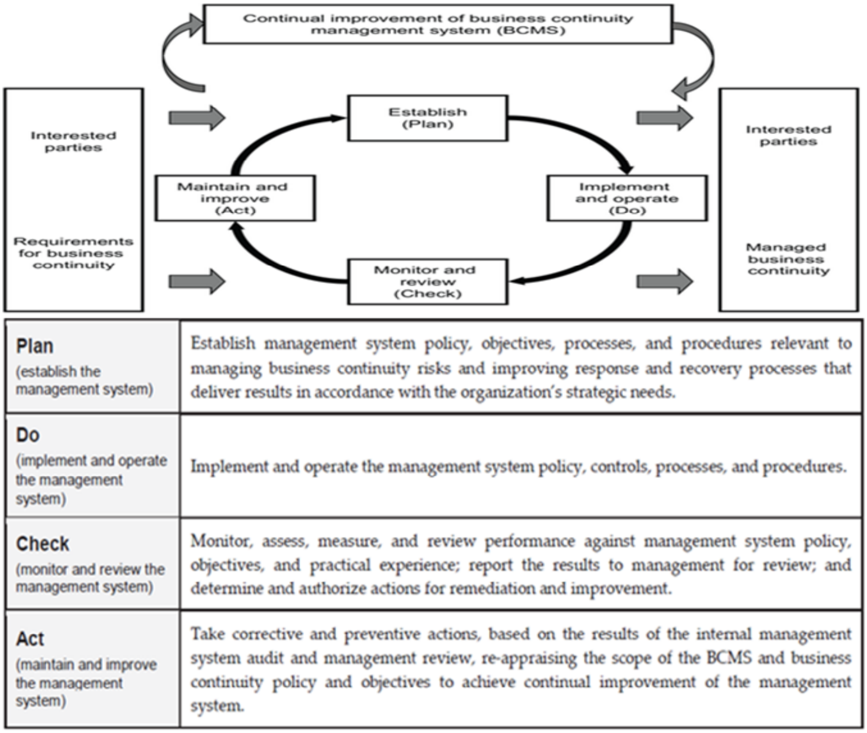
2.2.3.1 ISO Standard 22301: 2012 – business continuity management systems-requirements

The British Standards Institution (2017) developed International Standards to guide organisations. The internal standard setting body was referred to the International Organization for Standardization (ISO). ISO was an independent, non-governmental organisation composed of representatives from various national standard organisations. ISO developed the Annex SL as a generic management system which would become the blueprint for all standards going forward. ISO maintained that a management system were the processes needed by organisations to achieve its objectives. The Annex SL contained clauses, which cannot be changed (mandatory), subclauses and discipline-specific where changes and/or additions could be made. Clauses 1–4 were usually mandatory and covered the following:

- Clause 1: scope
- Clause 2: normative references
- Clause 3: terms and definitions
- Clause 4: context of the organisation.

Clauses 5–10 were discipline specific and were subject to amendments. According to the British Standards Institution (2012, p.2) the aim of the ISO management system was to assist organisations to enhance current processes. It reflected the significance of the management of business continuity to safeguard productive capability and stakeholder interests. According to British Standards Institute (2012, p.5) the ISO standard applied the Plan-Do-Check-Act model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organisations business continuity management system. The components of the Plan-Do-Check-Act model were divided into clauses and subclauses. The clauses and subclauses explained to the user what they needed to implement the standard. Figure 2 (ISO, n.d.) represented the Plan-Do-Check-Act model aligned to the International Standard 22301: 2012.

Figure 2 Business continuity management system, Plan-Do-Check-Act model – ISO (n.d.)


Continual improvement of business continuity management system (BCMS)
Interested parties
Requirements for business continuity
Establish (Plan)
Maintain and improve (Act)
Implement and operate (Do)
Monitor and review (Check)
Interested parties
Managed business continuity

Plan (establish the management system)	Establish management system policy, objectives, processes, and procedures relevant to managing business continuity risks and improving response and recovery processes that deliver results in accordance with the organization's strategic needs.
Do (implement and operate the management system)	Implement and operate the management system policy, controls, processes, and procedures.
Check (monitor and review the management system)	Monitor, assess, measure, and review performance against management system policy, objectives, and practical experience; report the results to management for review; and determine and authorize actions for remediation and improvement.
Act (maintain and improve the management system)	Take corrective and preventive actions, based on the results of the internal management system audit and management review, re-appraising the scope of the BCMS and business continuity policy and objectives to achieve continual improvement of the management system.

British Standards Institute (2012, p.6) further explained the Plan-Do-Check-Act model as follows:

- *Plan* was all about the establishment of a system for management. The business continuity management system comprised the following key components: business continuity policy, roles and responsibilities, business continuity management system, management processes, documentation, other relevant business continuity management processes.
- *Do* was concerned with the application and operation of the business continuity policy, controls, procedures and processes.
- *Check* encompassed monitoring and review of the management system.
- *Act* was interested in the maintenance and improvement of the business continuity management system.

Smith (2012, p.8) further maintained that the ISO standards were not designed to be limiting, complete or provide a decisive procedure/process to plan for all occurrences within business continuity management.

2.2.3.2 Business continuity management system

Wong and Shi (2015, p.31) explained that the business continuity management system was focused on understanding the corporate requirements and incorporating it into the business continuity policy and objectives. In an effort to align the business continuity management system to existing management processes it was useful to incorporate the business continuity standards within the context of corporate governance. This sentiment was supported by British Standards Institution (2012, p.2) in that an effective business continuity management system was one that was aligned to the organisation's corporate governance. The business continuity management system should be part of the entire management system which established, implemented, operated, monitored, reviewed, maintained and improved the continuity of business. This system of management system included the organisation's structure, processes, duties, procedures and resources.

Akinbami (2015) questioned whether business continuity plans were a real or a compliance issue? It acknowledged that a business continuity plan was essential as it set out the operations of the business and how fast it was able to return to normal business operations. Many organisations have business continuity plans, but they merely fulfil regulatory requirements. Often, they were drafted by IT departments with either little or no inputs from other business units. These plans were also not tested. The plans have not been drafted based on results of the analysis of the impact on business or the assessment of the risk. They were not customised and merely regulatory. A real business continuity management system had a business continuity plan which was developed based on a business impact analysis and risk assessment. The plan needed to be tested to ensure improvements. Business continuity was concerned with the continuous survival of the organisation rather than compliance.

Bakar et al. (2019) found that in the public service in Malaysia the demand to sustain the continuity of critical services during a disruptive event was becoming more critical. Various initiatives were undertaken by the public sector to strengthen business continuity management practices. A survey conducted in 2010 revealed that only 23% of the government agencies participating in the survey have started to implement business continuity management. Sumter (2011, p.4) found that although the occurrence of natural disasters was highly unlikely, the countries with whom they conducted business with were affected by disruptive events. The concept of business continuity was not well known, and many were unaware of its existence. Business continuity management was however required by stakeholders for compliance purposes. A risk assessment was completed to determine probability and impact. It was determined that business community management would start to play an important role should businesses want to operate in the international arena.

2.3 Linkage between risk management and business continuity

According to Smith (2012, p.26), business continuity should be aligned to the organisation's enterprise risk management program and account to the risk committee of organisations. A benefit of this approach was that it expands on what exists and ensures buy-in throughout the organisation. Price Waterhouse Coopers (2016), further explained that enterprise risk management and business continuity management shared a common goal in the identification, assessment and the management of risks that could prevent the attainment of strategic objectives. Notwithstanding that, Price Waterhouse Coopers (2016) highlighted the misalignment between enterprise risk management and business continuity management. Separate business continuity management and enterprise risk management steering committees and supervision could lead to business continuity management programs not addressing core strategic risks. Smith (2012, p.25) further maintained that the adoption of an interrelated whole-of-business/organisation method was key for business continuity to be successful. The approach aimed to endorse each of the key building blocks of the business continuity management system and elements of business continuity management. Berman (2015) provided that enterprise risk management was concerned with the identification of all threats that an organisation faces. This holistic approach provided a framework for not only mitigating risks but also advancing goals and opportunities when confronted with threats. A holistic model was needed integrating business continuity management and risk management in support of implementation and continuous management. This would result in a remarkable impact on the organisation's ability to deal with disruptions in the accomplishment of the organisation's activities. A distinction was drawn between risk management and business continuity management. The management of risk involved limiting probability whereas business continuity was involved in limiting the impact. By combining the management of risk and business continuity related into the level of resilience that an organisation must achieve. The blend was sure to not only reduce uncertainty but also to encourage a secure environment within which to operate.

Bakar et al. (2019) explained that the current world trend shows that compliance with business continuity standards is vital and demonstrates strong commitment to safeguarding business functions. It also demonstrates the realisation the importance of risk management and the protection of the organisation's assets.

3 Methodology

3.1 Research approach

The aim of the study was to explore how the public sector manages risks and business continuity. The interpretivist approach was deemed most appropriate for this particular study. Not only was this approach value laden but allowed for the exploration of the theory and to obtain rich in-depth data from the participants. It allowed for the contextualisation of the problem as it related to business continuity at the Western Cape Government. The research methodology for the study was qualitative and the use of semi structured interviews and focus groups were viewed as the most appropriate qualitative research approach. The Western Cape Government is comprised of 13 government departments. Each department is responsible for implementing laws and providing services to the citizens of the Western Cape Province. Six departments participated, with at least one representative per department. These representatives were chosen by virtue of their involvement in the management of business continuity for their respective departments. These representatives participated in the semi structured interviews. Western Cape Government (South Africa) (2016, p.30) appointed a specific department to support provincial government departments in the Western Cape to draft business continuity plans. These officials constituted the focus groups. These officials were operationally functional within departments and best suited to provide further insight in relation to their experiences in respect of the management of business continuity. Not only would their participation elicit whether they were functioning at the required levels in providing the support needed by departments, it would also provide an opportunity to gauge their level of understanding of business continuity management and their ability to impart knowledge and the implementation of such.

3.2 Sampling

The sampling frame included all those required to ensure the continuation of business within the business units of departments. The sample would therefore constitute representatives from the respective departments who had agreed to partake in the study. Non-probability sampling, specifically purposive sampling was the sampling type as it allowed for the selection of participants that could purposefully inform an understanding of risk management and business continuity within Western Cape Government departments. The study included six Western Cape Government departments. Departments were requested to identify persons who were tasked with the management of business continuity to participate in the semi structured interview. Eight individuals were identified. An observation from the sample was that more than 50% of the respondents were representative of middle and senior management. The participants of the focus group were operationally active within departments providing support with the development of business continuity plans. There were two focus groups, each group consisting of four individuals. Eight individuals therefore actively participated in the focus group which allowed for sufficient extraction of information. The respondents were not comprised of management but rather individuals who provided advice to Western Cape Government departments in relation to the development of business continuity plans. The sample therefore constituted representatives of the Western Cape Government that were tasked to either manage or provide support in respect of business continuity.

3.3 Data collection

A considerable amount of data was produced during the qualitative research. It was therefore essential to ensure the easy recovery of data for detailed analysis at a later stage. To support this type of collection of data, notes were taken during the interviews as well audio recordings and transcriptions where deemed appropriate and with the necessary permission to do so. An interview schedule was designed with the questions based on the management of risks and business continuity practices. The pre-set questions were posed to the respondents during the interview. Respondents would be allowed to provide answers in their own words and provided an opportunity to expand on their statements and/or viewpoints provided. Descriptive answers would be derived during the interview and take the form of written words. This collection method was deemed ideal for obtaining comprehensive and comparable data. The same questions were posed to all respondents. The data collected during the discussions with the focus group took the form of spoken words. The focus group discussion would be captured both in writing and recorded. A set of prearranged questions was developed to guide the discussion in relation to the research problem. Meticulous and concise notes were taken. Probing questions to elicit conversation and possibly debate was stimulated. Robust and participative engagement was encouraged. The sample was divided into two groups based on the availability of the individuals.

3.4 Data analysis

Data analysis took the form of transcription of the recorded data, typing up of the notes taken, arranging and organising the data into distinctive types depending on the source of the data. The semi structured interview allowed for more detailed discussion in respect of the questions posed. To achieve this the writer used open ended questions. The writer was able to prompt the participants to provide more information or elaborate on a thought. The study opted to use the focus group as another source of data which proved to be useful in that the participants had something in common which was important for the study. The data was analysed in order to identify whether trends and/or patterns existed. After analysis, a descriptive narrative was compiled to understand and interpret the extent of the problem and how that will lead to the facilitation of appropriate mitigations. The data collected during the interviews needed to be organised before it could be analysed. The data collected through the semi structured interviews were notes that were transcribed into written words. The recorded data captured during the focus group interviews was transcribed by typing up the notes. The narrative of the transcribed data was read and re-read for familiarisation. The data was then organised in a meaningful way using the axial coding method. This required linking related data together to reduce the data into smaller meaningful chunks. The coded data was then categorised into themes based on similarity. The themes were then consolidated to determine the final theme(s).

3.5 Reliability and validation

To ensure consistency in the interview process, the same set of pre-set questions were posed to all the respondents. To improve the assurance that the study was reliable, the qualitative analysis of the text was supplemented with other sources of information. The Western Cape Government comprised 13 government departments; each department established to serve a specific purpose. The participation of six departments was thought to be adequate to be elicit reliable and valid data. At least one representative per department was required to partake in the semi structured interview for the process to be viewed reliable and valid. The team appointed by the Western Cape Government to support departments with the development of business continuity plans had a staff compliment of 12 individuals. 50% of individuals participating was considered sufficient to extract enough information to render the process reliable and valid.

4 Findings and discussion

It is established that government has the obligation to provide services to the citizens of a country. Should government be faced with a disruption it ran the risk of being unable to deliver services to the citizens of the country. It was therefore assumed that government departments would be prepared to deal with any disruption, with the assurance that services to the citizens would continue and the risks faced by government departments were appropriately managed.

4.1 Risk management in the public sector: Western Cape Government

The review of the literature established that there was an onus on public service departments to manage risks appropriately. In the South African context, as determined in the Public Finance Management Act (Act 1 of 1999), heads of departments were deemed accountable for the appropriate management of risks. Risk management was considered a governance issue. As determined in National Treasury, South Africa (2010, p.28), Western Cape Government adopted an enterprise risk management process that provided the basis for risk management processes in departments. The process to identify risks was clearly articulated in terms of strategic, program and operational risks. It was also provided that enterprise risk management was concerned with the identification of all the threats that the organisation is faced with. A recommendation was that the management of risks should be integrated and embedded in the business activities of the organisation.

The analysis indicated that the process of risk management was a consultative process. It required engagement with business units to identify critical business units and key processes. The process of risk management entailed determining what prevented the achievement of goals. The enterprise risk management process was identified as the process for the identification of risks followed by departments which was aligned with the ISO 31000: 2009 methodology. Departments used the bowtie technique for risk identification. Enterprise risk was seen as a management issue and highly classified as it was a line function. The risk process involved the following: identification of a risk management structure at the different levels of management; indicating what the responsibilities were; ranking of risks as high or low. There were varied approaches to identify risks opposed to the enterprise risk management process; which included: stakeholder engagement, Pestle, SSRAs, RSATS, reports, incidents, root cause analysis technique, situational analysis, PDCA, hazards and MISS. Security risks were identified in terms of MISS whereas enterprise risk was seen to more financial or budget related.

The internal and external contexts of the organisation were viewed as determinants in identifying risk. The internal context related to policies, legislation. External context related to dependencies on other stakeholders. The internal and external environment with reference to the organisational cultures, political and technological environments were also determinants in the identification of risks. The findings indicate that risk management processes can be influenced. It can be argued from the findings that in order to influence the process one needed to become a subject expert to enable the relationships with departments and a partnership with the security manager was indicated as a means to influence risk management processes. A key success factor was indicated as understanding department's business processes which in turn could be used as a means for risk assessment. Furthermore, the subject expert will provide facilitation and seek buy-in from stakeholders. Not all risks were security related but related to projects. Due to the non-participation in service delivery loan itself to the inability to identify service delivery risks.

In respect to the management of risk, the following are the summarised responses from the participants:

- Enterprise risk management was a management issue; it was seen to be highly classified.
- Enterprise risk management was aligned with 31,000. The lead department was concerned with physical security and different elements of the industry. Enterprise risk management was better suited to influence on an EXCO level as it comprised management.
- Enterprise risk management was basically on a different methodology pertaining their risks which might be internal from department's inputs.
- The way risks were identified was based on stakeholder engagement and consultation, it started from there.

- The external context has different elements example technology, political, social environment and the legal environment.
- The internal context was in line with the four strategic thrusts of the WCG which was polices, organisational culture, applied methodologies, leadership and management.

From the findings it was evident that there was consensus amongst respondents that the enterprise risk management process was used by the Western Cape Government. No thought about the process but rather focused on the output. Perhaps on a strategic level this would suffice. The identification of risks by Western Cape Government departments were facilitated by the enterprise risk management team. Risks were identified during one-on-one interviews with management. During these discussions risks were identified, explored and detailed but most times not properly documented and narrated. Concerning though based on the responses was that the enterprise risk management process was deemed to be how risks were identified. No reference was made in respect of the varied sources available to identify risks as there did not seem to an exact science for the identification of risk. There was an assumption by the writer that the respondents would provide a step-by-step encounter as to how risks were identified during the enterprise risk management process. Based on this the writer was led to the assumption that a limited understanding existed amongst the respondents as to how risks were identified. There seemed to be a fair comprehension of the process of enterprise risk management. However, no mention was made in respect of the risk identification process. It would seem that the respondents on senior management level had a better understanding of the risk management process. However, they still failed to address the process of risk identification in response to the research question. Having said this, it was also noted that the lead department viewed security and enterprise risk as two different issues. The literature provided that in the context of government risk management referred to all the risks of the institution.

The writer further held the view that although an enterprise risk management strategy and implementation plan existed within government departments it was however limited to being a compliance issue and not much thought was given in respect of business continuity planning processes as outlined in ISO 22301: 2012 as opposed to having a business continuity plan in place.

4.2 Business continuity in the public sector of South Africa

From the data collected it was revealed that business continuity was actioned due to a disruptive event. A disruptive event referred to any incident, whether man-made or natural, that resulted in the non–achievement of objectives. Business continuity required a plan of processes to allow business to continue. It entailed conducting a business impact analysis to determine the critical business processes and the critical business units and staffing required. The drafting and implementation of a business continuity plan was also deemed a key process for business continuity. It was also alluded that in addition to the business continuity plan there were sub and contingency plans. The lead department indicated that support to departments were consultative, facilitative and advisory. Further to this, the lead department viewed their role to analyse documentation for departments, creating awareness and responsible for the risk management part of the business continuity plan. Building and maintaining trust, networking and using existing platforms within departments were viewed as a vehicle/mechanism to influence in favour of business continuity. The business continuity plan was a plan of action when a disruption occurred. It should include a communication protocol as to how business continuity was to be communicated amongst staff, stakeholders, and decision makers in relation to when the business continuity plan was to be actioned. The establishment of a team to run with the business continuity process, where roles and responsibilities were clearly defined.

In respect to the management of business continuity, the following are the summarised responses from the participants:

- A disruption to business may be resultant of a number of scenarios for instance: fire, water, any threats and civil unrest.
- The identification of units that would experience the biggest impact, these were units that the business cannot do without in event of an emergency.
- Focus was to have critical services up and running.
- Drawing up of plan to manage business continuity.
- Conduct a BIA, where critical business processes were identified, types of events, did review last year, how to continue critical service, flood, fire, etc. Power outages came to the fore impact on, identify events, impact, how to respond.

The findings also demonstrate that departments had a fair understanding of what business continuity meant and why it was important. The process alluded to by departments merely indicated what activated business continuity; it required the conducting of a business impact analysis in order to highlight the critical functions and business units required to perform them; resources required; clarification of roles and responsibilities; identification off the decision makers and management of the process; and the development of a business continuity plan. The findings were consistent with the requirements of the business continuity management system as identified in ISO 22301: 2012. However not all the key processes were taken into consideration. As such there was an inability to demonstrate the commitment of the leadership to business continuity as provided for in ISO 22301: 2012 and narrated in the business continuity policy. At least, the Top management's endorsement of the policy affirmed their commitment. Therefore, it is argued that the business continuity policy should be in line with the purpose of the organisation, provide the frame to establish objectives for business continuity and an assurance for the continuous improvement of the business continuity management system. It was very clear from the findings that none of the departments had a business continuity policy in place. According to the ISO standards, a business continuity management system should be implemented, which be aligned with existing management systems as business continuity affected the department holistically. This was not mentioned as part of the key processes listed by the participating departments. Neither was the importance of the legal and regulatory aspects taken into account. Smith (2012, p.8) maintained that the ISO standards were not designed to be restrictive or exhaustive to allow organisations to design its own business continuity management system appropriate to its needs. Unfortunately, the findings indicate that departments failed to have a business continuity management system in place.

5 Conclusions and recommendations

The literature reviewed affirmed that both risk and business continuity management were deemed governance issues. The literature supported that business continuity management should be aligned within the context of corporate governance. It would be most effective if embedded within government processes. The continuation of business required the appropriate management of risk to ensure continued service delivery. It can be argued that the processes in relation to risk and business continuity management were not fully understood. It was however conceded that the management of risk was an essential function of an organisation and its leaders. Of significance was the fact that risks needed to be managed for the entire organisation and not only in respect of specific business units and/or functions. Business continuity management was seen as a holistic management process that identified threats and the impact of the threats should they be realised. The literature further supported the notion that having sound business continuity processes in place would greatly support organisations with the management of disruptions. Business continuity was viewed as a process in response to managing threats posed against departments. It was found that business continuity processes were inadequate.

It is suggested that government's draft policy documents be implemented as a standard for all government departments. The failure of government has been demonstrated in this regard.

It is recommended that an appropriate structure for the management of business continuity for the government of the Western Cape should be established. A further recommendation in that the theoretical contribution to develop a framework for the Western Cape Government would prove valuable as it would guide departments with the implementation of a business continuity management system. It could therefore be concluded that business continuity should be viewed as a pre-emptive plan to circumvent and mitigate risks related with operations being disrupted. If the continuation of business can be ensured by managing risks appropriately which would in turn contribute to the resilience of the public sector.

Limitations in respect of skill, lack of experience in business continuity planning and disaster recovery skill were evident in the study.

References

Akinbami, B. (2015) *Business Continuity Lifecycle*, Linkedin [online] https://www.linkedin.com/pulse/business-continuity-lifecycle-babatunde-akinbami-abcp- (accessed 5 August 2018).

Australian Institute of Company Directors (2017) *Why Good Governance is Important to the Public Sector*, B2B Magazine [online] https://www.b2bmagazine.com.au/good-governance-important-public-sector (accessed 29 November 2018).

Bakar, Z.A., Yaacob, N.A., Udin, Z.M., Hanaysha, J.R. and Loon, L.K. (2019) 'Business continuity management implementation in the Malaysian public sector', *International Journal of Business and Technology Management*, Vol. 1, No. 1, pp.18–27.

Berman, A. (2015) *Risk Management and Business Continuity: Improving Business Resiliency, Risk Management Monitor* [online] https://www.riskmanagementmonitor.com/risk-management-and-business-continuity-improving-business-resiliency/ (accessed 9 August 2018).

British Standards Institute (2012) *The New International Standard for Business Continuity Systems* [online] https://www.bsigroup.com/LocalFiles/en-IN/Certification/ISO%2022301/ISO-22301-Implementation-Guide-web.pdf (accessed 20 October 2018).

British Standards Institution (2012) *International Standard 22301 Societal Security – Business Continuity Management Systems – Requirements*, BSI Standards Limited, UK.

British Standards Institution (2017) *International Standard 22316 Security and Resilience – Organizational Resilience – Principles and Attributes*, BSI Standards Limited, UK.

Coetzee, G.P. and Lubbe, D. (2013) *The Risk Maturity of South African Public and Private Sector Organizations*, Department of Auditing University of Pretoria and Centre for Accounting University of the Free State.

CQI (2016) *The True Meaning of Good Governance*, CQI [online] https://www.quality.org/knowledge/importance-good-governance (accessed 11 October 2018).

Denyer, D. (2017) *Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking*, BSI and Cranfield School of Management, Cranfield.

Department of Community Safety, South Africa (2018) *ERM Strategy and Implementation Plan*, Department of Community Safety, Cape Town.

Department of Planning, Monitoring and Evaluation, South Africa (2013) *Management Performance Assessment Tool*, Department of Planning, Monitoring and Evaluation, Pretoria.

Department of the Premier, Western Cape (South Africa) (2018) *Corporate Governance Framework for the Western Cape Government*, Department of the Premier, Provincial Government of the Western Cape, Cape Town.

Ferguson, C. (2018) 'Business continuity and disaster management within the public service in relation to a national development plan', *Journal of Business Continuity & Emergency Planning* [online] https://europepmc.org/abstract/med/29592825 (accessed 24 September 2018).

Fiksel, J.R. (2015) *Resilient by Design*, Island Press, Washington [online] https://www.amazon.com/Resilient-Design-Creating-BusinessesFlourish/dp/1610915879 (accessed 3 January 2018).

Hela, L. (2017) *3 Questions that the Public Sector Should Ask a Business Continuity Provider*, Continuitysa [online] https://www.continuitysa.com/3-questions-public-sector-ask-business-continuity-provider/ (accessed 30 April 2018).

Institute of Directors, South Africa (2016) *King IV; Report on Corporate Governance in South Africa, 2016*, South Africa [online] https://www.citethisforme.com/topic-ideas/other/Corporate%20Governance-43901327.

International Organization for Standardization (ISO) (n.d.) *Business Continuity Management System, Plan-Do-Check-Act Model, Digital Image* [online] https://www.iso.org/obp/ui/es/#iso:std:iso:22301:ed-1:v2:en (accessed 9 August 2018).

Moloi, T. (2016) 'Key mechanisms of risk management in South Africa's National Government departments: the public sector risk management framework and the King III Benchmark', *International Public Administration Review*, Vol. 14, Nos. 2–3, pp.37–52.

Naden, C. (2017) *Organizational Resilience Made Simple with New ISO Standard*, International Organization for Standardization [online] https://www.iso.org/news/Ref2189.htm (accessed 4 January 2018).

National Treasury, South Africa (2010) *Public Sector Risk Management Framework Guideline*, Office of the Accountant General, Pretoria.

National Treasury, South Africa (2016) *National Treasury Risk Management Forum*, PowerPoint Presentation, National Treasury, Pretoria, March.

National Treasury, South Africa (2018) *Business Continuity Strategy*, National Treasury, Pretoria.

National Treasury, South Africa (n.d.) *Draft Government Continuity and Resilience Guideline*. National Treasury, Pretoria.

Pheea, T. (2020) *Business Continuity Management, Business Resilience, Business Resilience Plan* [online] https://www.continuitysa.com/business-continuity-challenges-in-the-public-sector-and-how-to-overcome-them/ (accessed 13 January 2021).

Price Waterhouse Coopers (2016) *ERM006 – ERM and Business Continuity Management: Together at Last* [online] https://www.rims.org/Session%20Handouts/RIMS%2016/ERM006/ERM006%20ERM%20and%20BCM%20together%20at%20last%20v05%20Wed.pdf (accessed 8 June 2018).

Selowa, S. (2016) *Government Continuity Presentation – Office of the Accountant General*, PowerPoint Presentation [online] https://oag.treasury.gov.za/Event%20Documentation/20160901%20Public%20Entities%20Risk%20Management%20Forum/Government%20Continuity%20Presentation.pptx (accessed 24 September 2018).

Smith, D.J. (2012) *Organization Resilience: Business Continuity, Incident and Corporate Crisis Management* [online] http://disaster.co.za/pics/Smith_BC_Incident_Corporate_CrisisManagement_2012.pdf (accessed 26 August 2018).

South Africa (1996) *The Constitution of South Africa*, Government Printer, Pretoria.

South Africa (1999a) *National Treasury Regulations*, Government Printer, Pretoria.

South Africa (1999b) *Public Finance Management Act No. 1 of 1999*, Government Printer, Pretoria.

Southern Business School (2013) *Public Sector Management IV Study Guide*, Krugersdrop.

Sumter, G. (2011) *Business Continuity Management for Process Oriented Companies in Suriname*, Mthesis, Maastricht School of Management, Maastricht.

Venter, P. (2014) *Practicing Strategy – A Southern African Context*, Juta and Company Ltd., Cape Town.

Viljoen, R. (2015) *Organisational Change & Development, An African Perspective*, Knowres Publishing, Randburg.

Western Cape (South Africa) (2018) *The Enterprise Risk Management Process, Image*, Department of Community Safety.

Western Cape Government (South Africa) (2016) *Provincial Risks*, PowerPoint Presentation, Security Risk Managers Forum, Provincial Government of the Western Cape, Cape Town, September.

Wong, W.N.Z. and Shi, J. (2015) *Business Continuity Management System A Complete Guide To Implementing ISO 2230*, Kogan Page Limited, Great Britain and USA.