AN ANALYSIS OF THE RELATIONSHIP BETWEEN SECURITY RISK MANAGEMENT AND BUSINESS CONTINUITY MANAGEMENT: A CASE STUDY OF THE UNITED NATIONS FUNDS AND PROGRAMMES

by

JOHANNES JACOBUS VAN DER MERWE

submitted in accordance with the requirements for the degree of

MAGISTER TECHNOLOGIAE

in the subject

SECURITY MANAGEMENT

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Prof. M. SCHOEMAN

26 July 2015

TABLE OF CONTENTS

LIST OF FIGURES, TABLES & GRAPHS

LIST OF ABBREVIATIONS

BIS - Bank for International Settlements

DO – Designated Official for Safety and Security (Normally most senior UN official in country)

UN - United Nations

UNCTAD - United Nations Conference on Trade and Development

UNDCP - United Nations Office on Drugs and Crime

UNDP - United Nations Development Programme

UNDSS - United Nations Department of Safety and Security

UNEP - United Nations Environment Programme

UNFPA - United Nations Population Fund

UNHCR - Office of the United Nations High Commissioner for Refugees

UN-HABITAT - United Nations Human Settlements Programme

UNICEF - United Nations Children's Fund

UNRWA - United Nations Relief and Works Agency for Palestine Refugees in the Near East

UNW - UN Women

ITC - International Trade Centre

WFP - World Food Programme

SMT – Security Management Team

DECLARATION FORM

Student number: 39872262

I, JOHANNES JACOBUS VAN DER MERWE, declare that “AN ANALYSIS OF THE RELATIONSHIP BETWEEN SECURITY RISK MANAGEMENT AND BUSINESS CONTINUITY MANAGEMENT” is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete reference.

JJ van der Merwe	26 July 2015
SIGNATURE	DATE

(Mr JJ van der Merwe)

COPYRIGHT

ACKNOWLEDGEMENTS

"*Staff Security is not a luxury, it is not an option, it is a necessity and an essential part of the cost of doing business*."
Kofi Annan, the seventh Secretary-General of the United Nations, 1997-2006

This study is dedicated to the personnel of the UN system working in high risk security environments to further humanitarian and development goals.

In particular I would like to thank the following for their support throughout this study:

To my supervisor, Professor Marelize Schoeman, I really appreciate the continued support and understanding you provided throughout this research process. Without you this study would not have been completed as effectively.

To the UN Funds and Programmes and specifically the individual representatives who agreed to be interviewed, I am extremely grateful for your insights in risk management as it applies to your respective agencies. Without these valuable inputs it would not have been possible to complete the research.

To my family and friends, thank you for the constant motivation, assistance and support. In hard times, you were always there to cheer me up and encourage me to continue.

To my wife, Lisa Gomer, thank you for your tireless support throughout my studies. I was extremely grateful to have you as my sounding board, which ensured that the final product is practical and understandable.

EXECUTIVE SUMMARY

The goal of this research was to investigate the relationship between security risk management and business continuity management and to determine how these two methodologies are applied within United Nations Funds and Programmes. These United Nations (UN) agencies have been established to deliver humanitarian aid, economic and social development and reconstruction activities. The locations where these services are required are typically where security risks are also most prevalent. The staff of the UN, the International Red Cross and other humanitarian and development organisations have traditionally been treated as neutral parties and have not been targeted by belligerent groups. This study revealed that there has been an annual increase in security incidents against aid workers and employees of UN organisations. The changing security landscape worldwide and the increasing demand for aid and development services in especially fragile and post-conflict environments, require organisations working in these areas to maintain a high level of resilience. Their resilience can be strengthened by applying robust security risk and business continuity management methodologies.

The study included an examination of the global risk environment as it pertains to UN agencies, as well as key risk management concepts such as risk management, operational risk management, security risk management, business continuity management and organisational resilience. For the purposes of this study, security risk management is defined as the systematic approach to assessing and acting on security risks, while ensuring the safety and security of the organisation's personnel and facilities and ensuring that organisational objectives are achieved. Business continuity is a management process that identifies potential threats to an organisation, it assesses the impact to business operations − should the threats materialise − and it furthermore assists in the development of strategies to continue operations in the event of a disruption. In addition to looking at these concepts individually, the relationship between security risk management and business continuity management was also reviewed. The specific objectives set out to achieve the goal of the study were the following:

- Explore the perceptions of UN agencies about the link between security risk management and business continuity management.
- Analyse the extent of integration between security risk management and business continuity management processes and oversight.

- Make recommendations as to how security risk management and business continuity management can operate in an integrated manner with the goal of increasing the overall resilience of UN agencies.

To answer the research questions a qualitative research approach was adopted. This enabled the researcher to collect data through interviewing participants and analysing their feedback. The research focused on UN Funds and Programmes as a sub-set of agencies within the UN family of organisations. Each one of these agencies has a specific mandate, such as providing assistance to refugees, promoting food security, poverty reduction, improving reproductive health and family planning services. They also operate in fragile states as well as in emergency and humanitarian crises situations where the security risks are often higher than in normal developing countries. Eight out of 12 UN Funds and Programmes agreed to participate in the study, including: United Nations Children's Fund; United Nations Relief and Works Agency for Palestine Refugees in the Near East; Office of the United Nations High Commissioner for Refugees; World Food Programme; United Nations Development Programme; United Nations Office on Drugs and Crime; United Nations Human Settlements Programme; and UN Women. Data were collected through conducting semi-structured telephone interviews with the security manager and/or business continuity manager serving in the headquarters of each participating organisation.

Findings from the study indicated that security risk management within the UN system has evolved and that security has matured from a purely protective and defensive posture to following a risk management approach. The strength of the UN Security Management System lies in its Security Risk Management Model, which enables a thorough assessment of security risks and the implementation of commensurate mitigating security measures. In contrast to security risk management, the study revealed that business continuity as a management process is a fairly new initiative and has not yet been comprehensively adopted by all UN agencies. When combined, security risk management and business continuity management ensure the safety of staff, maximise the defence of the agencies' reputation, minimise the impact of events on the agencies as well as their beneficiaries, protect the organisation's assets, and very importantly, demonstrate effective governance. This can only be done through establishing an organisational risk management model by positioning security risk management and business continuity management within the UN agency's organisational structure so that they can effectively work together and at the same time allow access to senior management.

Good practices and apparent gaps were identified in how these two methodologies are implemented and five specific recommendations were made. The research confirmed the need for both security risk management and business continuity management and the role each function plays to enhance an organisation's resilience. It also highlighted that while they are two separate management functions, both need to be implemented within a larger risk management framework and need to be closely aligned in order to be effective. The five recommendations are:

- Incorporate security risk management and business continuity management functions and responsibilities into the larger agency-wide risk management governance framework.
- Expand the scope of business continuity in those UN agencies where it currently sits in the domain of information technology or has not yet been comprehensively implemented across the organisation.
- Establish a comprehensive crisis management framework spanning across the whole organisation from their headquarters to country offices.
- Develop the capacity to gather risk data across their agency and aggregate the data to view the full spectrum of risks, including security risks and business continuity risks in a holistic manner.
- Integrate security risk management and business continuity management processes to enhance their effectiveness.

This study contributes to the existing body of knowledge in the field of risk management by gathering relevant information from participating UN Funds and Programmes, comparing the information with other academic sources and drawing conclusions to answer the research questions. While it is expected that each organisation will have its own view on how to implement security risk management and business continuity management, the findings and recommendations as a result of the study present a series of practical recommendations on how the two functions can operate in an integrated manner in order to increase the overall resilience of these UN agencies.

Other non-UN organisations working in similar high risk environments could also benefit from the outcomes of the study, as it would allow them to compare their own approaches to security risk management and business continuity management with the information presented in this study

.

CHAPTER 1

FORMULATION AND MOTIVATION OF THE RESEARCH STUDY

1.1 INTRODUCTION

All organisations, whether they are private sector, public sector or non-profit, face the possibility of disruptive events that could impact their business operations. The consequences of these events range from short-lived disruptions to very destructive incidents. These disruptions can be caused by a wide range of threats, including loss of utilities, crime, political unrest, information technology breakdown, man-made or natural disasters, as well as social and economic issues (Graham & Kaye, 2006:1-15). If an organisation does not take proactive steps to plan and respond to these events it could have dire consequences for its business. According to Broder and Tucker (2012:225), the impact may include losing its competitive advantage and reputation, negative repercussions on the lives of its staff, and physical damage to the business and its assets. It is also estimated that between 35 to 50 per cent of businesses never recover after a major disaster (Broder & Tucker, 2012:225).

In order to prepare for and manage these threats when they occur, organisations have a variety of means available to them to increase their resilience in recovering from these incidents. Business continuity management and risk management are two key methodologies available to managers to respond to risks and their consequences. Managing risk takes place under the umbrella of risk management, which covers risk assessment, business impact analysis, risk communication and risk-based decision-making functions. According to Engemann and Henderson (2012:34), the starting point for the risk management process lies in a thorough risk assessment which aims to identify and analyse potential threats such as security risks, information technology risks and natural or man-made disasters that can impact business operations. It also includes reviewing control measures that can reduce the impact or probability of these threats from occurring.

Business impact analysis, the first step in the business continuity planning process, aims to identify critical processes and related dependencies. After analysing the potential consequences of identified risks on business operations, strategies for recovering these operations in the event of disruption can be developed. These recovery procedures are normally prioritised, since some processes have more urgent restoration requirements than others (Engemann & Henderson, 2012:4). In this study emphasis will be placed on investigating the relationship of security risk management and business continuity management.

To be effective, both methodologies, business continuity management and risk management, should be linked and not carried out independently (Graham & Kaye, 2006:65). However, if the techniques and methodologies underpinning these disciplines are not applied correctly, they could make an organisation even more vulnerable to threats and subsequent disruptions instead of increasing the organisation's resilience. This could result in strategic and operational missteps, and could potentially have a negative impact on the organisation's ability to deliver its core mandate (British Standards Institution, 2011:3-8). The focus of this study will be to investigate the relationship between security risk management and business continuity management to ensure that the two methodologies are implemented in an effective manner.

In this chapter the goals, objectives and purpose of this research study will be described. It will also state the research questions that will assist the researcher in collecting data that will be used to answer the problem statement. In addition, the chapter will explain the key concepts of risk management, security risk management and business continuity management, which will also be expanded upon in Chapter 3.

1.2 RESEARCH PROBLEM AND RATIONALE

Risk management and business continuity management are often treated as two separate methodologies, but for them to be most effective, they should be implemented in an integrated manner. By integrating these two methodologies an organisation can improve its security, reduce disruption to business operations and limit its overall exposure (Engemann & Henderson, 2012:4-5). The goal of this research is to investigate the relationship between security risk management and business continuity management and the extent to which these two methodologies are applied and integrated within the United Nations (UN) system in order for individual UN agencies to enhance their own resilience. Similar to any business environment, UN agencies are also challenged by a wide range of different internal and external factors that can test their resilience. In order for a business to achieve end-to-end service availability, operational planning and management processes must identify what kind of risks might threaten the delivery of desired results (Graham & Kaye, 2006:63). These risks are typically identified during the internal and external environmental analysis, which is performed during a strategic planning exercise.

Strategic planning is the process through which an organisation’s medium to long-term goals as well as the resources to achieve them, are defined. Internal environmental factors include issues related to the workforce, the reputation of the organisation, administrative systems and the financial strength of the institution (Ehlers & Lazenby, 2010:128). External factors include political and governmental issues, economic and technological aspects as well as the ecological environment (Ehlers & Lazenby, 2010:164). Risk management will enable senior management to identify threats and put in place appropriate mitigation measures to reduce the impact of these risks, should they materialise. Business continuity management will assist senior management to continue operations when risks disrupt business operations.

The UN is an international organisation founded in 1945 after the Second World War. The purpose of the UN is to maintain international peace and security, to develop friendly relations among nations and to promote social progress. In addition, it aims to develop better living standards and human rights throughout the world. The UN consists of six principal organs, namely the General Assembly, the Security Council, the Economic and Social Council, the Trusteeship Council, the International Court of Justice, and the Secretariat. The UN system is much larger, including 15 agencies and several other programmes and bodies (United Nations, 2004:3-6). See Annexure A for a schematic layout of the UN system.

The UN agencies have their headquarters in different locations such as New York, Geneva, Vienna, Rome and Nairobi. Many of them also have country offices or a field presence in over 100 developing countries, including in South Africa where 18 different UN agencies have established offices (Maringa, 2015). These developing countries include the “least developed” such as Angola, Chad, Eritrea, Mozambique, Bangladesh, Cambodia and Laos, to name a few (The World Bank, 2014). They also include “fragile states” which are countries in post-conflict/crisis situations or in political transition. The country contexts in fragile states range widely from violent conflict, poverty and a legacy of poor governance, to some that are emerging from crisis and cannot deliver basic services to their population. Fragile states include Nepal, Haiti, Sierra Leone, Democratic Republic of the Congo, Somalia, Afghanistan, South Sudan and Yemen (The World Bank, 2014). The security risks in these areas are typically higher than those found in developed countries and could pose additional challenges to UN agencies working in these countries.

The staff of the UN, the International Red Cross and other humanitarian and development organisations have traditionally enjoyed international legal protection in the locations where they are working. The legal basis for the protection of humanitarian workers in conflict areas is contained in the Geneva Convention of 1949 and the related Protocol of 1977 (International Committee of the Red Cross, 2013). According to Stoddard, Harmer and Ryou (2014:2), there has been an annual increase in security incidents against aid workers. In 2012 alone there were 167 incidents of major violence against aid workers in 19 countries. In 2013 there were 251 attacks affecting 460 aid workers. These attacks resulted in 155 aid workers being killed, 171 were seriously wounded and 134 were kidnapped (Stoddard et al., 2014:1). Overall this represents an increase of 66 per cent in the number of victims recorded in 2012. The majority of the persons affected were national staff employed by the different organisations. Afghanistan, Pakistan, South Sudan, Syria and Somalia continued to rank among the most violent environments for aid operations in 2013. Personnel working in these environments are exposed to security threats such as terrorism, crime, civil unrest, kidnapping, ambushes, illegal arrests, detention and natural disasters (Stoddard et al., 2014:6).

The dramatic increase in security threats and the loss of hundreds of aid workers over the past several years compelled UN agencies to re-examine the way in which they have been implementing security risk management and business continuity management (Ahtisaari, 2003:1). As a result of this analysis, UN agencies have made significant changes to their approach in employing these two methodologies, especially with regard to security risk management. This study aims to examine how UN agencies are currently applying these two methodologies in order to identify good practices as well as apparent gaps, and then recommend possible solutions.

The most prominent attacks against the UN in recent years have been in Iraq (2003), Algeria (2007) and Somalia (2013) (Doyle, 2013; Hawley, 2003; Whitlock, 2007). The attack in Iraq resulted in the death of 22 UN staff, including the Special Representative of the Secretary General, with over 150 staff members sustaining serious injuries. In Algeria, 17 UN staff members died after a suicide bomb blast (Ahtisaari, 2003; Whitlock, 2007). The attack on the UN compound in Mogadishu on 19 June 2013 resulted in extensive damage to the compound and 15 persons were killed (Doyle, 2013). Even though no such significant incidences have been recorded in South Africa, UN agencies working in South Africa also have to assess the local security situation and apply appropriate mitigation measures to reduce risks to an acceptable level. The attack on the UN office in Baghdad resulted in a comprehensive overhaul of the security management system throughout the UN. Some of the changes included the development of a security risk assessment methodology, a framework assigning accountabilities for security decisions, a methodology for measuring compliance, and recommendations for increased staffing and other resources to cover security needs (Brahimi, 2008:25).

All three of these incidents severely disrupted business operations of the UN in these three locations. Not only were staff members directly impacted, but the offices were also extensively damaged and required rebuilding before they could be reoccupied (Ahtisaari, 2003; Brahimi, 2008; Doyle, 2013). In the case of the incident in Iraq, the most senior UN manager was killed which left an immediate leadership vacuum. It is therefore clear that when security incidents do materialise, they have the potential to disrupt business operations, thus highlighting the importance of business continuity management. Any contingency planning therefore needs to take into account security risks and also strategies to recover business operations in a predefined manner. Within this context effective security measures will lessen the impact and allow business recovery strategies to be implemented more easily.

While the UN recognises the danger of working in some of these hazardous environments, the UN system through its Chief Executives Board for Coordination in 2009 endorsed a shift from “when to leave” to “how to stay” and continue to deliver their mandates, programmes and activities in spite of an increased insecure environment (United Nations, 2011). The key to this decision lies in the Security Risk Management Model utilised by UN agencies to assess the security environment in the context of delivering their respective humanitarian and development programmes in a specific location. The model also assists in identifying appropriate and commensurate security measures to reduce the level of risk to enable programmes to be implemented. This is done with the acceptance that some residual risk will remain present. The UN Security Management Model is a comprehensive security system which is coordinated by the UN Department of Safety and Security (UNDSS). In addition, many of the UN agencies also have their own security unit that provides advice to their respective managers on security matters (United Nations, 2011). The researcher has chosen to use the UN system, in particular UN Funds and Programmes for this study, because of the extraordinary security and business continuity challenges that these organisations face due to the locations where they are operating and the need to ensure business continuity in their operations.

Security risk assessments, prepared by the UN security management team in each country, are the foundation for all security measures, procedures and decisions. These assessments are made available to UN agencies present in respective countries. Each security risk assessment considers programme needs, vulnerabilities to staff, offices and residences, and the threats associated with working in a specific geographical location (UNDSS, 2009:1). The risks take into account the potential impact and probability of the threat occurring. Mitigating measures are developed to either reduce the likelihood of the threat from occurring or to reduce its impact. As a last resort, after exhausting all possible mitigation measures, the UN will consider evacuating all international staff from a specific location and relocating local staff to safer locations (UNDSS, 2009). Even though security risk management is a well-established management function within the UN system, it should not be the only risk management function these UN organisations rely on to improve their overall resilience. In 2010, the UN Joint Inspection Unit was requested to assess the status of enterprise risk management among the different UN agencies within the overall UN system. At that stage the conclusion from the assessment was that UN organisations were in the beginning stages of implementing enterprise risk management (Terzi & Posta, 2010:v). Enterprise risk management is a structured and comprehensive approach to risk management. It supports an organisation to accomplish its strategic objectives by identifying, assessing, evaluating, prioritising and controlling risks across the organisation (Terzi & Posta, 2010:1).

As will be discussed in more detail in Chapter 3, UN agencies also need to adopt business continuity management to allow them to continue their business operations when operations are disrupted (Posta & Wynes, 2011:5). This study will examine whether UN agencies have adopted both methodologies and to what extent they are integrated. The UN Joint Inspection Unit reviewed the existence of business continuity management within the UN system in 2011. The report concluded that the general level of preparedness for recovering from disruptions to business operations among the UN agencies was below the recommended level if compared to relevant international standards. The following aspects were identified as lacking: establishing relevant business continuity policies; the lack of ownership for the programme; the lack of assigning appropriate resources; and implementing business continuity programmes across the organisation (Posta & Wynes, 2011:v-iv). Only a handful of UN agencies such as the United Nations Development Programme, the United Nations Children Fund and the World Food Programme started implementing business continuity in a comprehensive way (Posta & Wynes, 2011:v).

The UN report also highlighted the potential value of following an integrated approach whereby business continuity is linked with emergency preparedness and disaster recovery methodologies in order to maintain continuous and uninterrupted operations. According to Posta and Wynes (2011:9), business continuity management is the foundation on which an organisation builds its resilience, and it facilitates the continuation of operations in the event of disruption to business activities. The report, however, did recognise that while most UN agencies did not have a comprehensive business continuity management programme in place, elements of the programme such as security risk management, medical emergency preparedness, information and communications technology systems and procedures, did exist. It was noted that each of these elements functioned in isolation and were not integrated into the overall risk management framework (Posta & Wynes, 2011:5). Building on the work of Posta and Wynes (2011:9) this study aims to explore current practice to determine if progress has been made in the implementation of an integrative approach in the utilisation of both security risk management and business continuity management programmes.

According to Graham and Kaye (2006:9), resilient organisations are better prepared to respond to disruptive events, and in some cases to prevent these incidents from escalating into more serious situations. This can be achieved by applying both risk and business continuity management methodologies. Risk management will assist with the identification of measures, and it will prioritise and treat those risks affecting an organisation. Business continuity management, in turn, aims to counteract the negative impacts of threats on the continuity of organisational activities (Graham & Kaye, 2006:9-11).

Risk and business continuity management should ideally form part of the strategic and operational planning processes. According to Graham and Kaye (2006:11-63), business continuity and risk management have historically been treated as two separate activities and in many cases these two methodologies are only considered as an afterthought. As mentioned, Posta and Wynes (2011:5) also identified the fragmented approach to risk management and business continuity management within UN agencies and recommended that they be integrated into an overall risk management framework. By employing both of these methodologies organisations can ensure that not only security risks will be considered in preparation for adverse incidents, but also their impact on business operations.

Since there are many different risks that organisations face, this research will concentrate on what are considered to be security risks, such as incidents caused through crime, civil disturbances, terrorism, man-made or natural disasters as well as the impact these security risks may have on the operations of UN agencies. In order to prepare for and respond to these risks, the researcher agrees with Posta and Wynes (2011:5) that UN agencies should strengthen their use of security risk management and business continuity management methodologies in an integrated manner to enable them to mitigate security risks and continue their operations in spite of deteriorating security environments. Integration in this case does not only refer to the actual processes, but includes establishing the appropriate governance structure, assigning sufficient resources and making sure that security risk management and business continuity management programmes span across the whole organisation.

This study has the potential to contribute to the existing body of knowledge in the field of risk management and business continuity management. Business continuity is still evolving as a business management process, and although security risk management has been practised for some time, the two processes have not yet been fully integrated. The researcher found limited literature where the relationship between security risk management and business continuity management was discussed, thus the study could make a contribution in enriching this knowledge base.

In addition, limited information exists about the perception of different UN agencies on how security risk management and business continuity management can be integrated and applied to allow good practices to emerge. As a result of this study, recommendations as to how security risk management and business continuity management can operate in an integrated manner, with the goal of increasing the overall resilience of UN agencies, would emerge. Not only will the UN agencies that are participating in the research benefit from the study, but other large non-governmental organisations such as World Vision, CARE, and international organisations such as the Red Cross, as well as South African businesses working in similar environments, would also be able to apply the lessons learned to their own organisations.

1.3 RESEARCH AIM, OBJECTIVES AND PURPOSE

Research is a process of collecting, analysing and drawing conclusions from information to answer specific questions. In addition, for it to be valid in an academic environment, the research must be carried out in a way that is controlled, systematic, valid, verifiable, repeatable and critical (Kumar, 2011:8). In order to steer the research in the right direction, the researcher identifies an aim and objectives. The aim is a broad statement emphasising what needs to be accomplished, and the objectives highlight specific issues that will be studied and are required to achieve the goal (Kumar, 2011:224). The aim and objectives of the study are therefore explained below.

1.3.1 Aim

The aim of this study is to explore the relationship between security risk management and business continuity management and to determine to what extent these two methodologies are applied and integrated by UN agencies. The researcher will also investigate if such integration can improve the overall resilience of UN organisations working in high risk security environments. Through the study good practices will be identified and apparent gaps in the effective application of security risk management and business continuity management will be highlighted, with the objective to make recommendations as to how these two methodologies should operate.

Although the study focuses on operations of the UN and in particular UN Funds and Programmes, findings from the study could potentially also be beneficial to South African businesses, especially those that have operations in multiple locations, in that it could assist with their approach for assessing security risks and ensuring the continuity of their own operations. In addition to being beneficial to the UN, the recommendations resulting from this research will also contribute to the body of knowledge in the field of organisational risk management in general

1.3.2 Specific objectives

In order to achieve the study's aim, the following objectives were identified:

- Explore the perceptions of UN agencies about the link between security risk management and business continuity management.
- Analyse the extent of integration between security risk management and business continuity management processes and oversight.
- Make recommendations as to how security risk management and business continuity management can operate in an integrated manner with the goal of increasing the overall resilience of UN agencies.

1.4 RESEARCH QUESTIONS

According to Yin (2011:67), specifying research questions is one of the first steps when undertaking research. The research questions identify the objectives that the study will address and guide the process through which data will be collected. The following research questions were identified for this study:

- How are security risk management and business continuity management applied within UN agencies?
- How do UN agencies manage their security risks and what are the main security risks faced by each organisation?
- What are the principles and methodologies that underlie UN agencies' security risk management approach?
- To what extent are security risk management and business continuity management processes and oversight integrated?
- Where do security risk management and business continuity management functions sit organisationally, and what are their reporting lines and areas where they interact?

1.5 KEY CONCEPTS

Definitions are used to help communicate and present arguments in a manner that is easily understood (De Vos, Strydom, Fouché, & Delport, 2011:33). As mentioned, this study will examine the relationship between security risk management and business continuity management. In order to prevent any vagueness or ambiguity related to the terms used in these two areas, the following key concepts are defined below: organisational resilience; risk management; operational risk management; security risk management; and business continuity management, as they apply to this study. In some cases an operational definition is included to clarify what the term means in the context of this study. According to De Vos et al. (2011:33), an operational definition links a concept with certain clearly identifiable objects in the social world.

1.5.1 Organisational resilience

According to McAslan (2011:1), the concept of organisational resilience is new to management thinking. In the past it was mainly used in the engineering field, environmental studies and when referring to the positive capacity of people to cope with stress and adversity. When referring to organisational resilience, it suggests the ability of an organisation to recover and return to normality after experiencing a disturbing and often unexpected risk (McAslan, 2011:1). It is also described as an organisation's ability to reduce and prevent any disruption to its services and its corporate governance structure (Graham & Kaye, 2006:62). Engemann and Henderson (2012:305) describe resilience as the ability of an organisation to withstand the impact of a crisis event.

In the context of this study the term organisational resilience refers to the ability of individual UN agencies to develop the capacity to recover and return to normality after experiencing significant security risks and subsequent disruption to their business operations.

1.5.2 Risk management

According to the International Standards Organisation (ISO), risk management “involves coordinating activities to direct and control an organisation with regard to risk” (ISO, 2009:10). Risk in this case is defined as the effect of uncertainty on achieving objectives (ISO, 2009:1), and it is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence. According to Engemann and Henderson (2012:35), risk management comprises the process of risk assessment, risk communication and risk treatment. Roper (1999:13) defines risk management as the process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost. He also describes risk as the potential for damage or loss of an asset.

For the purpose of this study risk management can be described as the process of identifying, analysing and communicating risk, to enable organisations to address it through accepting, avoiding, transferring or controlling measures in order to achieve an acceptable level of risk while considering associated costs and benefits of any action taken. While risk management in the context of this study will refer to all risks at an organisational level, including strategic, reputational, credit and operational risks, the specific focus will be on operational risks. Operational risk includes information technology risks and security risks.

1.5.3 Operational risk management

The term operational risk was developed by the Bank for International Settlements (BIS) and introduced in the Basel II Accords (Basel Committee on Banking Supervision, 2011). The BIS is an international organisation which facilitates international monetary and financial cooperation on banking supervisory matters. Its objective is to enhance understanding of supervisory issues and improve the quality of banking worldwide. According to the Hong Kong Institute of Bankers (2013:176-191), the Basel Accords outline a regulatory framework for banks and banking systems. Operational risk is defined as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events” (Basel Committee on Banking Supervision, 2011:3). The definition includes risks associated with legal liabilities, security, crime and business continuity, but explicitly excludes strategic and reputational risk. According to Storkey (2011:8), business continuity planning is a part of operational risk management. The objective is to prevent a business disaster when the business is impacted by an event and to ensure the continuity of operations until it can return to normal functioning.

Even though this term is not widely used outside the financial sector, it is of relevance in this study because operational risk naturally groups together individual risk areas such as security risk management, information technology risk management and procurement risk management that would otherwise remain siloed under one heading (Hong Kong Institute of Bankers, 2013:4). The causes of operational risks, according to the Hong Kong Institute of Bankers (2013:5-7), can be traced to a wide range of factors such as when employees, whether intentionally or otherwise, cause incidents, infrastructure and technology failures related to computer systems and power, or incidents where access to premises is denied. It also includes natural disasters, acts of terrorism and criminality. These causal factors are also typically the same ones that are involved in performing business processes.

Business processes are the activities that support an organisation to deliver its services. Failure in business processes, systems and people can have a direct and negative impact on the business processes that they support. The inability to perform business processes can severely impact the mission of the organisation (Hong Kong Institute of Bankers, 2013:4-5). Similarly, such impact on personnel, information, technology, equipment and other assets can also be caused by security risks. If the impact from these incidents exceeds the mitigation measures, it can have a follow-on effect by disrupting business operations. Taking these factors into consideration is thus critical from a security risk and business continuity point of view.

As mentioned above, operational risk management is a term mainly used in the financial sector and the reason why it was created, was to group risks (as explained above) that would otherwise remain separate, under one framework. Operational risks originate from inadequate or failed internal processes, people’s actions and systems failure or from external events. If they materialise then they can disrupt business operations (Graham & Kaye, 2006:92). The consequences of the disruption can have a severe impact on the organisation if the impacted processes are not restored in a timely manner. The relevance of this concept in this study is threefold: (1) it may offer an opportunity for UN agencies to group risks, including security risks that would otherwise stand alone, into one risk practice area; (2) since operational risks include crime such as fraud and other security risks like terrorism and political unrest that are considered external events, security risk management naturally fits under operational risk management; and (3) as operational risks arise from a disturbance in an organisation’s operational processes, there is a direct link with business continuity management to enable the recovery of disrupted business processes.

1.5.4 Security risk management

Security risk management is the demarcation of risks into a security silo under a broader risk management framework. Roper (1999:4) describes security as an integrated system of activities, programmes and policies for the protection of an organisation, its facilities, personnel and equipment. Risk management is defined as the method of selecting and implementing security actions to achieve an acceptable level of risk at an acceptable cost (Roper, 1999:13). The Merriam Webster dictionary (2015) defines the word “secure” as: “*to relieve from exposure to danger*” or “*the act to make safe against adverse contingencies*”; and “security” as: “*a state of being secure or measures taken to guard against espionage or sabotage, crime, attack, or escape.*” In the context of the United Nations, security risk management is defined as:

> *An analytical procedure that assists in assessing the operational context of the UN; and identifies the risk level of undesirable events that may affect personnel, assets, and operations; providing guidance on the implementation of solutions in the form of specific mitigation strategies and measures with the aim of lowering the risk levels for the UN by reducing the impact and likelihood of an undesirable event* (UNDSS, 2009:1).

Security risk management can therefore be described as taking measures to safeguard UN staff and programmes, reducing exposure to danger and creating a secure environment in order for UN agencies to implement their various humanitarian and development programmes.

For the purposes of this research, security risk management will be defined as the systematic approach to assessing and acting on security risks while ensuring the safety and security of the organisation's personnel and facilities and ensuring that organisational objectives are achieved. Security risks can originate from a wide range of sources, but for the purpose of this research these individual threats are aggregated into five main categories, namely: armed conflict; terrorism; crime; civil unrest; and hazards such as natural disasters.

1.5.5 Business continuity management

The ISO (2012:2) defines business continuity management 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 organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities*.

An incident can be described as a situation that might be, or could lead to, a disruption, loss, emergency or crisis. An incident occurs when a risk materialises and the impact of the risk results in the disruption of business operations. Depending on the nature of the risk, the impact may also directly affect the life and safety of the personnel in the organisation. Responding to these risks will require an initial response to protect staff, followed by a business response to recover impacted business operations (Engemann & Henderson, 2012:38).

The predecessor to business continuity management was disaster recovery planning, which was mainly related to recovering information and communication technology services following a disruption. The anticipated impact and wide-spread preparation for the millennium bug (Y2K) is a well-known example of successful continuity management. The preparation for Y2K resulted in the development of many processes and standards. These standards focused mainly on information technology services management and systems recovery. It became very clear, however, that the whole organisation, and not just the data or information technology infrastructure, needed protection. Information technology is just a subcomponent of business continuity management (Posta & Wynes, 2011:3).

Risk and business continuity management are key management functions in order for an institution to be resilient. Without risk management, threats that may affect the business will not be identified, and without business continuity management it will not be possible to determine the impact of these risks on the business and develop appropriate business recovery plans. In addition, in order to be effective, risk and business continuity management must be integrated and also support the organisation’s strategic and operational plans (Graham & Kaye, 2006:4). Through this integration, organisations will be able to reduce the impact and frequency of risks and also improve the ability and speed at which they respond and recover from disruptive events, which in the case of this study are caused by security risks.

1.6 VALUE OF THE RESEARCH

Research is a way of thinking with the objective to critically investigate various aspects of a stated problem in order to understand what the issue is and then to recommend suitable solutions (Kumar, 2011:1). Finding answers to a question through a research study also implies that the process is undertaken within a set of philosophies, procedures and methods that have been tested for their validity and reliability and are designed to deliver results that are unbiased and objective. The information builds on knowledge that was created in the past and is designed to solve a particular problem. The research must be of a high quality in order for it to be considered credible (Kumar, 2011:5). This study aims to review the body of knowledge around risk management and business continuity management and how these two methodologies have evolved. The research will investigate the relationship between security risk management and business continuity management and will explore how the two methodologies are applied by UN agencies in order to identify good practices and apparent gaps and to make recommendations as to how these two methodologies should operate with the goal of increasing the overall resilience of UN agencies.

As mentioned previously, when the security situation deteriorates, agencies would in the past temporarily suspend or terminate their operations, evacuate expatriate staff and relocate national staff to safer areas. This was done after all possible mitigation measures (such as sheltering) were in place, and the number of personnel had been reduced to essential staff only, to ensure that the safety and security of staff had been exhausted (United Nations, 2011). Recently, as mentioned previously, UN agencies have been adapting to the new approach, shifting from “when to leave” to “how to stay and deliver”. This approach requires these agencies to be more resilient to cope with security incidents and also to reduce the impact these incidents have on their business operations (United Nations, 2011). In effect, this approach means that UN agencies have adopted a higher risk tolerance, which also requires them to consider a wider range of risk mitigation measures as well as methods and procedures to continue their operations in the event that a security risk materialises. In this study it is proposed that business continuity management and security risk management should be aligned with the strategic and operational objectives of the organisation and that the two processes should be closely linked and not implemented in a siloed fashion. Combining security risk management and business continuity management in this manner will enhance their resilience and also be more conducive to an approach of “how to stay and deliver”.

1.7 CONCLUSION

This chapter described the aim, objectives and purpose of this research study. It also defined important concepts such as organisational resilience, risk management, operational risk management, security risk management and business continuity management that will be further elaborated on in Chapter 3. This chapter also gave a description of how organisations and businesses have been challenged by the significant rise in security threats over the past years, resulting in the need for utilising both security risk management and business continuity management methodologies as approaches for strengthening their resilience. This is especially true for UN agencies working in many volatile areas across the world.

Chapter 2 will describe the research methodology that was used to explore the relationship between security risk management and business continuity management, and how the two methodologies are applied by UN agencies.

CHAPTER 2

RESEARCH METHODOLOGY

2.1 INTRODUCTION

Research aims to answer academic questions. In order for it to be recognised as research it must be carried out within a predefined framework and it needs to meet the requirements of validity and reliability. The outcome must be unbiased, objective and the same conclusions should be reached if the particular study is repeated under the same circumstances (Kumar, 2011:5). As mentioned, the goal of this research is to investigate the relationship between security risk management and business continuity management and to determine how these two methodologies are applied by the UN agencies. In order to answer the research questions the researcher will gather and analyse relevant information from UN agencies. The methodology outlined below explains how this study will be carried out in order for it to be considered reliable academic research in accordance with the description above.

Data will be collected making use of semi-structured interviews with the security managers and the business continuity managers within the sample of UN agencies. At the conclusion of the data collection phase, all the information will be analysed and conclusions will be drawn from the findings. The final output from the research will be to make recommendations as to how security risk management and business continuity management can operate in an integrated manner with the goal of increasing the overall resilience of UN agencies.

2.2 RESEARCH DESIGN

Research design is a detailed plan for how the study is going to be completed. The research design has two main functions: (1) to identify and develop procedures required to undertake the study; and (2) to emphasise the importance of quality in these procedures to ensure the validity, objectivity and accuracy of the outcome (Kumar, 2011:94).

According to Yin (2011:76), the research design is a logical plan for linking the research questions to the data having been collected and the methodologies for analysing the information so that the findings which emerge, answer the research questions. The main components of the design are to: (1) decide on the subject of the study; (2) collect data from relevant sources to answer identified research questions; (3) analyse and interpret the results; and (4) draw conclusions based on the findings. The plan for conducting this research is outlined in detail below (also see Kumar, 2011:94). Research can be categorised from a number of perspectives. Firstly the researcher has to decide on the purpose of the research. Research can either be undertaken for academic or for functional and practical purposes (Kumar, 2011:10). Pure research, which is also known as basic research, focuses on developing and testing theories that may or may not have a practical application. Applied research is used to collect information and then applying it in a practical way to solve problems or to better understand a particular situation (De Vos et al., 2011:95). This particular study can be categorised as applied research because the information gathered will be used for practical purposes. The objective will be to understand and document the relationship between security risk management and business continuity management and to explore how the two methodologies should be implemented to enhance the resilience of participating UN organisations from a risk perspective.

Research projects can also further be divided according to the objective of the study, namely correlational, descriptive, explanatory and exploratory research (Kumar, 2011:10-11). Correlational studies establish a relationship or interdependence between two or more aspects in a particular setting. Explanatory research endeavours to explain why and how there is a relationship between two aspects in a situation. Descriptive studies attempt to describe a situation or a problem (Kumar, 2011:10-11). Exploratory research is when a study is undertaken with the goal of exploring an area where little is known, or investigating the possibility of undertaking particular research. It is typically used to gain more insight into a particular situation (De Vos et al., 2011:95). The researcher used the objective of exploratory research to identify good practices and apparent gaps, and make recommendations as to how security risk management and business continuity management can be more effectively implemented within UN Funds and Programmes.

The third perspective is the approach that will be adopted for finding the answers to the research questions, making use of either a qualitative, quantitative or mixed methodology approach (Kumar, 2011:11). Quantitative research is used when the researcher wants to quantify the variation in a situation. In this case information is mainly gathered through quantitative variables and the analysis is geared towards calculating the magnitude of the variation (Kumar, 2011:13).

Qualitative research, according to Yin (2011:7-8), is mainly used to study people in real-world settings, and it represents their views and perspectives as participants in the research. It focuses on real-world events and not the values or meanings held by researchers. The information is collected from a variety of sources rather than relying on a single source. Quantitative research, as compared to qualitative research, is structured and it is mainly used to quantify variations and diversity or to determine the extent of the issue. Everything that is included in the process is predetermined, such as the objectives, the design, research population, sample, and questions (Kumar, 2011:11-15). It is also possible to combine the two approaches and carry out mixed-method research (Kumar, 2011:15). According to Yin (2011:289-294), mixed-method research allows the researcher to take advantage of the good in both methods by making use of data collection methods from both approaches.

In this study, the researcher adopted a qualitative approach because the objective of the study was to examine how security risk management and business continuity management were being applied by UN Funds and Programmes. The study was not attempting to quantify or to measure change over time, which would have necessitated a quantitative approach.

In order to achieve the study's aim, an applied, exploratory and qualitative approach was thus followed. The approach was deemed well suited for the study because it is more flexible in its design and allowed for the collection of field-based data which reflected the views of all participants interviewed. It also allowed for the data to be analysed within the contextual environment of the UN Funds and Programmes.

2.3 POPULATION AND SAMPLING PROCEDURES

A research problem relates to a specific study population. In order for the researcher to achieve the goals and objectives of the research study, relevant data have to be collected from the study population (De Vos et al., 2011:93). Because it is often not viable and too costly to collect information from an entire population, researchers use sampling, which is the process of selecting a few participants from a larger group to collect information from (Kumar, 2011:193). The population of the study is a group of potential participants for whom you want to generalise the results of the study. It is also important to assemble a sample which is representative of the larger population (Welman, Kruger & Mitchell, 2006:55). For the purpose of this study the population will be the organisations that make up the United Nations system. The reason for selecting the UN is because it is a universal organisation and it's agencies work in a variety of locations where security threats are prevalent. Being exposed to security threats requires a higher level of resilience to enable their operations to continue in volatile environments.

2.3.1 Unit of analysis

According to Kumar (2011:55) there are two components of a research study that is important, one is a clear description of the research problem and the other is the identification of the study population from which data will be collected. Since the population may be made up of different groupings, such as individuals, organisations, or events it is necessary to identify the specific entity within the population which will being studied. These entities are referred to as unit of analysis (Welman, Kruger & Mitchell, 2006:53).

As previously mentioned, for the purpose of this study the unit of analysis was the UN Funds and Programmes. The UN system is very large and made up of many diverse organisations, some of which are based only at headquarters, and others which in addition to their headquarter offices, also work in field environments. The unit of analysis for this research will be those UN agencies that are considered as UN Funds and Programmes, namely the:

- United Nations Conference on Trade and Development (UNCTAD).
- United Nations Development Programme (UNDP).
- United Nations Environmental Programme (UNEP).
- United Nations Population Fund (UNFPA).
- United Nations Human Settlements Programme (UN-HABITAT).
- Office of the United Nations High Commissioner for Refugees (UNHCR).
- United Nations Children's Fund (UNICEF).
- United Nations Office on Drugs and Crime (UNDCP).
- United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA).
- United Nations Entity for Gender Equality and the Empowerment of Women (UN Women).
- World Food Programme (WFP).

According to the United Nations (2004:36-45), UN Funds and Programmes were created by the United Nations General Assembly to address specific humanitarian and development concerns. Each one of the funds and programmes is headed by an executive director who reports through an executive board, made up of representatives of member states to the General Assembly. Each one of these UN Funds and Programmes has a specific mandate, such as refugees, development assistance, food aid, or the environment. These agencies are subsidiary bodies of the General Assembly, but report to distinct inter-governmental bodies and derive most of their financial resources from other sources than the UN’s budget (United Nations, 2004:36-45).

The reason for choosing UN Funds and Programmes to participate in the research is because their activities are more operational and carried out at field level compared to other members of the UN family of organisations, which predominantly focus on political issues, global peace and security, and advocacy for women, human rights and education (Chief Executives Board Secretariat, 2014). Many of the UN Funds and Programmes operate in fragile states as well as in emergency and humanitarian crises where the risks are higher. As previously mentioned, it is considered very important for these organisations to be resilient and able to recover from the impact of all risks (including financial, reputational, operational and security risks) in order to assure the effective functioning of their operations while also protecting their staff and premises from harm.

2.3.2 Sample and sampling strategy

Kumar (2011:192) describes the purpose of sampling in qualitative research as to develop an in-depth knowledge about the study topic, whereas in quantitative research the objective is to derive logical conclusions about the population being studied. In addition, different criteria are applied for determining the sample size in qualitative research versus quantitative research. For a qualitative study the researcher does not necessarily have a predetermined sample size, because the participants in qualitative research are chosen based on who will be able to provide the required information, whereas the sample size for a quantitative study is normally predetermined (Kumar, 2011:192). In order to ensure that in this study the sample is representative of the larger population (the UN Funds and Programmes), three principles were adhered to. According to Kumar (2011:194-197), the first principle referred to as randomisation is used to ensure that each unit has an equal and independent chance of being selected in the sample. The second principle focuses on avoiding sampling errors. This aims to increase the accuracy of the information collected by increasing the sample size, since information collected from a small sample will not necessarily be representative of the overall population. The third principle focuses on the extent of variation in the sampling population, especially in cases where the variable that is being studied is very different in the population for a given sample size. Due to the small number of UN Funds and Programmes – and to uphold the principles suggested by Kumar (2011) – they were all invited to participate in the study.

According to Kumar (2011:198), there are two sampling strategies, random or probability sampling; and non-random or non-probability sampling. For a sample to be random, it is important to demonstrate that each element in the population has an equal and independent chance of being selected into the sample. Equal in this case means that the probability of selection of each element is the same, and independence means that the choice of one element in the sample is not influenced by other considerations (Kumar, 2011:198-199). In non-probability sampling the probability that any element of the population will be included cannot be specified (Welman et al., 2006:56).

In qualitative research, the sample is most often identified in a deliberate manner. This is called purposive sampling, which is a sub-category under a non-probability sampling strategy. The reason for this approach is to collect information from sources that are likely to have the most relevant data, given the subject of the study (Yin, 2011:88). This method is normally used when the researcher has a specific plan in mind. The researcher then relies on own experience or other factors to intentionally select the sample regarded as being representative of the population (Kumar, 2011:206-208).

Another important factor to be considered when identifying the sample is to ensure that it is representative of the study population from a generalisation point of view (De Vos et al., 2011:155). The researcher can only generalise the findings of the specific study when it can be assumed that findings from the original sample selection would also be observed if another sample were selected from the study population.

For this study the identified UN Funds and Programmes were deliberately selected from the rest of the UN system, as these organisations can provide the most relevant information to achieve the objectives of the study. This sample included all the identified organisations representative of the UN Funds and Programmes. Of the 12 UN Funds and Programmes which were invited to participate in the research, three agencies declined and one of the invited participants did not respond at all. The final sample thus consisted of eight UN Funds and Programmes.

The responsibility for managing security risks within the UN is a shared responsibility among managers and staff. In March 2004, the UN issued a comprehensive accountability framework outlining responsibilities at various levels (United Nations, 2011). In order to collect the information needed for this study from each of the UN Funds and Programmes in the sampling group, the researcher interviewed the security manager and/or business continuity manager serving in the headquarters of each invited organisation. The reason for selecting the security managers and business continuity managers to participate in this study was because they are usually senior managers in the organisation who are responsible for preparing, in consultation with the senior management team, the security and business continuity plans for the organisation as a whole, and then overseeing their implementation.

2.4 DATA COLLECTION

The term data refers to organised information collected though interviewing, observing or measuring, and it may consist of numbers, words and images. In qualitative research the researcher is the main research instrument and although the events being measured are external, the information is analysed and interpreted by the researcher (Yin, 2011:129-130).

Once ethical clearance had been granted for this study the researcher commenced with the field research. A cover letter requesting each organisation to participate in the study was sent to the Chief of Security for each one of the UN Funds and Programmes. The cover letter included a copy of the approved research proposal, an informed consent form (Annexure B), an ethical clearance certificate (Annexure C) and a list of questions to be asked during the interview. Due to the wide distribution of offices globally, the cover letter requested permission to conduct semi-structured interviews (Annexure D) by telephone with the relevant security managers and business continuity managers.

As representative(s) from each organisation agreed to participate in the research study, they recommended the names and contact details of relevant staff in their organisations for the researcher to interview. The researcher then contacted all of the potential participants and arranged for the interviews to take place by phone. The researcher confirmed with each interviewee at the beginning of the interview that their identity and the identity of the organisation they represented would not be disclosed. In addition, the researcher confirmed that the information collected would be kept confidential and only used for the purpose of the research study. A semi-structured interview was conducted with each participant. The researcher used a list of themes and questions to explore the subject of the research in an informal manner. The questions were open ended to limit single word responses and to encourage participants to use their own words to discuss the topic. It also allowed the researcher to obtain more in-depth information on the subject by asking follow-up questions. This approach made it less likely that a question would be misunderstood. The data collected from each interviewee were anonymised to ensure confidentiality by assigning each interviewee an alphabetic letter, for example, “Interviewee A”, instead of using their names or identifying their organisation.

2.5 DATA ANALYSIS AND INTERPRETATION

According to De Vos et al. (2011:397), analysing and interpreting collected data are seen as two steps in the research process. Yin (2011:177) recommends a five-phase cycle for analysing qualitative data. The five steps include: (1) compiling the information; (2)

disassembling the information; (3) re-assembling the information; (4) interpreting the information; and (5) reaching conclusions. The researcher followed Yin's sequence to analyse the data collected through the semi-structured phone interviews.

2.5.1 Compiling the information

During the interview the researcher took meticulous notes of the conversation. Where more information was needed, follow-on questions were asked. After each phone interview, the notes taken during the conversation were reviewed and converted to fuller notes. The next step was to organise the data in a systematic fashion and to structure it into a consistent format (Yin, 2011:182). This was done by sorting the notes from each interview into a particular order and ensuring that the information was complete and accurate.

2.5.2 Disassembling the information

During the semi-structured interviews, the interviewees were asked questions which they then proceeded to answer. However, since the questions were open ended, the answers sometimes covered one or more topics. When the notes were taken and later updated, the responses were kept in the order of the original conversation. According to Yin (2011:186-190), the researcher can then decide to code or not to code the data. Due to the amount of information collected in this study, it was not deemed necessary to code the information. During the second step of the analysis process the information in the interview notes for each participant was extracted and re-grouped with similar data from other participants under the topic of each question. This enabled the researcher to review the information from all the participants − grouped by topic − to see if there were common or diverging themes among the responses.

2.5.3 Re-assembling the information

After the information had been disassembled, it was re-assembled into smaller themes, assigning each section a specific label. These themes were then sorted by issues related to risk management, business continuity management and their relationship to each other. After this step, the information was re-assembled and grouped into specific themes. These themes became part of the final research report. While re-assembling the data, the researcher continued to assess the information to see if new patterns emerged and also how these patterns related to the research questions and objectives (Yin, 2011:191).

2.5.4 Interpreting the information and reaching conclusions

The final two steps entailed the interpretation process, when the researcher proceeded to draw conclusions and formulate recommendations as to how security risk management and business continuity management can operate in an integrated manner with the goal of increasing the overall resilience of UN Funds and Programmes. This phase may be seen as the culmination of the analysis where the data collected will achieve meaning (Yin, 2011:208).

2.5.5 Data security

The data and correspondence with the different participants have been properly secured throughout the process. The invitation email and follow-on exchanges have been saved in a specific folder in the researcher's Gmail (email) account. The account is password protected and the researcher is the only person with access to the information. During the interviews handwritten notes were taken and these notes were then converted into fuller notes. The handwritten notes have been filed and kept safely by the researcher. All other electronic information is stored on an external hard drive, which is used only by the researcher.

2.6 VALIDITY, RELIABILITY AND ACCURACY OF COLLECTED INFORMATION

According to Yin (2011:78), a valid study is one where the data have been properly collected and interpreted, so that the conclusions accurately reflect the environment that was studied. Kumar (2011:177) continues by saying that in order for a study to be recognised as reliable and accepted research, it has to meet the requirements of validity and reliability. The manner in which the research process is conducted can affect the accuracy and quality of the findings (Kumar, 2011:177). The feedback provided by the participants form the basis of the findings and conclusions of the study. Responses to the questions comprise the inputs for consideration and analysis, and the findings comprise the outputs. The criteria of validity and reliability must therefore be applied to every aspect of the research process, including the selection of the sample, the collection of the information, analysing the data and writing the final report. If one or more of these steps are not performed with precision, then the accuracy and quality of the final product will be questionable (Kumar, 2011:177).

Validity in the broader sense refers to the ability of the research instrument to demonstrate that it is finding out what it has been designed to do, and reliability refers to consistency in the findings when used repeatedly (Kumar, 2011:184). Validity can also be described as the correctness and accuracy of the research process adapted to finding answers to the set of research questions. It applies to the process as a whole and also to the individual steps within the process. Validity is the extent to which the research findings accurately represent what is really happening in the situation being studied (Kumar, 2011:178). Kumar (2011:181) defines reliability as the extent to which repeated measurements made under similar conditions will offer the same results. Reliability is concerned with the transferability and the credibility of the findings. Therefore, when the same set of information is collected more than once, using the same instrument and the same results are achieved under similar conditions, then the instrument is considered to be reliable. In this particular study, the use of telephone interviews combined with a clear set of interview questions which were communicated in advance of the interviews, resulted in the researcher collecting accurate, comprehensive and consistent data.

In qualitative research the validity and reliability of the research are determined by four indicators: credibility, transferability, dependability and conformability (Kumar, 2011:184-185). Credibility is synonymous with validity, and it is believed that participants are in a good position to decide whether or not the research findings have been able to accurately reflect their opinions. The more accurately the study reflects the views of the participants, the higher the validity of the study. Transferability may be more difficult to establish because it may be very difficult for the research to be generalised or transferred to other settings. Dependability is very similar to reliability, and it is concerned whether the same results can be achieved if the study is repeated. In qualitative research, it may also be difficult for others to replicate the study unless the researcher maintains an extensive and detailed record of the process. Lastly, conformability is the degree to which others can substantiate the results of the study (Kumar, 2011:184-185).

To meet the requirements of the concepts of validity and reliability the following specific practical steps were taken. First, all 12 UN Funds and Programmes: UNCTAD, ITC, UNDP, UNEP, UNFPA, UN-HABITAT, UNHCR, UNICEF, UNDCP, UNRWA, UNW and WFP were invited to participate in the study. The same process of data collection and analysis was followed with each one of them to ensure a consistent approach. This ensured that data gathered across the different UN Funds and Programmes could be properly compared. This verification of the information served as a way of strengthening the validity of the study. All the participants were asked the same basic questions and the information was cross-referenced to ensure accuracy and consistency. It was also important to gather a sufficient amount of detailed and varied data to analyse. Because the interviews were semi-structured, there was an opportunity to word questions in such a manner so that they were not ambiguous and were clearly understood, as well as giving the researcher the opportunity to probe deeper into an area through follow-up questions. In addition to the above, an attempt was made to ensure that each interview captured information related to the objectives of the research in a way as factually and neutral as possible.

By using a consistent approach, interviewing the same status of people in each of the UN Funds and Programmes, and by keeping meticulous records of the process and the data collected, the researcher enhanced the credibility and dependability of the research. By capturing and analysing the data in a factually neutral manner, the researcher increased the validity of the study because the analysis truly reflected the views of the respondents and was not distorted or tainted by the researcher's own views. As mentioned above, while the transferability of the research may be difficult, the results of this particular study could indeed be transferred to other similar types of entities such as non-profit organisations that also work in post-conflict and fragile state environments, because they face the same type of security and business continuity challenges as the UN agencies that participated in this study.

2.7 CHALLENGES EXPERIENCED DURING THE RESEARCH PROCESS

Carrying out the research presented four main challenges, but none of them were severe and neither did they impact on the validity and reliability of the study. The first challenge was to obtain permission from all the UN Funds and Programmes invited to participate in the research. In some cases it required the researcher to follow up multiple times with different people in the UN agencies to ensure that permission was granted. The researcher then had to identify the appropriate participants to interview from each of the UN Funds and Programmes. In some cases, through an interview with one representative of an organisation, the researcher obtained additional referrals of other appropriate staff to interview. Scheduling the phone interviews was time consuming because of the availability of the interviewees and the difference in time zones between the researcher and the interviewees. Due to the semi-structured nature of the interviews, it was difficult to keep them within the agreed time period of one hour. In some instances, the interviewee had so much relevant information to share that the interviews lasted up to 90 minutes. The researcher was flexible to accommodate the participants and so the challenges were not insurmountable.

2.8 ETHICAL CONSIDERATIONS

The research activity is usually described in a formal protocol that sets forth an objective and a set of procedures designed to reach that objective (National Commission for the Protection of Human Subjects of Biomedical and Behavioural Research, 1978:3). Ethical behaviour in research is not only restricted to honesty and plagiarism. It must also cover the whole research process, including respect for the rights of individuals in order for the output to be credible (Welman et al., 2006:181). The Belmont Report, developed by the National Commission for the Protection of Human Subjects of Biomedical and Behavioural Research, set out three basic principles for conducting research involving humans and provided guidelines to ensure that these principles were followed. The principles are respect for persons, beneficence and justice (National Commission for the Protection of Human Subjects of Biomedical and Behavioural Research, 1978:4).

In research, respect for persons requires that the participants enter into the research study voluntarily and that they are briefed on the goals of the research. Beneficence has to do with two complementary expressions: (1) do not harm; and (2) maximise possible benefits and minimise possible harms to persons participating in the study. Researchers and their institution have to plan to maximise benefits and minimise risks. In order to maintain confidentiality and ensure privacy, a researcher needs to keep the identifying details of the participants anonymous (National Commission for the Protection of Human Subjects of Biomedical and Behavioural Research, 1978:4-10). Justice, in the Belmont Report (1978), refers to the benefits and harm to individual subjects of research. An injustice occurs when some benefit to which a person is entitled is denied without good reason or when some burden is imposed unduly (National Commission for the Protection of Human Subjects of Biomedical and Behavioural Research, 1978:4-10). In accordance with De Vos et al. (2011:119) privacy deals with an individual's right to decide to what extent their beliefs and behaviour will be revealed and researchers should take this into consideration. Confidentiality deals with the agreement between the researcher and the participants regarding access to the other's private information, and anonymity can only be assured when no one, including the researcher, is able to identify participants during and after the research study (De Vos et al., 2011:119).

In addition to these three principles identified the Belmont Report (1978), it also provides guidance on the application of these principles. Respect for persons requires that the subjects participating in the study, to the degree that they are capable, be given the opportunity to choose what shall or shall not happen to them. The consent process must provide information to the participant about the research, confirm that they understand the information, and then allow the person to voluntary participate rather than being forced or coerced into participation. As can be seen from the above, a research process of this nature requires ethical considerations to be applied to all aspects of the process. Some of these include collecting information, seeking consent from participants, avoiding bias, incorrect reporting and the inappropriate use of information (Kumar, 2011:244).

In this research study no information was collected without the informed consent and voluntary participation of the participants. First, the researcher contacted the chief security or business continuity officer in each UN agency to explain the study and to seek their consent to participate. Secondly, when the identified individuals in each organisation were approached, they were also informed about the type of information being collected, why the information was being sought, how it would be used and how it would directly or indirectly affect them. Throughout the process, the identities of the UN Funds and Programmes and the individual participants, as well as the data provided, were protected and kept confidential. This study did not provide incentives to the participants and each interviewee freely agreed to participate in the study.

The researcher only collected information relevant to the objectives of the study through telephone interviews with each one of the participants. During each interview, the researcher took comprehensive notes which were safely kept and stored by the researcher on a home computer with proper password protection. Nobody else has access to the information. In addition, the nature of the data collected was not sensitive as it pertained to understanding and then evaluating the UN agency's approach and procedures with regard to security risk management and business continuity management. The names of the organisation and individuals interviewed were masked to ensure confidentiality and anonymity by assigning each respondent an alphabetical letter such as "Participant A" and only referring to that letter as a means of identifying the respondent in the study. Once all the data had been collected, the information was analysed and presented in the dissertation. At the end of the process, the information was archived by the researcher and will be stored for a minimum of five years as stipulated in the UNISA Policy on Research Ethics. The only person with access to the information throughout and after the research, is the researcher.

The researcher adhered to the UNISA Code of Research Ethics at all times in order to uphold the principles of quality and confidentiality. The information will not be shared with others for purposes other than this research and only appropriate methodologies, within the researcher's knowledge, were used to carry out the study. The final dissertation will be sent electronically to each of the UN Funds and Programmes that participated in the study.

2.9 CONCLUSION

The goal of this research is to investigate the relationship between security risk management and business continuity management and to determine how these two methodologies are applied by the UN agencies. The methodology outlined above explains how this study was carried out in order for it to be considered proper research. Data were collected through semi-structured interviews with the security managers and business continuity managers within the sample of UN agencies. At the conclusion of the data-collection phase, all the information was analysed and conclusions were drawn from the findings. Finally recommendations were made as to how security risk management and business continuity management can operate in an integrated manner with the goal of increasing the overall resilience of UN agencies. In order to achieve the objectives of the study an applied, exploratory and a qualitative approach was followed. The approach is well suited for the study because it is more flexible in its design and allowed for the collection of field-based data, which will reflect the views of all participants. It also allowed for the data to be analysed within the contextual environment of the UN Funds and Programmes.

Chapter 3 explores in more depth security risk management and business continuity management and the operating environment in which UN Funds and Programmes carry out their work.

CHAPTER 3

CONCEPTALISING BUSINESS CONTINUITY MANAGEMENT AND SECURITY RISK MANAGEMENT IN UN FUNDS AND PROGRAMMES

3.1 INTRODUCTION

As mentioned in Chapter 1, organisations must be able to cope with changes in the environment in which they operate. These changes may be as a result of new strategies adopted by competitors, stakeholder expectations, staff turnover and the requirements of new legislation (Graham & Kaye, 2006:1-15). Change is inevitable, but it is better dealt with proactively rather than reactively. Even though most organisations are normally able to deal with routine events such as the management of daily activities, they should also be prepared to respond to potentially disruptive events, which may exceed the capacity of existing management methods and structures. This can be done by developing contingent capacity within the management framework and by preparing for unforeseen events which might disrupt business operations. Being proactive will enable the organisation to change its mode of operations to help ensure the continuity of business operations, despite the occurrence of a potentially disruptive event. By having these capacities and plans ready, management can quickly turn their attention to stabilising the situation and recovering the most critical functions, until eventually all operations are restored. Maintaining business continuity is an important responsibility of good governance (Graham & Kaye, 2006:38). Organisations must develop strategies to effectively manage disruptions and to enhance their resilience. This will also create strategic and tactical advantages in uncertain and volatile environments for those organisations that are prepared.

Over the past decades natural disasters, pandemics, engineering failures, financial crises, cyber security incidents, crime, civil unrest and terrorism have increased the interest in risk management (Haimes, 2009:3). Risk is generally ever-present in our lives on a daily basis, whether we are crossing a street or while managing a business. According to Haimes (2009:4), risk is a measure of the probability and the severity of adverse effects. ISO (2009:1) in turn defines risk, as mentioned previously, as an effect of uncertainty on achieving organisational objectives. Risks are present in all decisions and activities undertaken by organisations, and some of these risks − if they occur − will present continuity issues. As previously explained in Chapter 1, business continuity management and risk management, including security risk management, are three key methodologies available to managers to respond to risks and their consequences. Proactively managing risks, as part of an organisation’s risk management process, will lessen the likelihood or impact of the incident. Implementing a business continuity plan will counteract disruptions to business activities and ensure their timely and orderly resumption. Business continuity is one of the ways to reduce the consequences if a risk factor or event occurs, while avoiding, transferring or accepting the risk is considered appropriate risk mitigation measures (Engemann & Henderson, 2012:4; Graham & Kaye, 2006:65).

This chapter will describe the current business operating environment and the increasing security challenges facing businesses and organisations around the world. For UN Funds and Programmes working in emergency and post-conflict situations, the complexity of this environment is even greater and more challenging, as they try to deal with these risks while still maintaining their operations. This chapter will also delve deeper into the concepts of risk management, security risk management and business continuity management. While these management functions have been historically treated as separate functions, there is a growing realisation that they should be more closely integrated in order to address the new realities of a complex business environment (Graham & Kaye, 2006:4).

3.2 GLOBAL RISK ENVIRONMENT

The global risk environment is constantly changing and political leaders, business managers as well as the heads of the UN Funds and Programmes need to be constantly aware of these changes and the potential impact they may have on their institutions. The World Economic Forum (2015:7) annually puts together a global risk report which is based on several discussions and workshops to identify events that − if they occur − could have significant consequences for a specific country/region or globally. The 2015 Global Risk Report highlighted five risks, namely:

(1) Conflict among states with regional consequences.

(2) Environmental issues related to climate change and water scarcity.

(3) Economic risks related to unemployment and underemployment.

(4) Cyber security.

(5) The spread of infectious diseases as main risks to watch out for over the next 10 years (World Economic Forum, 2015:13).

In addition to the report produced by the World Economic Forum, the International Crisis Group, which is an independent, non-governmental organisation committed to preventing and resolving deadly conflict, also produces a monthly bulletin on the state of affairs in all the most significant situations of conflict or potential conflict around the world (International Crisis Group, 2015). The February 2015 *CrisisWatch* publication highlights potential and on-going conflict situations in approximately 70 locations globally (International Crisis Group, 2015). In addition to the above, according to the World Bank (2014), one in four people in the world, or about 1.5 billion people, live in fragile and conflict-affected states or in countries with very high levels of criminal violence. Many of these countries and sub-national areas face cycles of repeated violence, weak governance and instability.

The attack on the World Trade Centre in New York on 11 September 2001 not only saw governments pass new laws pertaining to terrorism, but it also resulted in a renewed interest in risk management and business continuity. A review carried out in the United States after the attack concluded that only a few organisations had taken into account the potential for a disaster of the scale and nature that occurred in Manhattan on that day in their business continuity planning (Graham & Kaye, 2006:45). Prior to September 11th, most business continuity plans were based on the assumption that following a disaster, an organisation could function with a small percentage of its staff working from an alternate site and would eventually be able to move back into its offices. As it turned out, this was not the case, and many organisations had to completely reorganise themselves.

The Global Financial Crisis in 2007 and 2008 resulted in regulatory bodies issuing a number of regulations and guidelines to enable business institutions to become more resilient. The Basel Committee on Banking Supervision (2011) set out a number of accords on governance, defining operational risk management and linking it to business continuity. In South Africa, the South African Reserve Bank (2013) specifically refers to the *King Reports* (King Committee on Corporate Governance, 2002), which include several new sections focusing on risk management. The ISO (2009; 2012) published a Risk Management Standard in 2009 and a Business Continuity Standard in 2012.

Based on the above, one can deduce that the external environments in which most organisations operate are becoming increasingly complex and challenging. As discussed in Chapter 2, UN Funds and Programmes work in many of the countries where the situations highlighted in the abovementioned reports exist, delivering humanitarian aid, development and reconstruction activities in support of local governments and impacted communities. Those UN agencies working in fragile states and post-conflict environments not only face strategic and reputational risks, they also have to take into account security risks and the impact these may have on their ability to deliver their respective mandates. These security risks range in severity from petty crime or road traffic accidents to complex terrorist attacks, often specifically targeted at aid workers. Utilising risk management methodologies will increase the resilience of any organisation, especially those that, due to the nature of their mandate, have to operate in highly volatile areas (Posta & Wynes, 2011:5).

One of the earliest attacks recorded on a UN staff member was the killing of Count Folke Bernadotte, who was shot by Israeli extremists in Jerusalem in 1948. Bernadotte was a UN mediator in Palestine and had angered the Jewish underground by recommending that Jerusalem become an international city (Reynolds, 2003). Since then the scope of the work of the UN has expanded, and it is now present in more countries than ever before. With this expanded presence has come even greater exposure to all kinds of risks. In the past there were isolated incidents of violence against the UN, which were mainly the result of being in the wrong place at the wrong time, but over the past few years there have been instances where UN staff have been deliberately targeted (Brahimi, 2008).

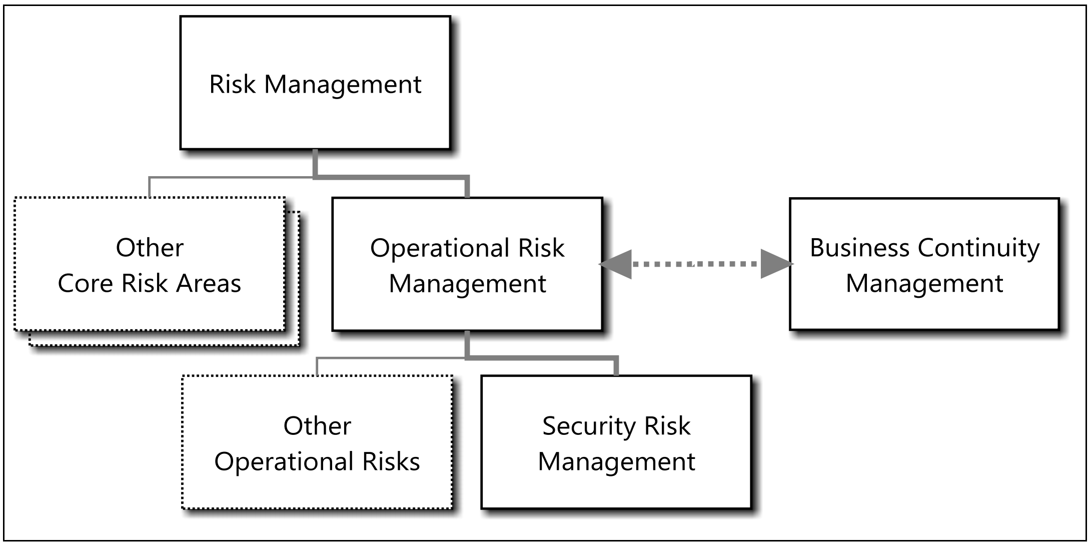
The attack on the UN headquarters in Iraq on 19 August 2003, resulting in the death of 22 UN staff including the Special Representative of the Secretary General and injuring several hundred others, had a profound impact on the UN and its approach to ensuring the safety and security of staff. The UN Secretary-General, Kofi Annan, appointed an independent panel to investigate the circumstances of the attack and to make recommendations as to how the UN could strengthen its security management system (Ahtisaari, 2003:29). The report identified several gaps and weaknesses in the UN security system which needed to be urgently addressed. Among its many recommendations, the panel emphasised the need for professional assessment tools for the collection and analysis of information on potential threats; a robust security management system; accountability at all managerial levels for the implementation of security regulations; a clear chain of command; and clear division of labour and coordination (Ahtisaari, 2003:25-27). One of the major outcomes of this report was the creation of the UNDSS, headed by a senior UN official at the rank of Under-Secretary-General, who would report directly to the UN Secretary General.

The United Nations Security Management System is based on the fundamental principle that the primary responsibility for the safety and security of United Nation’s personnel rests with the host government (Ahtisaari, 2003:3). Governments have the responsibility to maintain law and order in their country and under the charter of the United Nations are also responsible for the security of UN staff and facilities. This, however, does not take away the responsibility or duty of care that each UN agency has for its own staff, especially when working in an environment where the host government's capabilities are limited (Ahtisaari, 2003:3).

As can be seen from the discussion above, organisations face a wide range of threats daily. It is therefore imperative that executives and senior managers take ownership and responsibility for identifying and mitigating the risks that their organisations may encounter. In addition to mitigating the impact of the risks when they do occur, it is also important to consider the disruption that these risks, when realised, may have on business operations. In accordance with Graham and Kaye (2006:39), risk management and business continuity management are two business practices to deal with all types of risk and to ensure that plans are in place to respond to crisis situations. These two functions should also be seen as an integral part of corporate governance (Graham & Kaye, 2006:38).

In Chapter 1 a brief explanation was given of the concepts of risk management, operational risk management, security risk management and business continuity management. These concepts are of relevance because risk management is an important management tool for identifying and assessing risks and developing commensurate security measures to mitigate the impact of these risks (Engemann and Henderson 2012:34). In addition, business continuity management is necessary to identify critical business processes and identify recovery procedures in the event that a risk materialises and disrupts business operations (Engemann & Henderson, 2012:4). Risk management in the context of this study can be seen as being overarching, while operational risk management focuses on those risks arising from the execution of an organisation's business functions. Security risk management is considered as a sub-set under operational risks and it deals specifically with security risks such as terrorism, political unrest, civil unrest, crime and hazards. Business continuity management is also part of operational risk management as it assists in the continuity of business operations (Storkey 2011:8). Schematically the hierarchy and relationship between risk management, operational risk management, security risk management and business continuity management can be outlined as shown in Figure 1.

Figure 1: Risk management and business continuity management interface



(Adapted from Engemann & Henderson, 2012:4-34 and Storkey 2011:8)

3.3 RISK MANAGEMENT

As highlighted in the section above, all organisations are confronted with internal and external factors that can affect whether they will achieve their objectives. The effect of this uncertainty is categorised as "risk" (ISO, 2009:v). Organisations overcome this uncertainty by adopting a risk management methodology which includes identifying risks, analysing them and then determining whether and how the risk should be treated in order to satisfy their risk criteria. According to Haimes (2009:24), risk management attempts to answer the following questions:

- What can go wrong?
- What is the likelihood that it would go wrong?
- What will the consequences or impact be, if it did go wrong?

ISO (2009:1) defines risk as "the effect of uncertainty on objectives". A closer look at the definition shows that there is a focus on the organisation's objectives and it puts risk in a specific context pertaining to what the organisation wants to achieve. The objectives can be at various levels, for example the strategic, operational or tactical level. Objectives also refer to different areas that would be impacted if the risk materialises, such as strategic, reputational, legal, financial, market, procurement and human resources. Risks are not confined to the private sector or to a specific subject matter such as financial risks. Risk management has been around for decades and applies to individuals, projects and institutions (Graham & Kaye, 2006:1-4).

Past definitions of risk, such as the one found in Fay's security dictionary (2000:215) defines risk as the "loss potential that can be estimated by an analysis of threat and vulnerability". This definition focuses on the threat or a specific event rather than the impact or consequences that the event may have on an organisation in achieving its objectives. For example, it is not about an event, such as a crime being committed, but rather on the impact that the crime will have on the organisation in achieving its objectives.

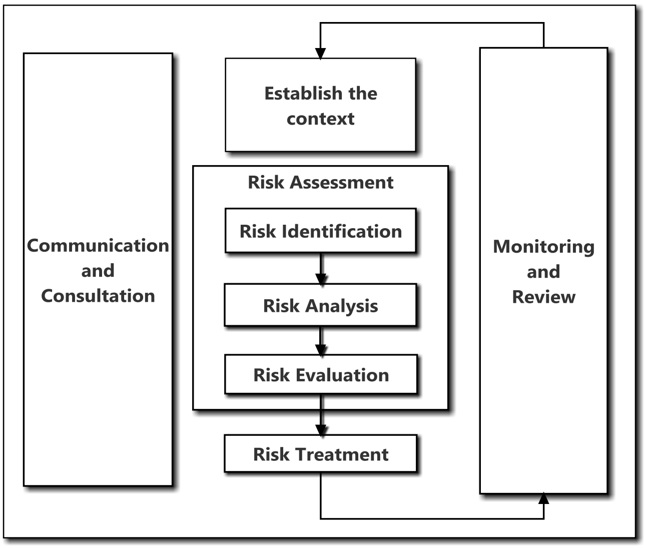
The term "uncertainty" in the definition relates to the internal and external environmental factors in which organisations operate. As explained above, the operating environments in which organisations function will vary and each situation poses its own challenges that need to be considered. For example, the environment in Somalia where UN Funds and Programmes are working is very different if compared to the working environment in South Africa, where the situation is more stable. In Somalia for example, UN Funds and Programmes need to take into account the lack of a stable government, the presence of different militant armed groups and the possibility that their staff and operations may be attacked, while the probability of similar incidents taking place in South Africa is more unlikely.

3.3.1 Risk management process

Fay (2000:215) defines risk management as a business function which includes loss prevention, loss control and loss indemnification. ISO (2009:2) describes risk management as a set of coordinated activities which are used to direct and control an organisation with regard to the risks they need to deal with. The commonality between the two definitions is the management aspect of dealing with risks. In accordance with Smit, Cronje, Brevis and Vrba, (2007:8-9), management can be regarded as the process of planning, organising, leading and controlling to achieve identified goals. When combining the two definitions (management and risk management) one can deduce that risk management includes: applying the functions of management (planning, organising, leading and controlling); identifying the risks an organisation is exposed to; allocating the necessary resources to manage the risks; ensuring that roles and responsibilities are clearly defined; and putting in place appropriate control measures to ensure that the risk management programme achieves its goals to minimise risks to the organisation. It can be further deduced that risk management is not static and needs to be dynamic to keep abreast of evolving threats, which is the reason why it should be looked at as a process and not just an activity.

In order to answer the three questions posed by Haimes (2009:24), namely: (1) what can go wrong; (2) what is the likelihood that it will go wrong; and (3) what will the consequences be if something does go wrong, one needs a process or methodology. The ISO Standard describes a process for managing risks, which is shown in Figure 2 below (ISO, 2009:14). The process has been designed to be used by any industry and to assess any kind of risk at any level. However, since there are many types of risks that organisations face, the identification and analysis of these risks cannot be done through a single generic process. The process for dealing with specific risks should be tailored to the specific risk area. While the process can be adjusted, the purpose of using this model ensures standardisation across an organisation, which is very important. For example, when compared to the Security Risk Management Model which has been adopted by the UN, outlined in Figure 4, it is clear that even though the steps are very similar, the factors being considered are tailored to be applicable to the UN.

Figure 2: Risk management process



(ISO 2009:14)

The risk management process as depicted above includes five main steps (ISO 2009:14). Firstly, the context within which the risk assessment process is being carried needs to be established. This is very similar to the internal and external analysis carried out during the strategic planning process, and includes looking outside and inside the organisation to identify possible trends that may have an impact on the organisation. At this time it is also important to review the organisation’s risk management policies and governance structure to identify any deficiencies. By reaffirming the context, the planner establishes the external and internal boundaries to be taken into account when managing risk, as well as the scope and risk criteria for the remaining steps. During the second step the risks that may affect the goals and objectives of the organisation are identified, as well as the potential impact if the risk materialises. The purpose of this step is to develop a complete list of risks that may prevent the achievement of objectives (ISO 2009:15-16).

Thirdly, each risk is analysed in more detail to develop a thorough understanding of the risk. It is important to look at the likelihood of the risk occurring and under what circumstances it may occur, as well as the potential consequences for the organisation (ISO 2009:16). This step is important because the information will be used to determine appropriate mitigation measures. In the fourth step, individual risks are evaluated to determine which risks need attention and to determine the priority in which mitigation measures will be implemented to reduce the overall risk to an acceptable level (ISO 2009:17). Typically, the options for treating risks include: (1) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; (2) accepting the risk through an educated decision; (3) transferring or sharing the risk with another party; and (4) reducing the severity of the loss or the likelihood of the loss from occurring (Engemann & Henderson, 2012:306).

The last and fifth step focuses on developing appropriate mitigation measures for each risk (ISO 2009:18-19). Risks are normally treated by implementing measures that can change either the likelihood of the risk taking place or reducing the magnitude of the impact, should the risk indeed take place. This involves selecting one or more options and implementing them. Each option must be subjected to a cost benefit analysis to determine which one is the most appropriate for the organisation to carry out. Broder and Tucker, (2012:29-30) explain that the purpose of the cost benefit analysis is to show that the effectiveness of a security measure will outweigh the acquisition and instalment cost of the item. As a general rule the optimum reduction of risk is at the point where the benefits to be gained outweigh the investment cost. Calculating cost/benefit of security measures when dealing with some risks such as terrorist acts is often very difficult because of the challenge to quantify potential damages. It is also important to continuously monitor and review the different steps in the process to ensure that nothing is overlooked and to make revisions as new risks appear (ISO 2009:18-19).

According to ISO (2012:8), risk appetite is the amount and type of risk that an organisation is prepared to accept before action is necessary to reduce it to an acceptable level. For example, a South African company could decide that it will not operate or have an office in a certain area of a city or province due to the high crime rates, whereas UN Funds and Programmes have decided that they have to try and operate wherever they are needed in spite of potential security risks. The decision is based on the criticality of their specific programme and an assessment of the security threats associated with working in a specific location, and then proposing options for mitigating the risk to a level which is acceptable to the management of the organisation.

According to Williams (2011:1-2), all risks are tied to the strategic objectives of an organisation, and risk management should be linked to the creation of strategies, operational priorities and tactical plans. Risk management is most successful when it becomes fully integrated into normal operating procedures, processes and systems. Risk management should be a continuous process. The ISO risk management process is well suited to be adapted to thematic risk areas that any organisation faces daily.

Throughout the discussion in this section the definitions of risk and the risk management process were referred to in a generic context and include any risk that an organisation may be exposed to. However, as indicated in Chapter 1, this study focuses on security risk management and is limited to a subset of risks referred to as security risks. Security risks include those threats that originate from armed conflict, terrorism, crime, civil unrest and natural disasters and their impact on UN Funds and Programmes' ability to achieve their objectives while operating in emergency and hazardous situations. However, even though the focus is on security risks, general risk management methodology and principles as described, still apply.

3.4 OPERATIONAL RISK

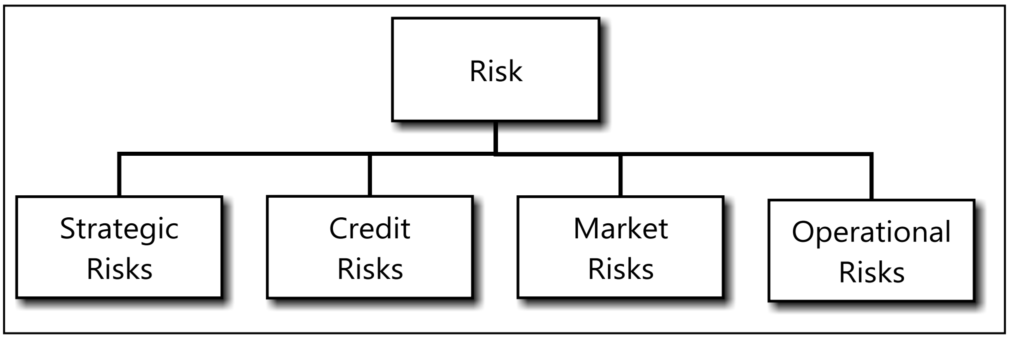
As previously noted businesses and organisations have to address various kinds of risk and they need to analyse them from different perspectives in order to develop a complete picture of the risks that their institution faces. Traditionally financial institutions have categorised risk at the enterprise level into three main areas: strategic, credit and market risks (Hong Kong Institute of Bankers, 2013:4). Other risks such as security, information technology, and legal and procurement risks also existed, but were treated independently and were never grouped under an overarching risk practice area. Since these individual risks were not clearly visible, senior management did not have a comprehensive picture of the risks their organisation was exposed to (Hong Kong Institute of Bankers, 2013:22).

In order to overcome this, the Basel Committee on Banking Supervision (2011), in the late 1990s, decided to create another risk category at the enterprise level for financial institutions, called operational risk management (Hong Kong Institute of Bankers, 2013:4). By creating this new category of risk, the Basel Committee and the Bank for International

Settlements consolidated all the risks that focus on mitigating vulnerabilities in operational business processes under one heading and placed it alongside the other main risk practice areas at the institutional level. Previously they were not integrated but rather fragmented to deal with a variety of risks. The organisational risk map was expanded as can be seen in Figure 3 below:

- Strategic risks. These risks are tied to changes in the political and regulatory environment.
- Credit risks. These risks are caused by a counterpart's inability to repay their debt.
- Market risks. These risks are related to fluctuations in the market value of different financial instruments.
- Operational risks. Operational risk arises from an organisation's operations and also from a disruption in its operational processes. It enables managers to create a detailed risk profile across their organisation in order to run it better (Hong Kong Institute of Bankers, 2013:4).

Figure 3: Generic organisational risk map



(Adapted from the Hong Kong Institute of Bankers, 2013:4)

As described in Chapter 1, operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel Committee on Banking Supervision, 2011:3). According to the Hong Kong Institute of Bankers (2013:5-7), the sources for operational risks can be traced back to a wide range of events including political issues, legislative issues, criminal acts, employment practices, workplace safety, system factors, damage to assets caused by natural and man-made hazards and terrorism. Included among the threats are those that also fall under the category of security risks. By grouping them all together under the umbrella of operational risk, it ensures that the risks tied to processes, people, systems and external factors are considered in an integrated manner. For example, a threat may originate from an external event such as an earthquake, but the impact may be on the organisation's systems, facilities and staff. It is clear that there are four underlying factors or causes for operational risk: (1) processes; (2) people; (3) systems; and (4) external factors (Hong Kong Institute of Bankers, 2013:6).

Process factors are related to risks associated with business processes that are performed by an organisation and could include, for example, data entry errors or insufficient policies and procedures (Hong Kong Institute of Bankers, 2013:6-7). The second factor relates to employees or people who provide services to an organisation, and whether deliberately or otherwise, there is fraud, high staff turnover especially in areas where critical processes are performed, and breaches in procedures (Hong Kong Institute of Bankers, 2013:7). The third causal factor is related to the systems that are employed by an organisation. Information technology systems such as hardware and software are extremely vulnerable to risks such as cyber attacks. The last factor includes risks external to the organisation such as crime, man-made or natural disasters, other security risks, and different political and legislative issues impacting the organisation (Hong Kong Institute of Bankers, 2013:7).

In addition to identifying the above four causal factors for operational risks, the consequences or results when these risks occur can be broken down into seven types of loss events (Hong Kong Institute of Bankers, (2013:72). The majority of security risks which typically occur from outside the organisation can be categorised under the heading "damage to physical assets" as shown in the list below. It is also important to note that while an event can originate from within one category, the impact can be found across multiple categories. According to the Hong Kong Institute of Bankers (2013:72), the seven types of loss events are:

- Internal fraud. Acts committed by employees with the intention to defraud, misappropriate assets, or circumvent regulations and policies resulting in losses to the institution.
- External fraud. Acts by third parties to harm an organisation through various fraudulent activities.
- Employment practices and workplace safety. Losses resulting from acts related to employment practices, workplace safety, workers compensation, and health.
- Clients, products, and business practice. In this category the losses can be contributed to market manipulation, improper trade activities, and product defects.

- Damage to physical assets. This category is directly relevant to this study and security risks are included under this heading. Assets in this case include all company assets, including personnel.
- Business disruption and systems failures. This event type includes losses arising from business or system failures.
- Execution, delivery, and process management. The last category includes losses that are incurred as a result of data entry errors, accounting errors, and reporting errors.

Since the origin of the category “operational risk” lies in the financial sector, the question may be asked why it is important to include reference to operational risk in this study, which mainly focuses on security risk management and business continuity management within UN Funds and Programmes. The researcher is of the opinion that non-financial organisations, including the UN agencies, can benefit from the work financial institutions have done since operational risks are present in all organisations but especially with regard to:

(1) Providing the opportunity to group risks, like security and information technology that would otherwise stand alone, into one governance framework. Standing alone, these individual risks may not receive the necessary attention, but by consolidating them under one heading (operational risk management), and elevating them to the institutional level alongside other core risk practice areas, will ensure that the institution has a comprehensive picture of all the risks it faces.

(2) Providing a home for security risk management and associated security threats such as civil unrest, abductions and terrorist act, since the definition for operational risks makes provision for damage or loss caused by external events.

(3) Linking operational risk management with business continuity management. As mentioned above, the causal factors for operational risks are tied to the actions of people, internal systems, technology failures, failed internal procedures and the impact from external events. A failure in one or more of these factors can lead to the disruption of business processes and ultimately the ability of an organisation to deliver its services. In this regard there is a direct link with business continuity management, which is aimed at restoring disrupted business operations in a timely manner, and operational risk management, including security risk management.

There is also a natural link between the causes of operational risks and the impact this may have on business operations. Risks that originate from any one of the four causal factors (processes, people, systems and external risks) have the ability to disrupt business processes. For example, a power outage caused by a bomb blast may affect the information technology systems. The lack of access to these systems in turn will result in the disruption of business operations. It is within this context that business continuity management can be beneficial because it can mitigate the impact of operational risks on business operations if and when they materialise. Similarly, such impact on personnel, information technology, equipment and other assets can also be caused by security risks. If the impact from these incidents exceeds the mitigation measures in place, it can have a follow-on effect by disrupting business operations. Taking all of these factors into consideration is critical from a security risk and business continuity point of view.

The responsibility for understanding and managing risks to an organisation lies with management of the organisation. In order to do it effectively, risks need to be categorised into a framework, and it is up to each organisation based on the nature of their core business and external risk environment, to design an appropriate risk taxonomy (Graham & Kaye, 2006:8). Very little evidence could be found that the use of the term "operational risk management" has expanded beyond the financial sector. Based upon the researcher's own experience and observation while working in the UN system, the concept of operational risk management has not yet been adopted by UN Funds and Programmes. It is, however, recommended that these UN agencies consider adopting it in their risk taxonomy as it consolidates various risk areas which are currently siloed under one heading. As mentioned above, operational risk management is also naturally linked to business continuity management as a response mechanism when operational risks materialise and disrupt business operations. It is therefore proposed that UN agencies learn from the work done in this field by financial institutions and consider following their example by creating an operational risk category as a sub-set of main risks at the institutional level consolidating operational risks under one heading.

3.5 SECURITY RISK MANAGEMENT WITHIN THE UNITED NATIONS

According to Terzi and Posta (2010:2), no organisation (including the United Nations) operates in a risk-free environment. In many cases UN agencies work in locations that are highly volatile and risky. In his 2013 report to the UN General Assembly, the UN Secretary-General summarised the environment under which UN staff are working, as follows:

> *United Nations personnel serve in an increasingly dangerous environment and encounter a variety of threats not previously encountered in the history of the Organization. The current asymmetric nature of warfare, seen in suicide bombings, the use of improvised explosive devices and random mass shootings, has a direct impact on the personnel and on the operations of the*

> *United Nations. Direct attacks against the United Nations are a distressing phenomenon that has developed over the past decade and those attacks are becoming more intense and more sophisticated. The most recent examples were the extremist attacks against the United Nations in Somalia and against the International Organization for Migration, which is a member of the United Nations security management system. The almost two-fold increase in the abduction of United Nations and humanitarian personnel in just the past six months is also a new and alarming trend* (UN Secretary-General, 2013:15-16).

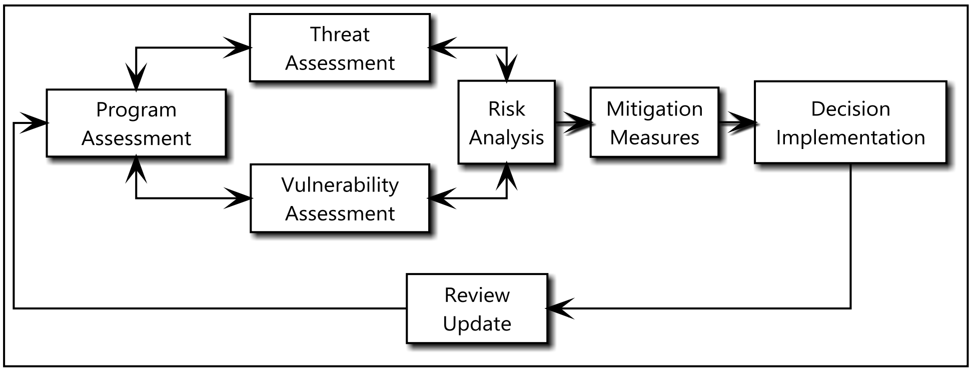
As previously described, a risk is an event, the occurrence of which has the potential to influence the achievement of an organisation's objectives. Risk is normally measured in terms of impact and likelihood. Risk management is not an end in itself, but a means to an end, which is to enable an organisation to have the resilience to withstand a risk and still be able to achieve its goals (Engemann & Henderson, 2012:34). This study focuses on security risks which typically originate from criminal acts, armed conflict, civil unrest, terrorism and natural hazards, which are the type of risks UN staff are exposed to. Security risks can also be considered a sub-set of operational risks when they originate from outside (external) the organisation. The direct impact on an organisation when security risks occur could result in death or injury to staff, damage or destruction to property or other company assets and systems. The follow-on consequences if these risks are not appropriately mitigated, could also lead to the disruption of business operations and even the temporary or permanent shut-down of operations.

As previously mentioned in Chapter 1, organisations are normally able to deal with routine incidents, but they need to develop the capacity through a security risk management plan to respond to potentially disruptive events that may seriously impact business operations. The security risk management plan should, therefore, provide guidance on the implementation of solutions in the form of specific mitigation strategies and measures, with the aim of lowering the risk levels of the organisation by reducing the impact and likelihood of an undesirable event. If this can be achieved, then it should also limit the disruption to the business operations of the organisation.

3.5.1 UN Security Risk Management Model

In order to assess security risks to UN agencies, the UNDSS developed a Security Risk Management Model which is currently used by all UN agencies (UNDSS, 2009:1). The Security Risk Management Model utilised by the UN is outlined in Figure 4 below. It is used to assess the context and operating environment in which UN operations are carried out and to identify the risks associated with working in this particular location to personnel, assets and operations. This analysis of the identified risks helps to determine specific mitigation strategies and measures with the aim of lowering the risk levels to the UN by reducing the impact and likelihood for each risk. Within this context, UNDSS (2009:1) defines a threat as any factor which has the potential to cause harm, loss or damage to the UN, including its personnel, assets and operations. A risk is defined as the combination of the impact and likelihood for harm, loss or damage to the UN from the exposure to threats. In this context, the UN views crime, political instability, civil unrest, terrorism and natural hazards as possible sources for risks.

Figure 4: UN Security Risk Management Model



(UNDSS, 2009:2)

The UN Security Risk Management Model is very similar to the ISO risk management model described in Figure 1, but it has been tailored to meet the needs of the UN (UNDSS, 2009:2). The process starts with a programme assessment, which includes a contextual analysis of the organisation's goals and objectives and identifies which components of the programme may require security support. The threat and vulnerability assessments provide the required information to discover vulnerabilities and identify potential threats to the UN. The sum of the programme, threat and vulnerability assessments provides the context for the operational environment in which the organisation needs to operate. The threats are then analysed in detail. The next step is to carry out a risk analysis which takes into account the probability of a threat from occurring and the impact or consequences on the organisation if the threat materialises. The results are displayed on a risk matrix. This information is then used to develop appropriate risk mitigation measures. Mitigation measures may include: (1) accepting the risk without the need for any further mitigating measures; (2) controlling the risk by implementing preventative and/or mitigating measures to reduce the risk to an acceptable level; (3) avoiding the risk by temporarily distancing the potential target, like for example UN staff from the risk; and (4) transferring the risk by sub-contracting the implementation to other parties who can operate more safely in the hazardous environment (UNDSS, 2009:2).

At this point different options to mitigate the identified risk are presented to heads of the UN agencies in the country for their approval. In addition to considering the appropriateness of each mitigation measure in relation to the risk, the costs associated with each measure are also taken into account. In some cases the costs to reduce a risk to an acceptable level may be prohibitively expensive and may exceed the organisation’s security budget. In this case it means that the risk cannot be adequately controlled, and a decision is then made to either avoid the risk or transfer responsibility to another entity to manage it. After a decision has been made by the heads of the individual UN agencies, the measures are implemented and the situation is monitored and reviewed regularly to address any changes in the environment (UNDSS, 2009:2).

The following illustration, which is based on the researcher’s own experience and observation while working in the UN system, describes how the UN’s security risk assessment process works. After the Comprehensive Peace Agreement signed between Sudan and South Sudan in 2005 (Council on Foreign Relations, 2005), one of the UN agencies planned to deliver humanitarian supplies by truck to isolated areas in South Sudan. The route that these convoys had to take required them to travel through remote areas which could have contained landmines left over from the 20-year civil war. Travelling on these roads without them being cleared of landmines and other explosive devices could have hampered the delivery of supplies and could also have led to the death or injury of the drivers as well as cause damage to their vehicles and destruction of the cargo. Ultimately it could have impacted the organisation’s general ability to deliver humanitarian supplies to needy villagers in future. In this instance the UN agency had to assess the situation by utilising the Security Risk Management Model (Figure 4 above). Relevant project and security staff of the UN agency would then have explored all the potential options to mitigate the immanent risk. They would have then presented different options to management in order to address these risks while also achieving the organisation’s objectives, for example:

- <u>Option 1</u>: The risk was considered too high to accept without trying to mitigate it. They considered delivering the humanitarian supplies by helicopter or plane. Another option was to have the road cleared of landmines prior to delivering the supplies by road, or purchasing trucks with a protective cabin to at least protect the driver in the event of a mine incident. These options would have reduced both the risk to the UN agency's staff and increased the likelihood that the humanitarian supplies would be safely delivered.

- Option 2: The organisation could transfer the risk to a third party by sub-contracting the activity to another vendor who would assume the risk to deliver the supplies on behalf of the UN agency. In this case, the UN agency would eliminate the risk to its staff, but would not necessarily achieve its objectives of delivering the humanitarian supplies safely unless they ensured that the contractor was taking the necessary precautions. Under this particular option, the expense of sub-contracting this potentially hazardous activity could have been prohibitively costly due to the extra insurance costs that the contractor would have required to accept the contract.
- Option 3: Avoiding the risk was also not considered an option because the humanitarian situation in South Sudan after the cessation of the civil war was the exact reason why the UN agency was involved in this particular operation.

Each option needed to be developed in sufficient detail, including estimated costs, in order to allow managers to select the one that would be most cost-effective. Managers had to compare the advantages and disadvantages of the different options before a final decision could be made. In similar cases, eliminating or seriously reducing the risk may not have been feasible because of prohibitive costs.

This example focuses on security risk management and shows how the model would have been applied in this particular situation to identify and assess the risk and develop appropriate risk mitigation strategies. It also highlights the impact of security risks on achieving business objectives which go beyond the realm of security risk management and are better dealt with through business continuity management.

As previously discussed, it is proposed in this study that security risk management and business continuity management should be integrated in order to address risks that are security related in nature, but will also have an impact on continuing business operations. The business continuity management concepts and processes are explained in more detail below.

3.6 BUSINESS CONTINUITY MANAGEMENT

Since organisations are exposed to a number of risks, they need to take proactive measures to prepare for potential incidents and disruptions to business processes. If they do not have a proper plan in place to effectively respond, the disruption in operations could result in significant financial loss, physical damage to facilities or even loss of life (ASIS International, 2009:18).

Business continuity planning is the process that organisations use to identify their critical business functions in order to assist them in developing procedures to restore and continue these functions following a disruption. It also helps to ensure the safety and security of employees and assists in timely and orderly recovery after these events (Broder & Tucker, 2012:223-225).

As mentioned previously, the origin of business continuity management is in disaster recovery planning, which focuses on recovering information technology systems, including telecommunications and data centres. It has expanded to include the recovery or continuity of business unit operations (Graham & Kaye, 2006:11). ISO (2012) describes business continuity as the ability of the organisation to continue delivery of its services at predefined levels following a disruptive incident. There must be an acceptance that while business operations are being recovered, business activities may have to be performed at a lower level than under normal circumstances. For example, normally communications may be sent by email, but following a disruption of the information technology system or access to a power source, these may have to be sent via express mail or by overnight delivery services, which may cause a delay in the arrival of the message.

3.6.1 Business continuity process

Similar to risk management, business continuity plans are typically developed through a series of integrated steps (Engemann & Henderson, 2012:7-10). These steps, which are described in detail below, include: the initiation of the process; carrying out a business impact analysis as well as risk assessment; development of recovery strategies; followed by implementing and maintaining the plan.

3.6.1.1 Programme initiation

The process starts by establishing the context within which the business continuity plan will be developed. This takes into account the organisation's strategic objectives, its risk appetite, and any regulatory, contractual and stakeholder obligations (Engemann & Henderson, 2012:8). It is important to link business continuity with the organisation's goals and objectives, otherwise the plan might focus on recovering business processes that are not critical to achieving the mission of the organisation, thus investing resources in nonessential activities. Since the risk management process (as explained in Figure 2) also starts by establishing the context within which the risk assessment is carried out, it is not necessary to duplicate this step for both processes. In this instance information collected from setting the scene could be utilised for both risk assessment and business impact analysis.

3.6.1.2 Business impact analysis

The second step involves conducting a business impact analysis (Graham & Kaye, 2006:109-146). The business impact analysis is the foundation on which business continuity rests. The business impact analysis determines the importance of the business operations by assessing the impact on operations over time in the event that they are disrupted. This process helps to rank business processes in order of priority based on the need to resume the process. The purpose is to identify processes that are critical to achieving the primary objectives of the organisation. The criticality assessment is done by determining the impact that downtime will have on each process. Organisations typically use a rating scale describing the loss or damage that may be caused in the event that a process is not recovered within a specific timeframe. The purpose of this scale is to assist in prioritising the urgency of order in which disrupted processes need to be recovered (Graham & Kaye, 2006:101).

A business impact analysis is therefore used to prioritise among all the business processes performed by an organisation in order to identify in which order processes will need to be recovered. Business processes are dissected in detail to identify all the resources involved such as the staff responsible for performing the individual activities in the process, IT systems, office locations, other inputs and outputs, key documents and other information required to perform the process. This information is used to develop recovery procedures or ways to work around the disruptions.

Although not part of the business continuity management process, a risk assessment should also be carried out and the output from the risk assessment should be considered in the business impact analysis. This is important because through the risk assessment, risks that may cause a disruption in business operations are identified (Engemann & Henderson, 2012:8). The impact of these risks should be mitigated through strategies developed during the risk management process, and strategies for continuing business operations should be identified as part of the business continuity process.

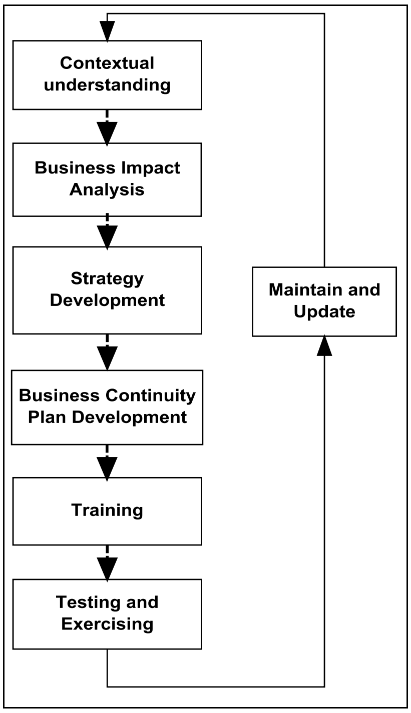
3.6.1.3 Strategy development

The third step in the process is to develop strategies to meet the response, continuity and recovery objectives for each process. These continuity strategies focus on the organisation’s capacity to respond to events in order to continue business operations (Engemann & Henderson, 2012:60). Instead of developing a contingency plan for each possible event, planners typically narrow their planning down to three main scenarios: unavailability of the location where the processes are performed; unavailability of the IT infrastructure to perform the processes; and unavailability of the required staff to perform the processes. Identified strategies are selected by assessing their effectiveness, costs to implement, and time to implement in the event of a crisis (Engemann & Henderson, 2012:60). Specific strategies could include: identifying remote locations where work can be conducted from; installing backup equipment such as electricity generators in the event of power disruptions; distributing tasks to be performed in other locations away from the main office; optimising the work hours of staff; identifying multiple suppliers in the event that one supplier cannot deliver the required services; and developing systems to allow staff to work from home (Engemann & Henderson, 2012:63-65). The result of this step is the development of a comprehensive business continuity plan that documents the continuity and recovery procedures for crisis events.

3.6.1.4 Maintenance

The last step in the process involves creating an awareness of business continuity, on-going testing of the plan and updating it where required (Graham & Kaye, 2006:87). Risk management is seen as being part of the process, since it should provide input into the business impact analysis process by identifying what can go wrong, what measures are currently in place, what is the exposure to the organisation and identifying new or enhanced measures to reduce the risk. Not all risks require the activation of a business continuity plan, since the plan should only be activated when the impact of the identified risks is critical for business operations. It would, however, be negligent for business continuity units to only adopt a pure reactionary approach and wait for risks to affect business operations (Graham & Kaye, 2006:326-327). The maintenance phase includes training and regular testing of the plan (Engemann & Henderson, 2012:8). Schematically the business continuity management development process described by Engemann and Henderson (2012:8) is shown in Figure 5 below:

Figure 5: Business continuity management development process



(Adapted from Engemann and Henderson, 2012:8)

3.7 RELATIONSHIP BETWEEN SECURITY RISK MANAGEMENT AND BUSINESS CONTINUITY MANAGEMENT

Exploring the relationship between security risk management and business continuity is at the core of this study. Graham and Kaye (2006:89) say that risk management and business continuity management are complementary functions and that both should be implemented. Graham and Kaye (2006:11) also remark that business continuity management mainly remains in the domain of information technology or facilities functions, rather than being imbedded as part of a risk management framework. Engemann and Henderson (2012:4) propose that implementing both risk management and business continuity management in an integrated manner is sound and useful. The linkages, integration and delineation of roles and responsibilities among the different players potentially involved, are however unclear. A need therefore exists to align the risk management and business continuity processes.

Alignment of the processes should start with the risk assessment process whereby risks that could affect the institution and its ability to carry out its operations are identified. Business continuity management should consider security risks and corresponding mitigating measures to address the risks, in particular those that will require business process recovery. Lastly, both disciplines, namely security risk management and business continuity management, should be involved in managing crisis events when risks do materialise (Engemann & Henderson, 2012:9).

Security risk management focuses on the likelihood of an adverse event occurring and the steps required to mitigate its impact, while business continuity management focuses on what needs to be done if an adverse event occurs (Engemann & Henderson, 2012:4). Business continuity management is therefore less concerned with the cause of the disruption, but more with what needs to be done to maintain an organisation's activities (Engemann & Henderson, 2012:4). Risk management can therefore be seen as being preventative, while business continuity focuses more on the impact on business operations.

Table 1 below depicts a comparison displaying the key focal differences between security risk management and business continuity management (Engemann & Henderson, 2012:21-31; Graham & Kaye, 2006: 89):

Table 1: Comparison: security risk management and business continuity management

Item	**Security risk management**	**Business continuity management**
Methodology	Risk assessment.	Business impact analysis.
Key parameters	Impact and probability.	Impact on business processes.
Type of incident	Security risks.	All events that may cause a significant business disruption, including security risks.
Size of event	Any security risk affecting the people, resources and other assets of the organisation.	Only those events threatening the availability of the organisation's core processes.
Response	Incident response focused on life and safety of staff and other protection of other assets.	Response is focused on recovering disrupted business processes after the emergency response activities have been dealt with.

According to Graham and Kaye (2006: 89), there is closer alignment of risk management and business continuity management functions, and it is clear from the above comparison that there are areas where security risk management overlaps with business continuity management. One such area is the type of incidents that may cause a business disruption. The residual risk from security incidents may also lead to business disruptions. A correlation can be noted between business impact analysis and risk assessment (Engemann & Henderson, 2012:9). While conducting the business impact analysis, the security risks associated with personnel, facilities, equipment, suppliers and technology need to be considered and appropriate mitigation measures put in place. The opposite is also true. The business impact analysis may reveal locations where critical processes are performed that are considered low risk from a security point of view, but due to the high importance of these locations for the functioning of the business, the security risk analysis may have to reconsider the assessment of these locations (Engemann & Henderson, 2012:62).

A typical example would be where organisations move some back office operations, such as accounting or human resources, to another location away from the company headquarters. The security risks in this other location may be low, but the business impact analysis may reveal that critical processes are performed at this location. Due to the criticality of the work being carried out in this office, security measures may have to be strengthened to protect the staff and premises. While the security risk assessment and business impact analysis are performed separately, the results of the security risk assessment and business impact analysis should be shared. The importance of the worksite within the whole organisation will be identified through the business impact analysis, and this information needs to be considered during the security risk assessment to ensure that it is taken into account when mitigation measures are considered. This may lead to a re-analysis, and where required, adjustments should be made in both the business continuity and security risk management plans (Engemann & Henderson, 2012:62-63).

Another area where security risk management links with business continuity management is when incidents do occur. Depending on the nature and the scope of the incident, management may decide to activate contingency plans. At this time staff members involved in security risk response management and business continuity response management come together to coordinate their response to the reported incident (Engemann & Henderson, 2012:97-108).

This study proposes that UN Funds and Programmes working in high risk environments should apply both methodologies in an integrated manner to deliver their programmes. This will not only increase their chances of success, but will also ensure that they meet their duty of care towards their personnel. Other organisations, irrespective of nature or size, can also benefit from this approach because it is a key contributor to effective corporate governance.

3.8 CONCLUSION

From the discussion in this chapter it is evident that UN Funds and Programmes often work in high risk environments where the safety of their staff and premises is threatened and where their business operations can easily be disrupted. Unfortunately this work environment is becoming increasingly treacherous. This chapter also described the concept of risk management and gave a brief overview of operational risk management, which also includes security risk management. The chapter then explained the security risk management process currently being followed by UN Funds and Programmes and gave an example of how this process is implemented. The role of business continuity management was also explored as well as its inter-relationship with security risk management.

Developing an integrated framework will improve the management of operational and security risk and will assist in the establishment of processes and procedures relevant to strengthening continuity and recovery of critical business processes. By linking business continuity management and security risk management, organisations will be able to develop a clear picture of the risks from a security point of view and plan accordingly. In the next chapter, the data collected through the interviews with representatives of the different UN Funds and Programmes will be analysed to determine how these organisations are currently addressing security risk management and business continuity management.

CHAPTER 4

FINDINGS: AN ANALYSIS AND INTERPRETATION OF THE RESEARCH DATA

4.1 INTRODUCTION

Chapter 1 outlined the rationale for conducting this study. Chapter 2 explained the design and methodology that were used to carry out the research, and Chapter 3 provided an analysis of relevant literature on security risk and business continuity management. In this chapter the findings from the interviews with representatives from participating UN Funds and Programmes will be presented.

The data collected will provide insight into how UN Funds and Programmes are implementing security risk management and business continuity management programmes, which is key to achieving the goal of this study. Furthermore the collected data will assist in answering specific research questions by: (1) providing a more detailed description of how these two management functions are integrated within the agencies that have implemented both methodologies; (2) expanding on the security risks each organisation faces; and (3) explaining why there is a need to enhance the overall resilience of these organisations to continue working in evolving risk environments.

4.2 PARTICIPANTS' INFORMATION

According to Yin (2011:133-135), interviews involve the interaction between the interviewer and a participant with the objective of enabling the researcher to understand the participant's world. The unit of analysis for this study was the UN and the research focused specifically on collecting data from UN Funds and Programmes, being a subset of organisations within the UN family of agencies. Twelve UN Funds and Programmes were invited to participate in the research and interviews were conducted with representatives from these agencies who are involved in security risk and business continuity management. The mandate of each agency is described below.

UNICEF is headquartered in New York City and provides long-term humanitarian and development assistance to children and mothers in developing countries. Most of UNICEF's work is in the field, with staff in over 190 countries and territories. Seven regional offices provide technical assistance to country offices as needed (United Nations, 2004:42).

UNRWA was established following the 1948 Arab-Israeli conflict to carry out direct relief and works programmes for Palestine refugees. The agency began operations on 1 May 1950. In the absence of a solution to the Palestine refugee problem, the General Assembly has repeatedly renewed UNRWA's mandate, most recently extending it until 30 June 2017. UNRWA's headquarters are interspersed between the Gaza Strip and Amman, Jordan, and its operations are organised into five geographic areas, including Jordan, Syria, Lebanon, West Bank and Gaza (United Nations, 2004:43).

UNHCR is mandated to protect and support refugees and this agency assists in their voluntary repatriation, local integration or resettlement to a third country. Its headquarters are in Geneva, Switzerland and it has more than 8 600 staff working in 126 countries through a series of regional offices, branch offices, sub-offices and field offices (United Nations, 2004:41).

WFP is the food assistance branch of the UN and the world's largest humanitarian organisation addressing hunger and promoting food security. From its headquarters in Rome and more than 80 country offices around the world, WFP focuses on food assistance for the poorest and most vulnerable (United Nations, 2004:42).

ITC’s mission is to foster sustainable economic development and contribute to achieving the Millennium Development Goals (MDGs) in developing countries and countries with economies in transition through trade and international business development. ITC is headquartered in Geneva, Switzerland (United Nations, 2004:37).

UNCTAD was established in 1964 as a permanent intergovernmental body. UNCTAD is the principal organ of the United Nations General Assembly dealing with trade, investment, and development issues. The conference ordinarily meets once in four years and the permanent secretariat is based in Geneva, Switzerland (United Nations, 2004:36).

UNDP is the UN’s global development network. Headquartered in New York, UNDP’s programmes focus on four main areas: poverty reduction and achievement of the MDGs; governance; crisis prevention and recovery; environment and energy for sustainable development. The organisation has country offices in more than 170 countries (United Nations, 2004:39).

UNFPA assists countries to improve reproductive health and family-planning services on the basis of individual choice. It is headquartered in New York and supports programmes in more than 150 countries and territories around the world (United Nations, 2004:40).

UNODC was established in 1997 with the purpose of assisting the UN to address the interrelated issues of crime, drugs and international terrorism. The agency, employing about 1 500 people worldwide, is headquartered in Vienna, Austria, with 21 field offices and two liaison offices in Brussels and New York (United Nations, 2004:37).

UNEP coordinates environmental activities, assisting developing countries in implementing environmentally sound policies and practices. It was founded in June 1972, has its headquarters in Nairobi, Kenya, and supports various country offices around the world through six regional offices (United Nations, 2004:38).

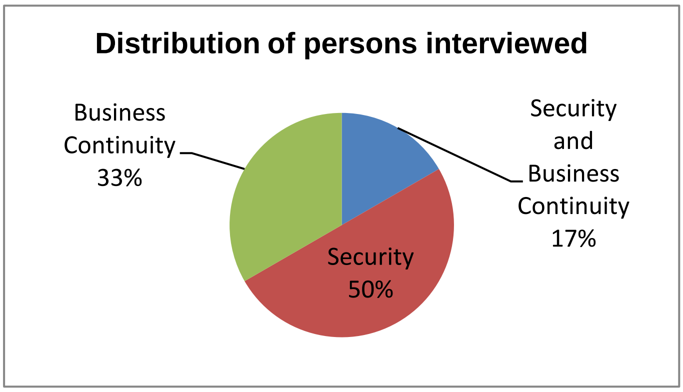
UNHABITAT was established in 1978 and has its headquarters in Nairobi, Kenya. It works in more than 70 countries with a mission to promote socially and environmentally sustainable human settlements development and the achievement of adequate shelter for all (United Nations, 2004:45).

UN Women was created in July 2010 to focus exclusively on gender equality and the empowerment of women. The agency is headquartered in New York and currently works in 98 countries worldwide (United Nations Women, 2014).

Out of the 12 agencies, three responded by saying that they were unable to partake in the study and one agency did not respond to the invitation. The reasons provided by two of the agencies that were unable to participate were that they did not have their own in-house security and/or business continuity management units and felt they would not be able to contribute to the study. The eight remaining agencies participated in the research.

After receiving the invitation to participate in the study, each agency identified the appropriate person(s) to be interviewed. While it was planned to interview the security manager as well as the business continuity manager in each participating agency, it became apparent that these functions were not always divided into two separate positions in all of the organisations, neither did all the agencies have both positions established. Graph 1 below indicates the percentages of the persons interviewed by job function. Twelve persons were interviewed in total. Out of the 12, two participants were responsible for both security and business continuity, four dealt only with business continuity, and six others focused only on security risk management. It should also be noted that out of the eight participating agencies, only six had implemented business continuity programmes while they all had security programmes. This, however, was not considered to be a problem because the participants interviewed had experience in security and business continuity management and thus had the necessary expertise required to answer the research questions. Since the number of participants that had business continuity and security risk management responsibilities was equally divided, the sample was representative.

Graph 1: Breakdown of the sample by job function



The demographic information of the 12 participants is outlined in Table 2. Anonymity and confidentiality were assured by anonymising the data.

Table 2: Research participants' demographic data

Research participants	Gender	Field of coverage
A	Male	Security and business continuity
B	Male	Business continuity
C	Male	Business continuity
D	Male	Security
E	Female	Security and business continuity
F	Male	Security
G	Male	Security
H	Female	Security
I	Male	Business continuity
J	Male	Business continuity
K	Female	Security
L	Male	Security

All the interviews were conducted by phone. The semi-structured interviews undertaken were based around a series of six questions (see Annexure D) aimed at exploring how security risk management and business continuity management are implemented by each organisation. In some cases, follow-up questions were asked to clarify and or explore additional areas which were raised by the participants.

In the following section of this chapter the findings from the interviews will be presented. The findings were analysed and cross-cutting themes identified. Chapter 5 will contain recommendations that are based on these findings.

4.3 INTERVIEW RESPONSES AND ANALYSIS

According to Yin (2011:233), it is challenging for researchers to present their data in qualitative studies due to the fact that the information is normally descriptive instead of being numeric. For this reason it is typically represented in narratives, tables or through the use of nonverbal methods such as photographs or graphics. Yin (2011:234-235) continues to say that readers are not only interested in the researcher's findings and conclusions, but also in a condensed version of the collected data which will present each participant's perspective. Researchers have the option to use quoted words or short sentences included in the researcher's own narrative, or using longer presentations containing a mixture of the researcher's own description and quoted or paraphrased dialogues (Yin, 2011:236-238). For qualitative studies, tables and lists are used to display data such as demographic information about the participants (Yin, 2011:241-243).

Since the information for this study was collected through semi-structured phone interviews, then analysed and interpreted, it is presented in a narrative format linking the data to the 12 participants through an alias to protect their identify. The discussion below includes both the data collected as well as the researcher's deductions that have been drawn from the information.

4.1.1 Security risk management approach

The research participants were asked to summarise how their agency manages its security risks and what the principles and methodologies are that underlie their security risk management approach.

The majority of participants (A, B, C, D, E, F, G, H, K and L) reported that their agencies follow a model that adopted the UN Security Risk Management Framework for Accountability. Under this framework the executive director (head of the UN agency) is ultimately responsible for the safety and security of all staff in the agency and is accountable to the UN Secretary General for exercising his/her duties in this regard. The responsibility for the safety and security of staff has been delegated to all the line managers in the organisation, including the heads of their overseas offices which are typically referred to as field or country offices. The heads of these overseas offices are accountable to their agency’s executive director for the safety and security of the staff in their field office through the heads of their respective geographical regional departments. These country representatives together with the heads of the other UN agencies present in a specific country, are also part of the local Security Management Team (SMT). The chair of the SMT is called the designated official who is appointed by the UN Secretary General and is responsible for the safety and security of all UN staff in that country.

In addition to the above, research participants H and I indicated that their organisations had recently adopted a risk appetite statement. They explained that risk appetite *“...is the amount of risk an organisation is willing to accept...*” and that it will vary from organisation to organisation, depending on their external work environment, systems and policies.

It is important for any organisation to consider their tolerance for risks. It not only defines the amount of risk an organisation is willing to accept, it also defines the level of action or the amount of resources an organisation is willing to invest to mitigate identified risks (Engemann & Henderson, 2012:19). According to the Hong Kong Institute of Bankers (2013:20), an organisation’s approach to risk management should be tied to their willingness to take on risks and it is important to define the organisation’s risk appetite to prevent exposure beyond an agreed level. The lack of defining a risk appetite is in itself a risk to an organisation and as an element of good practice other UN Funds and Programmes are strongly advised to develop risk appetite statements of their own.

Research participant A explained that the UN is currently reviewing their approach of “*how to stay and keep delivering*” by focusing on how to continue delivering programme activities while not necessarily being present in the specific location. This approach will reduce security risks to UN staff, if it means they need not be present in certain high risk locations. Participants B, G and F added that their approach to security also heavily relies on working with local communities and other relevant stakeholders to establish good relations. In this way the UN organisations obtain acceptance for their presence and work. Through this recognition, the UN agency is protected by the community. Other agencies (participants G and F) follow a similar approach but also train community members to implement their projects, while the organisation provides the materials and project oversight. This approach of using more local persons rather than deploying their own staff mitigates the risk to the agency by avoiding putting their own staff in harm’s way. The principle behind this reasoning could be that locals are more familiar with field conditions and are less likely to be directly targeted.

Regarding the organisational structure established for security, interviewees from five organisations (participants C, D, F, G, H, I, J, K and L) explained that their agencies have established a security unit within their headquarters and have also outposted security personnel to field offices, who are responsible for advising their respective managers on security in the specific country. In some of these agencies (participants F, H, I, K and L), the headquarters unit also includes an analytical and training element. Participant A explained that their agency only established a headquarters-based security unit, while participants B and E stated that their agencies do not have an in-house security unit since they rely on security support provided by another UN agency. The reason for this is that these agencies are co-located with another UN organisation which could outsource security to them. In the case of co-location the organisation does not employ dedicated security practitioners, but makes use of a security focal point system where a person is assigned security responsibilities in addition to their primary function. In this regard participant B said "*an example of this is when the head of the administrative unit in the field office is also assigned the responsibility for overseeing certain security functions in addition to their other job functions*".

According to participants B and E, the reasons for these different approaches can be attributed to the size of the organisation, the locations where they are working and available resources. The larger agencies (participants C, D, F, G, H, I, J, K and L) delivering humanitarian aid in emergency situations typically have a comprehensive security risk management structure in place, while smaller organisations either rely solely on UNDSS for security support or other UN agencies when they share the same office space. While the security structure in the agencies may differ, all the participants (A, B, C, D, E, F, G, H, I, J, K and L) confirmed that their agencies are part of the UN Security Management System and recognise the leading role played by UNDSS. These agencies also adopted the UN's Framework for Accountability, which defines roles and responsibilities for safety and security at various levels through the UN Security Management System and internally in each agency. Security risks and appropriate mitigating measures are identified through the Security Risk Management Model which was described in Chapter 3.

While it was not the purpose of this research to test the effectiveness of the different approaches, some of the interviewees did comment on why certain decisions have been made within their organisations related to the investment in security and the allocation of resources to this important management function. According to participant G, the agency managers view security as a drain on the limited resources the agency receives. Another participant (F) said that changes to their security programme only take place in response to "*traumatic incidents*". Three interviewees (C, H and I) commented on the fact that their agencies have recently been putting a lot of effort into reviewing their approach to risk management and security risk management, and that their security programme has evolved from taking a risk aversion approach to following a risk management approach. It is thus clear that there is no uniform standard of security risk management across all UN Funds and Programmes.

Working effectively in these high risk environments requires a level of resilience which would not be typically found in a normal business established in a developing country. It is therefore more important for all these UN Funds and Programmes to establish comprehensive security risk management and business continuity programmes to not only deliver their services, but also to ensure that they meet their duty of care responsibilities to their staff (UN Secretary General, 2002:2). These requirements were highlighted in the framework for accountability for the United Nations field Security Management System requiring the executive heads of UN agencies to: (1) have "duty of care" for staff employed by their agency and to ensure they are not exposed to significant risks; and (2) ensure that all programmes and projects being implemented by field offices adhere to UN security procedures and that sufficient provision is made for the security of staff working in these programmes (UN Secretary General, 2002:2-4). Since UN Funds and Programmes rely on funding from member states, it is important that these organisations continue to make the point that they cannot be asked to work in dangerous locations without donors making available sufficient funds to cover their security needs (UN Secretary General, 2002:7). Ultimately each agency has a duty of care for its own staff, and this includes doing what is reasonably possible to protect them.

4.1.2 Security risk exposure

Chapter 3 included an overview of the risks UN staff face daily. However, the researcher wanted to know if there were any particular risks that the participating agencies face due to the nature of their mandate or the specific location where programme activities are being conducted. The question posed to the interviewees was: "What are the most predominant security risks faced by the organisation?"

Participants A, B, C, D, E, F, G, H, I, J, K and L indicated that their agencies face similar risks such as abductions, robberies, and civil demonstrations as identified by other UN agencies working in the same location. They also highlighted that there are risks associated with the specific mandate of their organisations and the location where their services are being delivered. For example, participant B said that "*the demand for their agency's services* *in high risk locations has increased*", while research participant G mentioned that "*currently the highest risk location for their staff is in Syria*". Participants A, C, F, H, I J, K and L agreed that those UN Funds and Programmes that deliver humanitarian aid in emergency and conflict environments are generally more vulnerable to abductions, robberies, armed attacks, and civil demonstrations than those UN agencies that are mainly working closer to the capitals of the countries. All the participants (A, B, C, D, E, F, G, H, I, J, K and L) concurred that the environment in which they are working is becoming increasingly hazardous and the number of security incidents involving their staff is increasing.

Participant G explained that member states expect their agency to be present in high risk locations to deliver aid, emergency and other development services. On the other hand, according to participants C, E and G, their agencies also have to maintain a delicate relationship with host country governments where they work. For example, some of the governments do not always agree with the agency's assessment of the level of security risk, especially when the agency announces that it wants to relocate or evacuate staff from a specific conflict area. It therefore requires a delicate balance to continue working in locations that hold security risks, while knowing that host country governments may not be able to create a safe environment for the UN agencies to operate. Many of the security threats that occurred in 2012/13 such as intrusion onto premises, deliberate attacks on UN offices, abduction of staff and theft of emergency supplies, directly impacted on the continuity of operations (participants A, B, C, D, E, F, G, H, I, J, K and L). Not only are security strategies required to reduce the likelihood of these incidents from occurring, or to reduce the level of impact, but business continuity plans are required to deal with the residual risk when critical business operations are disrupted (participants B, I and J).

4.1.3 Business continuity programme

While the concept of security risk management has been standard practice within the UN system since UNDSS developed a Security Risk Management Model, business continuity management is a relatively new initiative (UNDSS, 2009:1 & Posta & Wynes, 2011:25). In line with the study's aim, the researcher wanted to explore the relationship between security risk management and business continuity management within UN Funds and Programmes and asked each research participant whether their agency has a business continuity programme, and if so, how does it work?

Participant A explained that their business continuity management programme is designed to respond to incidents that may result in the disruption of business functions due to man-made and/or natural events such as: loss of personnel; interruption of mission-critical systems; denial of access or loss of buildings; loss of vital records and/or loss of supply chain products and services. Business continuity management has been rolled out across all their offices, including their headquarters, regional offices and country offices (participant A). Business processes are considered critical if their disruption will severely impact one or more of the agency's critical functions and restrict the agency to deliver its mandate (participant A).

Participant B described that they have had a business continuity plan in place for the past three years. The plan is currently only applied to the headquarters of the organisation and has not been rolled out to their regional and country offices. The approach they take is slightly different from the approaches described above. According to participant B, their plan is focused on those critical business processes that need to be recovered within a period of 72 hours, and the plan takes the following scenarios into account:

- "*A major information and communication technology system failure.*
- *Denial of access to their offices.*
- *Loss of a strategic vendor or supplier.*
- *A catastrophic loss to staff*."

Participant B mentioned that they use a combination of the following strategies to continue operations, following a disruption in their business processes:

- "*Implement manual work arounds to carry out business activities such as faxing documents instead of sending them by email.*
- *Work remotely if the office is inaccessible. This is done by having an information technology system that allows remote access so that staff can work from home.*
- *Transfer services to an office in another location. This way the other office takes over the responsibility for carrying out the transferred activities.*
- *Identify another office location in the city where their headquarters is located, so that in the event that their main office is inaccessible, key staff will work from this location.*
- *Postpone or temporarily suspend activities depending on the scope of the incident*."

Participant E explained that they also have a business continuity management plan for their corporate operations. Since they are co-located in the same compound with a number of other UN organisations, their plan is coordinated by UNDSS and involves all the agencies based in this location. It follows similar scenarios and response mechanisms as described by participant B, namely a significant information technology system failure, denial of access to their offices, and a loss of staff. At the corporate level business continuity and security are situated in different departments. Business continuity management has also been rolled out to their field offices (participant E). Similar to participant B's agency, participant E observed that since their field offices are also co-located with other UN agencies, their business continuity plans are prepared in conjunction with that agency because their offices are responsible for providing administrative services to the participating agency's local office. According to participant E, in many cases the local offices "*did not carry out a business impact analysis because they viewed it as being too elaborate and complicated*". This participant also remarked that from experience, business continuity management at headquarters is recognised as being a management function and not part of security. However, in the field business continuity management is seen as a security issue.

Participant I explained that their business continuity programme was recently completely revised. The current approach focuses on identifying critical functional areas within the organisation at the corporate level. Fourteen functional areas including human resources management, corporate treasury, and security were identified as being critical to the agency. After identifying the 14 areas, time-critical business processes within each one of the areas were identified. The maximum tolerable period of disruption which was used to identify individual time-critical processes, is a period of 48 hours. The maximum tolerable period of disruption was estimated to be the length of time after which an organisation's viability will be significantly threatened if the disrupted business operations cannot be resumed.

Different terms exist in business continuity management to describe outages, for example maximum acceptable outage or maximum tolerable downtime, but for the purpose of this study an outage is considered as the period of time that a business function or process is expected to be unusable or inaccessible following a disruption (Graham & Kaye, 2006:396). Among the time-critical business processes were several security risk management processes such as accounting for staff following a security incident, but different from other organisations, they did not carry out a security risk assessment to feed into the business impact analysis (participant I). In accordance with Graham and Kaye (2006:89) risk management and business continuity management are complementary and neither is optional; both are required. In addition, the business impact analysis and risk assessment should also be carried out, because together they help develop an understanding of the organisation and its exposures and will assist in developing commensurate mitigation and recovery strategies.

Participant J explained that their "*agency's business continuity programme is divided into three tiers: (1) corporate level; (2) regional level; and (3) country office level*." At the corporate level eight core critical functions have been identified. Management determined that if these functions are not recovered within a period of one week the disruption/outage would have a severe impact on the agency achieving its mandate. These critical functions include: maintaining staff safety and security (which is mainly focused on accounting for staff following an incident and communicating with staff during the emergency); processing the payroll to ensure staff get paid on time; corporate treasury functions; and information technology functions as they relate to maintaining global connectivity among the headquarters and overseas offices for enterprise software and services. In the event of a disruption, priority would be given to the recovery of the eight critical functions followed by the recovery of other business operations. According to Graham and Kaye (2006:60), it is good practice to develop recovery strategies for each identified time-critical business function and it is up to senior management to determine the critical functions to be included, as well as approve recovery strategies to recover selected critical business operations. The criteria involved in selecting recovery strategies may include cost, the time to recover the disruption, reliability of the strategy and the level of recovery once the strategy has been deployed (Graham & Kaye, 2006:60).

Participant L explained that the purpose of their business continuity programme is not to address immediate emergencies that are covered by other contingency plans, but is focused on responding to events that will adversely affect the agency's financial status, reputation, running of normal operations as well as the safety and security of its staff and other assets. The objective of the plan is to minimise the loss of life and damage to assets and to continue business operations at the headquarters and field level (participant L). Their plan is designed to achieve operational status no later than 12 hours after activation following a disruption (participant L). The plan also includes a detailed crisis management framework to respond to emergencies and is usually activated prior to activating the business continuity plan.

According to participants G, F and J, their agencies have not yet implemented business continuity management programmes. They have developed information and communication technology disaster recovery plans, which are focused on the recovery of their information technology system in the event of a disruption such as a power failure or network failure. Participants G, F and J explained that the information technology disaster recovery programme is mainly focused at the headquarters level. At the field level they rely on contingency plans focusing on the life and safety of staff to deal with emergencies and not the continuation of their business operations. According to participant F, "*business continuity activities are typically considered at the last minute*" when there is a looming crisis situation. Another approach utilised by these two agencies is to review the activities performed at the field level and rank them in order to preserve life (i.e. water, sanitation, food, nutrition, shelter, and health care). In the event of a deteriorating security situation they may have to reduce the number of staff, and this reduction may require scaling back on the services provided until only those that are critical to save lives are maintained (participants G, F and J).

According to participants A, B, E, J and L, each geographical regional department is responsible for establishing its own business continuity plans within the framework of the corporate plan, but focusing on their geographical region, including country offices. At the country office level, business continuity plans focus on the recovery of critical processes aimed at ensuring the safety and security of the staff and continuing programme activities. Security risks are considered when business impact assessments are carried out (participants A, B, E, J and L).

Two participants (B and E) mentioned that the key risks that their field offices face from a business continuity point of view are that many of their administrative business processes are performed by other UN agencies on their behalf. When these processes are disrupted, it not only impacts both organisations, but the participant's agency has to rely on the effectiveness of the other UN agency's business continuity plan to recover the disrupted process in a timely manner.

As previously explained, the purpose of business continuity management is to identify the critical functions performed in an organisation and to develop strategies to continue these functions following a disruption which causes an outage or loss of services (Engemann & Henderson, 2012:4). While all business functions may be deemed important, not all are categorised as critical. Critical business operations are those that are required to support the mission of the organisation and are also time sensitive and cannot be disrupted for an extended period of time (Engemann & Henderson, 2012:23-24). In addition, since it may not be possible to recover all business functions at the same time, it is good practice to identify the priority order in which these functions need to be restored (Engemann & Henderson, 2012:22). The business impact analysis can therefore be considered as the foundation upon which the rest of the business continuity plan is built because it helps identify time-critical business processes.

The findings indicated that agencies have tailored their approach to business continuity management to suit their own needs. Outlined in the paragraphs below is a summary of the different approaches taken by the participating UN agencies:

a. Maximum tolerable period of disruption. According to Graham and Kaye (2006:94), business processes have to be assessed to determine the time during which a process, after being disrupted, must be recovered before the outage severely impacts the organisation's ability to achieve its objectives. While it is up to each organisation to determine their tolerance for outages, participant I mentioned that in their agency their maximum tolerable period of disruption was 48 hours, participant B said that they had identified 72 hours as the cut-off time and participant J mentioned that they had decided on one week. It was also not clear whether the time frame was the maximum time and whether individual processes were actually assigned specific outage periods within this timetable. Setting the point in time when a process must be resumed, allows the organisation to prioritise its recovery efforts.

b. Security risk assessment and business impact analysis. According to Graham and Kaye (2006:89), risk management and business continuity management are increasingly moving together since they are complementary. The purpose of the security risk assessment is to identify security risks, estimate the probability of those risks impacting the organisation and put into place security measures to mitigate the risk and identify any residual risk that still remains. Business impact analysis is all about determining the impact that could occur when a time-critical business process is disrupted for any reason. Based on the feedback received from participants A, B, E, J and L, their organisations incorporated a security risk assessment as part of the process to develop their business continuity plan. In addition to performing a security risk assessment in conjunction with the business impact analysis, participants A, B, E, I, J and L also mentioned that business operations related to safety and security, such as accounting for staff following a security incident, were identified as a time-critical process. However, it is not clear whether the security risk assessments honed in on each time-critical business process in addition to looking at security at the organisational level. Since the business impact analysis focuses on individual business processes, the security risk assessment should also be applied to individual business processes to identify security risks that may adversely affect the process if not properly mitigated (Graham & Kaye, 2006:104).

c. Critical business operations. Another difference in approach that was highlighted was the identification of critical operations. Critical operations or business functions are those that are required to support the primary mission of the organisation (Engemann & Henderson, 2012:23). Participant J said they had identified eight critical functional areas within their agency and participant I explained that they had identified 14. Within these identified functional areas they then proceeded to identify critical business processes. This sound risk management approach is good practice because there may be many important business operations that are performed within an organisation, but they are not all time sensitive and therefore not time-critical business operations.

d. Headquarters versus country-based offices. Among those UN agencies that implemented business continuity programmes, the majority of the agencies centred their business continuity programmes around business functions performed at their main or headquarters office. Only three agencies (participants L, J and I) have expanded their business continuity programmes to include business operations performed at their country offices. The functions performed at the country office level, such as local human resource activities, payroll and project administration may not be deemed as critical to the overall existence of the organisation, but these functions are important and essential at that location to support local communities that are the beneficiaries of the programme. According to Graham and Kaye (2006:57), it is good practice for organisations to apply the principles of risk and business continuity management within the context of the location where business operations are carried out, even when it is in a location away from the main office.

4.1.4 Organisational structure, security risk management and business continuity management functions

Since the aim of the study is to examine the integration of security risk management and business continuity management, the researcher was not only interested in it from a process level, but also from an organisational structure point of view. Research participants were therefore asked to describe where security risk management and business continuity management functions are located in their organisational structure, as well as the reporting lines and areas where they interact.

Participants A, C, and I indicated that the same person responsible for security is also responsible for business continuity, and in some instances these functions are part of the same department. In the rest of the participating agencies, security and business continuity functions are located in different units within the overall organisational structure (participants

B, D, E, H and L). In these agencies there is close cooperation between the two functions and security issues are included in the formulation of business continuity plans (participants B, D, E, H and L).

Half of the participants (A, B, C, D, E, and J) indicated that their security unit was located within a department also responsible for other management or administrative functions such as human resources and procurement. One of the other participants explained that their security unit is part of an operations department which is responsible for overseeing the agency's geographical regions and operations (participant L). In none of the participating agencies did the security unit report to the chief risk officer or the unit responsible for enterprise risk management where these functions existed (participants A, B, C, D, E, F, G, H, I, J, K and L). In the majority of cases the agency's security manager had direct access to senior management within their agency, which was a positive observation. This good practice is in line with Roper's (1999:98-99) recommendation that an organisation should employ a full-time security risk manager if the organisation is large enough to afford and fund the position, and that the security risk manager should report directly to senior management and not through an intermediate manager.

In two of the agencies where security and enterprise risk management units exist, three of the interviewed participants stated that they functioned autonomously and had little contact with each other (participants F, K and L). According to participant F, "*the enterprise risk management function in their agency focuses on financial, reputational and information technology risks*". Participants G and F explained that business continuity in their agency still only focuses on information technology disaster recovery and has not evolved to encapsulate organisational business processes.

It should also be noted that, as mentioned previously, two out of the three organisations that declined to participate in the study did so because these agencies did not have security or business continuity units as part of their organisational structure. They relied on the support provided by other UN agencies for security risk management support. It is unknown if these organisations have developed their own security and business continuity plans.

According to Graham and Kaye (2006:38-39), the risk management governance model within an organisation (which would include UN agencies) should reflect the nature, scale of operations, complexity of the organisation's risk profile, risk appetite and the environment in which it operates. Even though there is no one-size-fits-all approach to it, as can be seen in the findings from this study, senior managers and their boards need to understand that it is their responsibility to pay attention to the risks their agencies are facing. In carrying out their work it is therefore good practice for them to establish an effective risk management framework, including security risk management and business continuity management functions for their organisations (Graham & Kaye, 2006:34).

The responses to this question were a good indication of the maturity of security risk management and business continuity management within each one of the UN Funds and Programmes. Even though, as was highlighted in Chapter 3, many of the participating agencies identified security risks to their staff and achieving the organisation's objectives as a concern in their respective strategic plans, this did not always translate into a comprehensive risk management framework as reflected in the findings from this study.

4.1.5 Business continuity in offices away from the headquarters

Since the agencies included in this study also have a field presence, the researcher wanted to examine to what extent business continuity programmes are implemented in offices away from the headquarter locations.

Findings indicated that business continuity management was predominantly regarded as a management function applicable to operations at headquarters (participants A, B, E). Out of the eight UN agencies, only three (participants L, J and I) have rolled out business continuity to their field offices, three others have not yet implemented business continuity programmes at country offices (participants B, G and K), while the rest are in different stages of implementing business continuity programmes at their overseas offices (participants A and E).

Participant E explained "*that the roll out of business continuity among their country offices was at various levels of maturity. Most offices are in the process of completing a business impact analysis, security risk assessment and developing recovery strategies. A few offices have completed the full plan*".

Two of the participants (B an E) explained that their overseas offices are normally co-located with other UN agencies and their local business continuity plans are prepared in consultation with the hosting agency, since this organisation performs most of the agency's administrative functions. According to participant B, this increases the vulnerability of the participating agency because they have to rely on another organisation for their business continuity plan. In the event that the hosting agency cannot perform its functions, it will harm their agency (participants B an E). Participant E mentioned that among their field offices there was a perception that "*business continuity is seen as a security issue*" and that conducting a thorough "*business impact analysis is seen as being too elaborate and complicated*".

Only two participants (J and I) indicated that their business continuity programme extends to their field offices. They (participants J and I) highlighted that core critical processes for field offices include: (1) "*safety, security of staff and accounting for staff in emergency situations*"; (2) "*delivery of critical programme/project activities*"; (3) "*processing the payroll for payment of staff*"; and (4) "*providing various support functions to other UN agencies*". Three of the agencies that do not have formal business continuity programmes at country level, explained that their offices and individual projects have developed extensive contingency plans to continue delivering their activities in spite of deteriorating security situations (participants F, G, and K). These approaches include using other organisations to deliver programme activities as a way of transferring the risk.

Although the majority of the agencies incorporated both security risk management and business continuity management functions in their respective organisational structures, in most cases this did not extend down to the field level. Findings from the study indicated that, notwithstanding it being recommended that both security risk management and business continuity management should be implemented in UN agencies, the majority of the agencies still largely only utilise security risk management at the field level as discussed below in section 4.3.5, instead of applying both methodologies as part of an integrated risk management model (Graham & Kaye, 2006:63). As a result, this addresses only security risks and not the recovery of business operations which are disrupted when security risks do materialise. It is therefore good practice for business continuity plans to be integrated throughout the organisation in order for them to be most effective.

4.1.6 Integration of security risk management and business continuity management

While the previous research question focused on the organisational structure, the purpose of the following question was to examine to what extent security risk management and business continuity management processes and oversight are integrated. With this in mind, participants were asked to indicate if the outputs from security risk assessments are considered as inputs into the business impact analysis, and if so, how.

During the interviews, some of the participants (A, B, E, I and L) who had indicated that their agencies implemented a business continuity management programme, mentioned that security risk assessment was also performed. The results of the assessment were included in the business impact analysis as well as into the overall business continuity plan. The objective of incorporating the security risk assessment in the business impact analysis is to develop a picture of the security risk landscape in which the agency operates (participants A, B, E, I and L). For example, participant L mentioned that "[they] *we identified a pandemic outbreak, terrorist attack and failure of their servers as high risks in addition to other risks that are ranked as medium and low*". According to Graham and Kaye (2006:94), it may seem as if security risk assessment and business continuity overlap, but both have a specific purpose; the security risk assessment identifies risk that may cause harm (and the potential consequences), while the business impact analysis focuses on identifying critical business processes.

Participants A, B, E, I and L mentioned that risks in most cases were looked at from an agency perspective rather than identifying the risks associated with individual business processes and the location where these processes are being performed. This approach may be acceptable when all the processes are performed in one location, but once the analysis identifies activities that are performed in another location, then the security risk assessment needs to be expanded to include the other locations as well (Graham & Kaye, 2006:93 & 95).

Participants A, B, E, I and L also explained that apart from considering the security risk assessment during the business impact analysis, there was no other interaction during the rest of the steps in the two processes. Another area where the security risk assessment may play a role is when strategies are identified to maintain and recover critical operations (Engemann & Henderson, 2012:62). For example, to continue a specific business function, the use of an alternative worksite may be considered if the primary office is not accessible. However, before this site can be included in the plan, good practice would dictate that a security risk assessment of that location also needs to be performed to identify any security concerns.

4.1.7 Crisis management

Although not part of the original set of questions, the issue of crisis management was highlighted as a predominant theme during interviews with participants and therefore merits further discussion in this study. A crisis is the materialisation of a threat and it could range from minor incidents with limited impact to the organisation, to major events with the ability to significantly impact the organisation (Engemann & Henderson, 2012:302). In order to manage the response to the incident as well as to oversee the implementation of the business continuity plan, when activated, an organisation requires a crisis management team normally consisting of senior managers who have the authority to make decisions during the crisis (Broder & Tucker, 2012:264).

Within the context of this study many of the participants explained that their agency has started to implement the Organisational Resilience Management System, which was recently adopted by the UN as their emergency management framework (participants A, C, D, H, I and L). According to Graham and Kaye (2006:362-363), organisational response plans should include: (1) an emergency response plan to respond to location-specific incidents focusing primarily on ensuring the life and safety of employees; and (2) a business continuity plan outlining the plan of action to resume identified time-critical business operations. The security risk assessment and business impact analysis are where the requirements for these plans are identified (Graham & Kaye, 2006:363). It thus seems as if there is a greater recognition at the institutional level of the UN of the importance of including both security risk management and business continuity management in order to enhance emergency response capabilities.

Participant A explained that the origin of the "*United Nations Organisational Resilience Management System framework was as a result of Hurricane Sandy that impacted New York as well as the United Nations premises in October 2012*". The objective of the Organisational Resilience Management System framework is to mitigate the impact of, and respond to disruptive events by applying crisis management, emergency response and business continuity methodologies. According to participants A, C, H, I and L, this allows emergency medical support, business continuity, security, crisis management, crisis communications and information and communication technology disaster recovery to function within a wider context of enterprise risk management.

Only two participants (F and I) highlighted the importance of training and exercising of staff as a requirement to maintain their level of preparation. Participant F said that "*all their* [our] *field managers undergo security training at their training centre*". Participant I explained that they will carry out an exercise following the revision of their business continuity programme. This good practice is highlighted by Broder and Tucker (2012:254), who recommend that one table-top and one full-scale exercise be held once a year. Without regular testing and exercising, security and business continuity contingency plans can fail, which may result in injuries or loss of life (Engemann & Henderson, 2012:165)

The findings indicated that in the majority of cases the responsibility for responding to incidents was decentralised to the office closest to the origin of the incident (participants A, C, D, H, I and L). In some UN agencies, crisis management response is limited to those incidents that affect the life and safety of staff and those that impact information technology systems, as opposed to viewing crisis events in the broader sense. Only a few organisations (participants A, C, D, H, I and L) have established a comprehensive organisation-wide crisis management framework, which includes the capacity to respond to incidents and the recovery of business operations in an integrated manner across the UN agency. The findings also showed that regular exercises of contingency plans are not carried out throughout UN agencies (participants F and I).

4.4 DISCUSSION OF FINDINGS

The responses to the research questions provided a better understanding of how security risk management and business continuity are approached by the different UN Funds and Programmes, how they are structured and organised within each agency, how they are carried out and integrated, as well as how the UN agencies deal with crisis management. It was clear from the interviews that although there were some similarities in approaches, there were also significant differences, many of which were due to the different mandates of the organisations, the threats they face working in high risk countries, and the maturity in understanding and applying the concepts of risk management.

Findings from the study indicated that security risk management within the UN system has evolved since the bombing of the UN headquarters in Baghdad in 2003; resulting in the recommendation of the Ahtisaari report (2003:25) that a comprehensive review and reform of the UN security system had to be carried out. In most agencies, security has matured from a purely protective and defensive posture to following a risk management approach. According to Roper (1999:ix), following a risk management approach is key to implementing a modern security programme. Risk management offers a deliberate and structured method for decision making about the utilisation of resources and the selection of cost-effective security measures to protect assets (Roper, 1999:3). Findings indicate that the strength of the UN Security Management System lies in its Security Risk Management Model, including the UN Security Risk Management Framework for Accountability, which enables a thorough assessment of security risks and implementation of commensurate mitigating security measures.

In contrast to security risk management, findings from the study revealed that business continuity as a management process and important tool for risk management, has not yet been comprehensively adopted by all UN Funds and Programmes. Out of the eight UN Funds and Programmes that participated in this study, six have established a business continuity programme at both headquarters and regional levels and only three have extended it fully to their field offices. Two organisations' business continuity programmes have not evolved beyond the realm of information technology disaster recovery. In some of the UN agencies, business continuity is part of the wider risk and strategic management framework, while in others it still needs to be adopted. It seems as if senior management of these organisations has not yet adopted a proactive business continuity plan as good practice to enhance the resiliency of their agency, which could impede them from achieving their objectives.

Although the approach and objectives of security risk management and business continuity are different, both need to be incorporated within the broader risk management framework of the organisation. The business impact analysis was identified as being the foundation upon which the rest of the business continuity programme is built. The purpose of the business impact analysis is to identify and analyse business processes with the objective to understand the impact of downtime, which then drives the assignment of recovery strategies and prioritisation. On the other hand, the objective of the security risk assessment is to identify and analyse security risks that may affect the organisation's ability to carry out its business processes and to develop controls to decrease the likelihood or impact of a disruption.

Evidence from the findings indicated that there are areas where business continuity management and security risk management activities do interact. One area where this interaction occurs is when the business impact analysis is carried out. Many of the UN agencies are considering the results of the security risk assessment as inputs into the business impact analysis. However, all the organisations aggregated their security risks and applied it to the organisation as a whole, but did not identify the specific security risks associated with each individual process. This is an important distinction, since the objective is to focus on the identification of time-critical business processes and the security risks that may cause disruptions to the specific process. Drilling down to the process level ensures that all the potential causes for disruptions are identified. It is then up to the security unit to mitigate the impact of security risks, while the business continuity unit develops recovery strategies in the event that these security risks do materialise and disrupt business operations. The impact of a disruption typically leads to one or a combination of the following: (1) unavailability of the location where the processes are performed; (2) unavailability of the IT infrastructure to perform the processes; and (3) unavailability of the required staff to perform the processes to continue operations (Broder & Tucker, 2012:233-234). Recovery strategies should therefore be developed around these scenarios.

When combined, security risk management and business continuity management ensure the safety of staff, maximise the defence of the agencies' reputation, minimise the impact of events on the agency as well as their beneficiaries, protect the organisation's assets and very importantly, demonstrate effective governance. This can only be done by establishing an organisational risk management model and by positioning security risk management and business continuity management within the UN agencies' organisational structure so that they can effectively work together and at the same time allow access to senior management.

Another area, which did not seem to be well defined, related to individual agencies' ability to respond to crisis situations in a holistic manner. In accordance with ISO (2012:17) organisations are advised to establish a management structure and procedures to respond to disruptive incidents focusing on life safety of staff as the first priority and then to activate an appropriate business continuity response. Disruptive incidents are any events that may cause an outage in business operations, which will include security risk incidents. Most organisations have a fragmented and decentralised approach to dealing with emergencies, while it is advisable to create a comprehensive crisis management framework spanning across the whole organisation as proposed by ISO (2012:17).

4.5 CONCLUSION

The goal of this research was to investigate the relationship between security risk management and business continuity management and to determine how these two methodologies are applied within the UN system in order for UN Funds and Programmes to enhance their own resilience. Interviewing representatives from the eight participating agencies enabled the researcher to acquire relevant information to answer the research questions.

UN Funds and Programmes exist to deliver humanitarian aid, economic and social development and reconstruction activities, and the locations where these services are acutely required are typically where security risks are also most prevalent. The demands on UN agencies to deliver services in high risk locations have increased. The number of security incidents involving UN staff members is increasing annually. In order to respond to the consequences of security threats, the security risk management system has evolved and continues to mature. Agencies under the leadership of UNDSS use a Security Risk Management Model for identifying and assessing the risks that they are exposed to, before developing commensurate security measures to mitigate the impact and reduce the likelihood of the threats from occurring. This process, however, does not eliminate all risks and there will always be some residual risks.

The majority of the agencies participating in this study have implemented business continuity management programmes to deal with disruptions in their core business processes, such as processing the payroll to pay staff each month. These programmes are mainly centred at headquarters and only a few have rolled it out across the whole organisation, in spite of the fact that security risks are more acute at the field level than at headquarters. In some organisations business continuity remains focused on the recovery of information technology systems and has not yet evolved into a comprehensive programme. In the same way that security risk management has evolved, business continuity management needs to emerge and position itself as part of the wider risk management framework of the organisation.

A lack of resources and making decisions in response to security incidents should not be the drivers for implementing effective security risk management programmes. The heads of the different UN Funds and Programmes need to recognise that this is a management function and should be incorporated into the agency's corporate governance responsibilities. Security risk management can also not stand alone. It needs to be included in an overarching risk management framework of the organisation. This requires an effective governance structure to ensure that the strategy, policy-making, governance and required oversight functions are put into place.

Chapter 4 provided a detailed account of the data collected from the research participants, and it reflects an accurate account of their views on the relationship between security risk management and business continuity management and how these two methodologies are applied in UN Funds and Programmes. It also includes an analysis and interpretation of the qualitative data collected. Chapter 5, which is the final chapter, will cover the recommendations and conclusion of the study drawing from the literature review and the data collected through the semi-structured interviews.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 INTRODUCTION

This study set out to explore the relationship between security risk management and business continuity management and to determine how these two management functions are applied by UN Funds and Programmes to enhance their own resilience. Resilient organisations are those that are able to identify threats, understand the consequences if the threats materialise, react effectively to incidents, and recover from disruptions.

The researcher recognises that resilience and risk management in an organisational context encompass much more than just security risk and business continuity, but it was decided to limit the scope of this study to only focus on two specific business management functions, namely security risk management and business continuity management, which were described in Chapter 1. For the purposes of this research, security risk management is defined as a systematic approach for assessing and acting on security risks while ensuring the safety and security of an organisation's personnel and facilities and ensuring that organisational objectives are achieved. The objective of business continuity management is to identify critical business functions and to develop procedures to restore and continue these functions, following a disruption.

To answer the research questions, the researcher adopted a qualitative research approach. This flexible approach enabled field-based data to be collected through interviewing participants and analysing their feedback. The research focused on UN Funds and Programmes as a sub-set of agencies within the UN family of organisations. Twelve participants, representing security and business continuity functions from eight UN Funds and Programmes, agreed to partake in the study and were interviewed. Each one of these agencies has a specific mandate, such as providing assistance to refugees, promoting food security, poverty reduction, improving reproductive health and family planning services. They also operate in fragile states as well as in emergency and humanitarian crises situations where the security risks are often higher than in normal developing countries. Data were collected through conducting semi-structured telephone interviews with the identified participants from each agency. The findings from the interviews were discussed in Chapter 4 and conclusions and recommendations stemming from the findings are outlined below.

Being able to proactively mitigate the impact of inherent security risks and being able to respond to the impact from residual risks on business operations, should be regarded as extremely important for any organisation. This is equally true for UN organisations that work in fragile states and conflict environments where beneficiaries depend on their daily support. As mentioned previously in Chapter 4, there is an increasing demand for the services being provided by UN Funds and Programmes while their working environment is constantly evolving. The potential impact of disruptions to their operations cannot be overestimated, and the way they plan for and respond to these various threats, needs to keep pace with the environment in which they are working.

5.2 CONCLUSIONS OF THIS STUDY

As mentioned before, the aim of this study was to explore how UN agencies apply security risk management and business continuity management as well as the linkages between the two methodologies. Through this research, good practices and apparent gaps in how these two methodologies are implemented, were identified. In this chapter recommendations will be made with the aim of increasing these organisations' overall resilience.

The research confirmed the need for both security risk management and business continuity management and the role each function plays to enhance an organisation's resilience. It also highlighted that while they are two separate management functions, both need to be implemented within a larger risk management framework and they need to be closely aligned in order to be effective. The analysis of the information gathered from the UN Funds and Programmes showed that while security risk management has been well established, it is not the case with business continuity management. In addition, where both are being implemented there are varying degrees of interface between the two functions. While the following recommendations are specifically aimed at the UN Funds and Programmes, the researcher is of the opinion that other organisations working in humanitarian and emergency situations in high risk locations such as international NGOs and the International Federation of the Red Cross, will also benefit from the proposed recommendations to enhance their own systems and procedures. The findings led to five main recommendations which are organised around the specific objectives of the study described in Chapter 1.

Even as the working environment for UN Funds and Programmes has become increasingly dangerous, UN agencies have taken the decision to "stay and deliver" as opposed to withdrawing from high risk areas. As mentioned in Chapter 1, this means that these UN agencies have to be resilient to cope with security incidents and also reduce the impact these incidents have on their business operations. The literature review shows that both security risk management and business continuity management are two important methodologies that organisations use to mitigate risk and to keep their critical operations functioning. This research studied whether UN Funds and Programmes used these two management processes in an integrated manner so that they could achieve a high level of resilience. As the research findings show, there is a wide range of good practices among the different UN agencies in how they use and integrate security risk management and business continuity management. In some of these organisations, both processes exist but are not necessarily integrated, while in others, the agency either focuses on only security, or only contingency planning.

The findings from this research study show apparent gaps in how UN Funds and Programmes employ these two methodologies, and the researcher has made recommendations on how these organisations can strengthen the interface between security risk management and business continuity management so that they can continue to work in these very dangerous environments and be more resilient. For other organisations, such as those in the private sector or non-profit organisations, there are many lessons to be learned from this study which can be applied to the way they operate in difficult environments.

A summary of these recommendations is presented below and recommendations are expanded on in the rest of this chapter.

Recommendations for better integration of security risk management and business continuity management functions:

- Incorporate security risk management and business continuity management functions and responsibilities into the larger agency-wide risk management governance framework.
- Expand the scope of business continuity in those UN agencies where it currently sits in the domain of information technology, or has not yet been comprehensively implemented across the organisation.
- Establish a comprehensive crisis management framework spanning across the whole organisation, from headquarters to country offices.

Recommendations for strengthening security risk management and business continuity processes and oversight:

- Develop the capacity to gather risk data across the agency and aggregate it to view the full spectrum of risks, including security risks and business continuity risks in a holistic manner. This will enable the UN agency to prioritise and manage a portfolio of risks rather than responding to individual risks.

- Integrate security risk management and business continuity management processes to enhance an organisation's resilience to more effectively address security incidents in high risk locations, as well as to resume disrupted critical business functions in a timely manner.

5.3 RECOMMENDATIONS FOR BETTER INTEGRATION OF SECURITY RISK MANAGEMENT AND BUSINESS CONTINUITY MANAGEMENT FUNCTIONS

5.3.1 **Recommendation 1:** Incorporate security risk management and business continuity management functions and responsibilities into the larger agency-wide risk management governance framework

The first recommendation is that UN Funds and Programmes should incorporate security risk management and business continuity management into a larger enterprise-wide risk management governance framework, to enable senior managers to make strategic and operational decisions.

In the private sector there are numerous laws and other requirements that focus on strengthening standards for corporate governance. These initiatives help businesses to operate more efficiently, improve access to capital, mitigate risk, and safeguard against mismanagement. The responsibility for understanding and managing risks to the business ultimately rests with the board of directors and senior management, and this ensures that risk management is incorporated into the overall corporate governance framework.

As indicated in the findings of this study, not all UN agencies have adopted an enterprise-wide risk management approach. This means that risk management in these agencies is siloed, and some risk practice areas are absent. Since risk is measured against its impact on the achievement of organisational goals, it is important to have a comprehensive view of the risks that may affect the organisation. Because senior management is responsible for achieving the organisation's objectives, they are also responsible for managing the risks that may affect their ability to realise these goals. They can only do this if they have a holistic overview of the risks, including security risks that their organisation is exposed to.

The ultimate accountability within UN agencies for risk management and business continuity management lies with executive heads and senior managers, while other managers and staff are responsible for implementing risk mitigation measures. Currently, as indicated by the findings of this study, this responsibility is often fragmented as it may lie in different parts of the organisation and even in different geographical locations. Strengthening the risk management governance structure does not necessarily require additional layers of management. It is, however, essential that accountability and responsibility for security risk management and business continuity management, within the larger risk management framework, are clearly identified and formally assigned. Some of this is already addressed through the UN Security Risk Management Framework for Accountability, but it needs to be expanded to cover risk management in a broader sense. Specifically, it is recommended that the UN Funds and Programmes do the following:

- Develop a risk policy and risk appetite statement, which should be endorsed by each agency's executive head and senior management, and if possible, its executive board. The risk policy should create a shared understanding of, and promote a consistent approach to: risk awareness; risk intelligence; and risk management within the organisation in order to make better, more "risk-intelligent" strategic and operational decisions. The risk policy should articulate risk principles and risk appetite levels related to key areas of the organisation's operations. Because it is difficult to aggregate all risks into a single number, it may help to set the risk appetite for identified risks such as security risks, separately.
- Establish a risk committee which is responsible for overseeing all risk management functions within the agency. This committee must ensure that there is a cohesive corporate risk management strategy in place across the agency, which must include strategies for security risk management and business continuity management.
- Appoint a chief risk officer or assign a senior manager with the responsibilities that would normally be assigned to a chief risk officer. The main task of this position is to provide strategic oversight of the entire risk management framework. Individual line managers remain responsible for risk, including security risk management, but the chief risk officer needs to ensure that all risks to the organisation are understood, managed and, when required, communicated.

5.3.2 **Recommendation 2:** Expand the scope of business continuity in those UN agencies where it currently resides in the domain of information technology, or has not yet been comprehensively implemented across the organisation

According to the findings of this study, the majority of the UN Funds and Programmes have not yet implemented business continuity comprehensively across their agency, and in two agencies it still remains in the domain of information technology. The recommendation is for all UN agencies to expand the scope of their business continuity management programme to cover the entire organisation and to expand its focus beyond disaster recovery of information technology systems. The business continuity programme should also span across the UN agency, both at headquarters and at country level. The business continuity programme must match and directly support the agency's strategy and goals, focusing on identifying critical business processes and developing appropriate recovery strategies. The starting point for UN agencies to establish a business continuity programme is to develop a policy outlining the basic principles and framework and to specifically: (1) identify situations that may cause disruption of critical processes; (2) identify maximum outage times given the strategic, stakeholder or financial impact that this situation might cause; (3) outline the governance structure; and (4) provide guidelines for developing recovery strategies.

UN agencies should also adopt a risk management approach to their business continuity management programmes. Instead of focusing on the organisation as a whole, they should start off by identifying individual business units within the agency that provide critical functions to the organisation as a whole, such as finance, human resources and information technology. Once these departments have been selected, identify the individual business processes performed by each unit and rank them in order of priority, based on the amount of time a business process can be disrupted before the impact reaches a point where the consequences to the organisation reach a significant strategic, reputational or financial level. The period of disruption may vary from one agency to the next, based on their individual needs. The strategies considered for recovering the impacted business processes should focus on reducing the likelihood of disruption, shorten the period of disruption, and limit the impact of disruption on the UN agency's critical processes. It is also proposed that instead of developing a contingency plan for each possible crisis event, UN agencies develop contingencies for one or a combination of the following three scenarios: unavailability of the location where the processes are performed; unavailability of the IT infrastructure to perform the processes; and unavailability of the required staff to perform the processes.

5.3.3 **Recommendation 3:** Establish a comprehensive crisis management framework spanning across the whole organisation, from headquarters to country offices

The findings of this study indicated that, although the responsibility for responding to incidents is decentralised to the office closest to the origin of the incident, in most cases the UN agencies do not have an organisation-wide crisis management framework which could be activated to respond to incidents and coordinate the recovery of business operations across the UN agency. To address this shortfall it is recommended that all UN Funds and Programmes establish a comprehensive crisis management response framework spanning across the whole organisation, from headquarters to country offices. The structure must be designed to respond to a broad spectrum of incidents, including those that arise from risks related to security, pandemic outbreaks, information technology, and facilities. The structure should be modular, scalable and empower managers closest to the incident to take charge, but include the ability to escalate it to a higher level if the scope of the incident increases or additional support is required to deal with it. Functions need to be clearly delineated and decision-making authority should be well defined.

According to the findings of this study, the top priority should be the safety of UN agency personnel and dependents, followed by the recovery of facilities, systems and restoration of normal business activities as soon as feasible. The structure should therefore include the capability to respond to incidents as well as managing strategies for recovering disrupted business operations. In order to implement this recommendation, the membership of individual crisis management teams should be agency specific, but the following functions should be included:

- Security responsible for all tactical operations concerning the life and safety of staff and the protection of the agency's assets.
- Facilities responsible for addressing real-estate issues that may have been affected in the incident, related to offices, warehouses and other types of real-estate that the UN agency may need to function.
- Information technology responsible for the recovery and continuity of critical systems and infrastructure.
- Human resources responsible for accounting for all staff involved in an incident and coordinating all medical support.
- Logistics responsible for all logistical support required by the crisis management team and additional support in response to the incident.
- Finance responsible for monitoring and documenting all costs and providing the necessary financial support relating to the incident.
- Communications responsible for developing and issuing communications regarding the incident, both internally to staff and externally to the media, clients and other stakeholders.
- Business units responsible for the implementing of recovery strategies for the continuation of the identified time-critical business processes.

In addition to establishing the crisis response management structure, there should be an exercise annually to allow the members of the various teams to work together and make decisions that are likely to be outside their normal experience and roles.

5.4 RECOMMENDATIONS FOR STRENGTHENING SECURITY RISK MANAGEMENT AND BUSINESS CONTINUITY PROCESSES AND OVERSIGHT

5.4.1 **Recommendation 4:** Develop the capacity to gather risk data across the agency and aggregate it to view the full spectrum of risks, including security risks and business continuity risks in a holistic manner

The research concluded that all risk management practice areas, such as security risk management, business continuity management and crisis response management are not fully integrated within each of the UN Funds and Programmes. Part of the problem is that risks remain siloed and senior managers may only see the risks associated with their department, without ever seeing the full picture of all risks across the organisation and how they may be related or have an impact on each other. In order to overcome this problem, a complete picture of the spectrum of risks needs to be developed and made available to senior management.

It is therefore recommended that UN Funds and Programmes develop the capability to gather risk data throughout the organisation and group the various risks into different practice areas (e.g. strategic, stakeholder, financial and operational) at the institutional level, as was shown in Figure 3. This is an example of how different risks identified by an organisation can be grouped together under various headings. Doing it in this manner will ensure that all risks are consolidated and grouped at a higher level into different risk practice areas. It will further enable the UN agency to prioritise and manage a portfolio of risks rather than responding to individual risks.

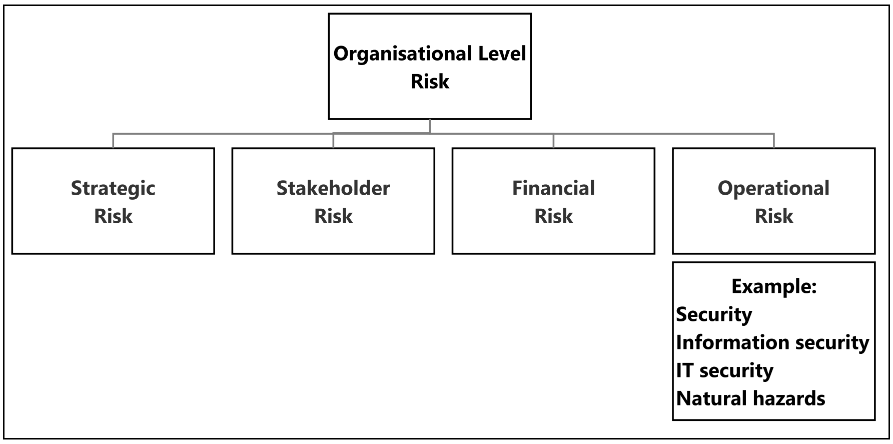
Grouping risks together in this manner is the first step in adopting an integrated risk management approach. Since risks have an impact on the achievement of organisational objectives, this holistic approach will ensure that all risks, including security risks and risks associated with the continuity of operations, are presented to senior management in the context of their impact on the organisation. The risks arise because organisational objectives are pursued against a certain backdrop, which in the UN's case is directly tied to the location and environment where their services are being delivered. This approach also provides a structured process for prioritising and managing the risks instead of dealing with them one by one.

It is further recommended that UN agencies follow the example of financial institutions and create an operational risk category to group those risks, such as security risks and information technology risks that affect business operations under a central heading. As explained in Chapter 3, operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel

Committee on Banking Supervision, 2011). According to the Hong Kong Institute of Bankers (2013:5-7), the sources for operational risks can be traced back to a wide range of events including political issues, legislative issues, criminal acts, employment practices, workplace safety, system factors, damage to assets caused by natural and man-made hazards, and terrorism. Included among the threats are those that also fall under the category of security risks. By grouping them all together under the umbrella of operational risk, it ensures that the risks tied to processes, people, systems and external factors are considered in an integrated manner. The chart in Figure 3 highlighted operational risk as one of the core risk practice areas at the institutional level. In Figure 6 the chart has been expanded to include some of the typical risks that would fall under the operational risk category.

By following this example, UN agencies can group security risks along with other risks, such as information technology and medical risks that would otherwise stand alone, into one governance framework allowing the development of a complete picture of the operational risks the organisation faces, as shown in Figure 6 below. Delineating risks into these different areas also provides a clear demarcation for the scope of the business continuity programme. Business continuity typically focuses on those risks that have an impact on business operations, which are usually found under operational risks. Integrating business continuity and risk management into the same wider framework will also enable UN agencies to develop a better idea of the risks they face, and it should assist in the development of comprehensive response strategies to mitigate the impact of the risks and assist in continuing operations following a disruption.

Figure 6: Organisational level risk practice areas



(Adapted from the Hong Kong Institute of Bankers, 2013:4)

5.4.2 **Recommendation 5:** Integrate security risk management and business continuity management processes to enhance their effectiveness

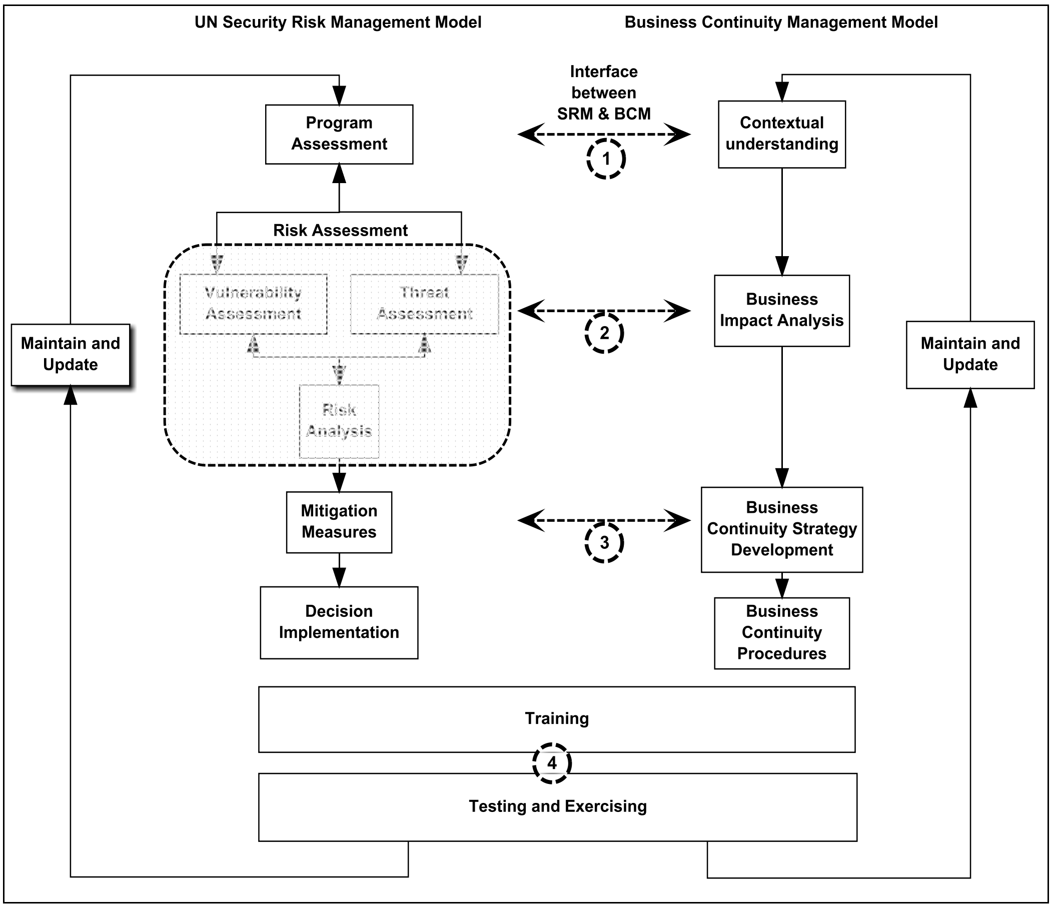
The fifth recommendation relates to the interface between security risk management and business continuity management methodologies. As discussed in the literature review, historically security risk management and business continuity management have been seen as two separate functions, but it was also highlighted that in order to be effective, the two processes need to be closely connected. Risk management, including security risk management, is concerned with the likelihood of an adverse event occurring and the measures to control it, while business continuity focuses on what must be done if the adverse event has indeed occurred and critical business operations are disrupted.

The steps involved in carrying out a risk assessment, implementing the UN Security Risk Management Model and developing a business continuity management plan, were described in detail in Chapter 3. At the onset of the study no evidence could be found to link the UN Security Risk Management Model with the process for developing a business continuity management plan. Based on the findings from the study, it is clear that the resilience of the UN agencies can be enhanced if the two processes are more closely aligned. Through this study the researcher was able to identify the areas where the UN Security Risk Management Model and Business Continuity Management Model should be linked. Figure 7 below depicts the UN Security Risk Management Model and Business Continuity Management Model side by side and highlights the steps, based on the findings from the study, where the two processes interface. Findings from the study support that integrating the two processes in this manner will greatly improve the quality of the outputs and subsequently enhance the resilience of UN agencies.

As mentioned before, the UN Security Risk Management and Business Continuity Management Models were described in detail in Chapter 3, and only the areas where the two processes interface will be highlighted below. In addition to the areas of training and testing, there are three other steps which provide a natural link between the two processes due to the analysis performed during each step, as can be seen in Figure 7. The four steps are identified by the numbers 1, 2, 3 and 4 in the schematic presentation.

The first interface is when both processes start where security and business continuity are put into the context of the organisation and its objectives. The second opportunity is when the business impact analysis is performed. During this step the assessment of security risks plays a role in identifying risks that may impact business operations. The third link is when strategies are developed to mitigate security risks and recover disrupted business operations. The forth area where there is a linkage, can be seen in the steps which cover training and exercising the different plans. Each step is discussed in more detail in the following section.

Figure 7: Linked Security Risk Management Model and Business Continuity Management Model



(Adapted from UNDSS, 2009:2 and Engemann & Henderson, 2012:8)

Interface 1: Programme assessment (security risk management) and contextual understanding (business continuity)

It is evident from the literature that risk management, including security risk management and business continuity management, must form an integral part of the organisation's strategic planning design and management processes. In the findings of the study this was also identified as one of the [apparent] gaps in the UN management processes. Many of the participating agencies identified security risks to their staff and achieving the organisation's objectives as concerns in their respective strategic plans, but this did not always translate into a comprehensive risk management framework in the UN agency. The purpose of the programme assessment within the UN Security Risk Management Model is to analyse the

UN agency's goals and objectives and identify which components of the programme may require security support (UNDSS, 2009:2). The first step in the business continuity model, as explained in Chapter 3, is to establish the context within which the business continuity plan will be developed, taking into account the organisation's strategic objectives and its risk appetite. Both these initial steps establish the foundation on which the rest of the security risk management and business continuity processes are built. From the findings of this study it became clear that these two steps are very similar and can be carried out simultaneously, or the information from the one can be applied by the other.

Interface 2: Risk assessment (security risk management) and business impact analysis (business continuity).

One of the main areas of convergence between the two models as highlighted in this study, lies in the risk assessment and business impact analysis steps. As explained in Chapter 3, within the UN Security Risk Management Model, the sum of the programme, threat and vulnerability assessments provides the context for the operational environment in which the organisation needs to operate. The output of this step provides an understanding of security risks and highlights the probability of a threat from occurring and the impact on the organisation if the threat materialises. The business impact analysis, within the business continuity management model, determines the importance of the business operations by assessing the impact on operations over time in the event that they are disrupted.

While risk assessment and business impact analysis are two separate steps, they should be executed concurrently or in parallel with each other to identify security risks associated with the process and to determine the impact on business operations, if the risks do occur. As explained earlier, if a business activity is only performed in one location by a certain sub-set of staff, the impact on the UN agency, if a security risk materialises, could result in the denial of access to the UN office, the unavailability of IT systems or the unavailability of staff to perform their business operations. In addition to mitigating the security risk, possible solutions to continue operations could include identifying an alternate work location and/or identifying alternate staff to perform the business functions if the primary location, systems and/or personnel were unavailable. This could not be achieved without integrating the security risk assessment and business impact analysis

More specifically, a UN agency operating in a location where violent protests occur regularly, and consequently presents a threat to staff trying to commute to the office, would have to identify alternative ways of conducting business. The staff's absence from the office would affect the UN agency's business operations, but staff being caught up in a demonstration would also be a security risk because it could lead to death or injury. One way to mitigate the security risks is to close the office and allow staff to remain at home during the period of unrest, protecting them from being exposed to a potentially dangerous situation. However, while they are at home their daily work will not be done. Over the short term this many not be major problem, but if they remain home for an extended period of time the disruption could become significant.

Based on the example above, the threat, its impact and the probability of occurring would be identified through the security risk assessment, while the business impact analysis would determine the consequences if business functions were disrupted due to the denial of access to the office. Security's response to the threat is to remove the staff from the risk environment, but from a business continuity perspective, there are business functions that still need to be performed. This analysis would identify business functions that can be delayed and those that cannot. For example, if the demonstration occurred at the end of the month when the payroll for the office staff has to be processed, it would be deemed a time-critical function, and not having access to the office would result in the employees not getting paid. There is therefore a need for interaction between the security risk assessment and the business impact analysis to reach a solution that would aim to reduce the risk to a minimal level, and if it leads to a disruption, ensure that strategies are in place to recover the processes within the identified time.

Interface 3: Mitigation measures (security risk management) and business continuity strategy development (business continuity management).

Security risks are normally addressed by implementing risk mitigation measures that can change the likelihood of the risk taking place or reduce the impact, should the risk materialise. While security measures focus on individual security risks, business continuity response strategies typically follow an “all-hazard” approach. This means that instead of having contingency plans for individual threats, business continuity planning normally focuses on three main scenarios: unavailability of the office location where the processes are performed; unavailability of the IT infrastructure to perform the processes; and unavailability of the required staff to perform the processes. The cause of the threat is not that important; what is important is the impact on business operations. Again the two processes need to complement each other. If security risks are appropriately mitigated, the level of impact on business operations from residual risk will be lower compared to the consequences that may materialise if the risk was not anticipated or not reduced to an acceptable level.

Expanding on the abovementioned example, a thorough analysis of the payroll process would have identified all the steps to be carried out, as well the staff involved, the required IT systems, critical documents and other dependencies, if they exist. Possible strategies to ensure the continuation of processing the payroll could be too: (1) work with security to see if there is a way to safely escort only the staff involved in the payroll process to the office, while other office personnel remain at home; (2) see if the payroll functions can be transferred to another office for a limited time period; and (3) see if it is possible for the payroll staff to perform the necessary steps remotely while working from home. Each one of these scenarios has to be thoroughly analysed and weighed against each other to see what is feasible and what the associated costs are. Moreover, there may be a need for an additional security analysis for each individual scenario. Integrating both security risk analysis and business continuity in this way reduces the risk to the staff and also ensures that the payroll is processed on time.

Interface 4: Training, testing and exercising

The findings of this study highlighted that training and exercising of security and business continuity contingency plans are not regularly carried out. This is a critical component to successfully implement any contingency plan, including business continuity and security risk plans. A holistic approach should be taken when developing training events and exercises for general staff and persons specifically involved in security and business continuity. Staff, and more importantly the members of various crisis management teams throughout the UN agency, need to understand their responsibilities with respect to both security risk management and business continuity, and the roles they play to enhance the overall resilience of the agency. Good crisis management requires that security and business continuity plans have to be exercised at least once a year.

5.5 FURTHER RESEARCH

It is recommended that this research is expanded to compare the way in which the UN agencies deal with risk and business continuity threats, to include other large international organisations working in emergency or conflict situations. These include organisations such as the Global Fund to Fight AIDS, Tuberculosis and Malaria; Save the Children; or World Vision. Another area proposed for further research is to compare the risk management roles and responsibilities of board directors and senior management in private and non-profit organisations.

5.6 VALUE OF THE STUDY

This research set out to identify the relationship between security risk management and business continuity management and to determine how the two methodologies are applied by UN Funds and Programmes. Adapting to the new approach of staying, instead of suspending or terminating their operations in a specific area after an incident, requires these organisations to become more resilient. This can only be achieved through integrating business continuity management and security risk management and aligning these functions with the strategic objectives of the organisation. This study contributes to the existing body of knowledge in the field of risk management by gathering relevant information from participating UN Funds and Programmes, comparing the information with other academic sources and drawing conclusions to answer the research questions. While it is expected that each organisation will have their own view on how to implement security risk management and business continuity management, the findings and recommendations as a result of the study present a series of practical recommendations on how the two functions can operate in an integrated manner in order to increase the overall resilience of UN Funds and Programmes.

Other non-UN organisations working in similar high risk environments could also benefit from the outcomes of the study, as it would allow them to compare their own approaches to security risk management and business continuity management with the information presented in this study.

5.7 CONCLUSION

This chapter analysed the findings from the research study to determine how UN agencies are currently addressing security risk management and business continuity management, and the linkages between the two methodologies. The research confirmed the need for both security risk management and business continuity management. It also highlighted that while they are two separate management functions, both need to be implemented within a larger risk management framework and need to be closely aligned in order to be effective. Through this study, the researcher was able to identify good practices and apparent gaps in how these two methodologies are implemented. The researcher makes five specific recommendations as to how UN agencies can strengthen their resilience by better integrating these two management methodologies and improving their respective processes and oversight. As discussed above, other types of organisations working in high risk environments within humanitarian and emergency situations can also benefit from the outcomes of this study to enhance and strengthen their own resilience.

BIBLIOGRAPHY

Ahtisaari, M. 2003. *The independent panel on the safety and security of UN personnel in Irak.* New York: United Nations.

ASIS International. 2009. *Organizational resiliance: Security, preparedness, and continuity management systems: Requirements with guidance for use.* Alexandria, VA, USA: American National Standards Institute.

Basel Committee on Banking Supervision. 2011. *Principles for the sound management of operational risk.* Basel: Bank for International Settlements.

Brahimi, L. 2008. *Towards a culture of security and accountability: The report of the independent panel on safety and security of UN personnel and premises worldwide.* New York: United Nations.

British Standards Institution. 2011. *Business continuity management and risk management: The role of standards.* London: British Standards Institution.

Broder, J.F. & Tucker, E. 2012. *Risk analysis and the security survey.* 4th edition. Waltham, MA, USA: Butterworth-Heinemann.

Chief Executives Board Secretariat. 2014. *United Nations system.* Available at: http://www.unsceb.org/ (accessed 30 January 2014).

Council on Foreign Relations. 2005. *Comprehensive Peace Agreement (CPA), Sudan.* Available at: http://www.cfr.org/sudan/comprehensive-peace-agreement-cpa-sudan/p8477 (accessed 1 March 2015).

De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grass roots: For the social sciences and human service professions.* 4th edition. Pretoria: Van Schaik.

Doyle, M. 2013. *BBC News - Somalia UN office attack by al-Shabab kills 15.* Available at: http://www.bbc.com/news/world-africa-22965842 (accessed 26 April 2014).

Ehlers, T. & Lazenby, K. 2010. *Strategic management: Southern African concepts and cases.* 3rd edition. Pretoria: Van Schaik.

Engemann, K. & Henderson, D.M. 2012. *Business continuity and risk management: Essentials of organizational resillience.* Brookfield, CT, USA: Rothstein Associates.

Fay, J.J. 2000. *Security dictionary.* Alexandria, VA, USA: ASIS International.

Graham, J. & Kaye, D. 2006. *A risk management approach to business continuity: Aligning business continutity with corporate governance.* Brookfield, CT, USA: Rothstein Associates.

Haimes, Y.Y. 2009. *Risk modeling, assessment and management.* 3rd edition. Hoboken, NJ, USA: John Wiley & Sons.

Hawley, C. 2003. *BBC News - 2003: Attack on UN in Baghdad.* Available at: http://www.bbc.co.uk/news/world-middle-east-14818918 (accessed 26 April 2014).

Hong Kong Institute of Bankers. 2013. *Operational risk management.* Singapore: John Wiley & Sons.

International Committee of the Red Cross. 2013. *Geneva Conventions.* Available at: http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp (accessed 14 February 2014).

International Crisis Group. 2015. *CrisisWatch.* Brussels: International Crisis Group.

International Standards Organisation. 2009. *ISO 31000 Risk management: Principles and guidelines.* Geneva, Switserland: ISO.

International Standards Organisation. 2012. *ISO 22301 Societal security: Business continuity management systems: Requirements.* Geneva, Switserland: ISO.

King Committee on Corporate Governance. 2002. *King Report on corporate governance (King II),* s.l.: The Institute of Directors in Southern Africa.

Kumar, R. 2011. *Research methodology.* 3rd edition. London: SAGE Publications.

Maringa, E. 2015. *UN at country level.* Available at: https://undg.org/home/country-teams/africa-eastern-southern/south-africa/ (accessed 13 February 2015).

McAslan, A. 2011. *Organizational resiliance: Understanding the concept and its application.* Shrivenham, UK: Centre for International Security and Resilience, Cranfield University.

Merriam Webster. 2015. *Merriam Webster - security.* Available at: http://www.merriam-webster.com/dictionary/security (accessed 14 February 2015).

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. 1978. *Belmont Report: Ethical principles and guidelines for the protection of human subjects of research.* Bethesda: Federal Register.

Posta, I. & Wynes, M.D. 2011. *Business continuity in the United Nations system.* Geneva: United Nations.

Reynolds, P. 2003. *BBC News - Why the UN is a target.* Available at: http://news.bbc.co.uk/2/hi/middle_east/3164675.stm (accessed 26 April 2014).

Roper, A.R. 1999. *Risk management for security professionals.* Burlington, MA, USA: Butterworth-Heinemann.

Smit, P., Cronje, G., Brevis, T. & Vrba, M. 2007. *Management principles: A contemporary edition for Africa.* 4th edition. Cape Town: Juta.

South African Reserve Bank. 2013. *South African Reserve Bank: Risk management.* Available at: http://www.resbank.co.za/AboutUs/RiskManagement/Pages/default.aspx (accessed 1 March 2013).

Stoddard, A., Harmer, A. & Ryou, K. 2014. *Aid worker security report.* New York: Humanitarian Outcomes.

Storkey, I. 2011. *Operational risk management and business continuity planning for modern state treasuries.* Washington D.C., USA: International Monetary Fund.

Terzi, C. & Posta, I. 2010. *Review of enterprise risk management in the United Nations system.* New York: United Nations.

The World Bank. 2014. *Fragility, conflict and violence.* Available at: http://go.worldbank.org/BNFOS8V3S0 (accessed 28 April 2014).

UN Secretary General. 2002. *Inter-organizational security measures: framework for accountability for the United Nations field security management system. A/57/365.* Available at: http://www.un.org/ga/acabq/documents/all?type%5B%5D=report&year%5Bvalue%5D%5B%5D=2002&session%5B%5D=57&keys=Inter-organizational+security+measures%3A+framework+for+accountability+for+the+United+Nations+field+security+management+system (accessed 1 November 2014).

United Nations. 2004. *Basic facts about the United Nations.* New York: United Nations Department of Public Information.

United Nations. 2011. *Protecting UN Staff.* Available at: http://www.un.org/en/memorial/security.shtml (accessed 31 January 2014).

United Nations Department of Safety and Security (UNDSS). 2009. *Security management: Security risk management.* New York: United Nations.

United Nations Women. 2014. *UN Women.* Available at: http://www.unwomen.org/en (accessed 1 November 2014).

UN Secretary-General. 2013. Safety and security of humanitarian personnel and protection of United Nations personnel. A/68/489. Available at: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a_68_489.pdf (accessed 1 November 2014).

Welman, C., Kruger, F. and Mitchell, B. 2006. *Research methodology.* 3rd edition. Cape Town: Oxford University Press South Africa.

Whitlock, C. 2007. *Dozens killed in Algiers bombings.* Available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/12/11/AR2007121100276.html (accessed 26 April 2014).

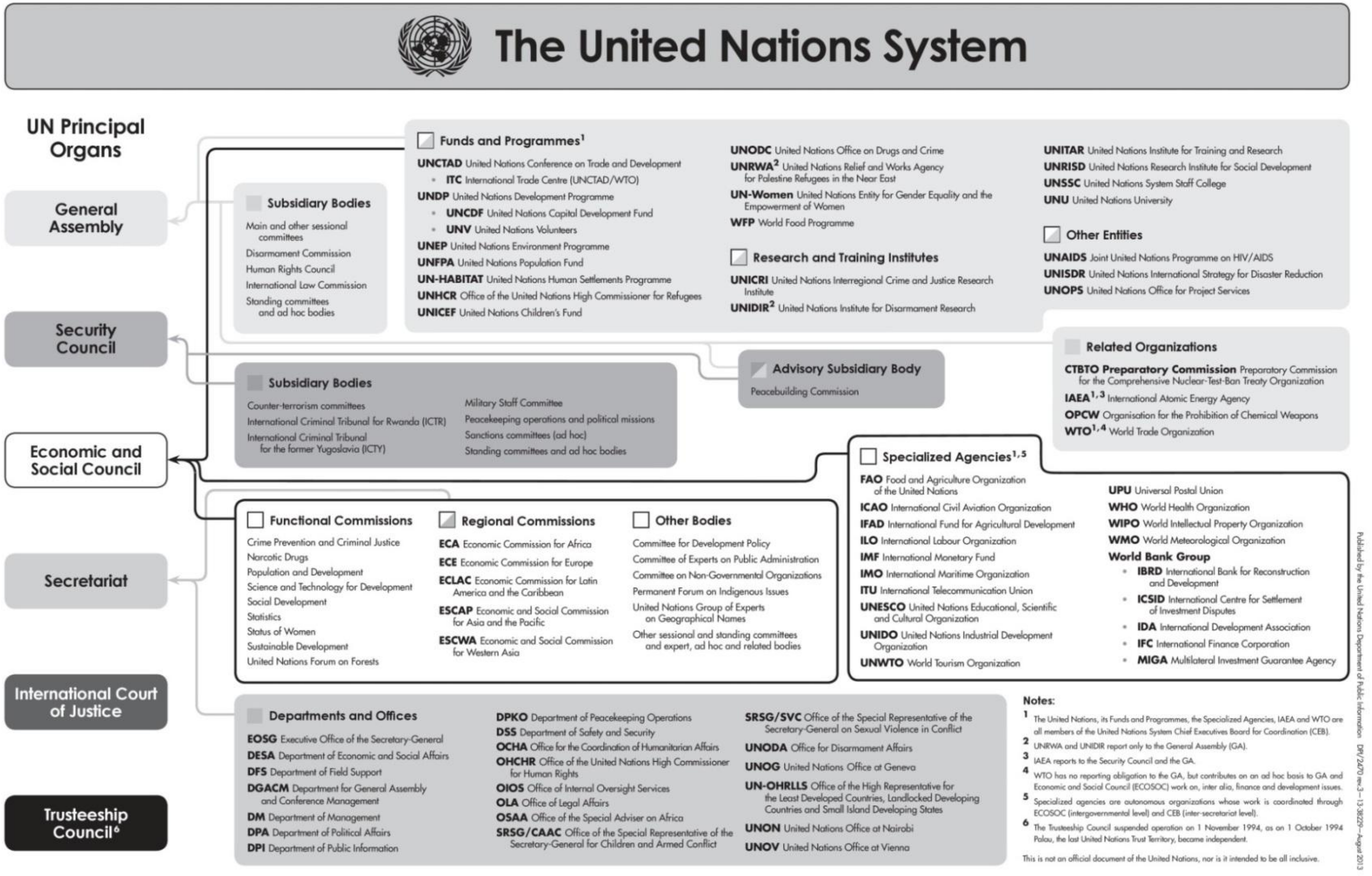
Williams, D. 2011. *Risk management guidelines: Western Australia government.* 2nd edition. Perth: RiskCover Division.

World Bank. 2014. *Fragility, Conflict and Violence*. Available at: *http://go.worldbank.org/ZEPJOFJEW0* (accessed 27 February 2014)

World Economic Forum. 2015. *Global Risks 2015.10th Edition.* Geneva, Switzerland: World Economic Forum.

Yin, R.K. 2011. *Qualitative research from start to finish.* New York: The Guilford Press.

ANNEXURE A: SCHEMATIC LAYOUT OF THE UN SYSTEM



The United Nations System

UN Principal Organs

General Assembly

Security Council

Economic and Social Council

Secretariat

International Court of Justice

Trusteeship Council[6]

Subsidiary Bodies

Main and other sessional committees

Disarmament Commission

Human Rights Council

International Law Commission

Standing committees and ad hoc bodies

Funds and Programmes[1]

UNCTAD United Nations Conference on Trade and Development

- **ITC** International Trade Centre (UNCTAD/WTO)

UNDP United Nations Development Programme

- **UNCDF** United Nations Capital Development Fund
- **UNV** United Nations Volunteers

UNEP United Nations Environment Programme

UNFPA United Nations Population Fund

UN-HABITAT United Nations Human Settlements Programme

UNHCR Office of the United Nations High Commissioner for Refugees

UNICEF United Nations Children's Fund

UNODC United Nations Office on Drugs and Crime

UNRWA[2] United Nations Relief and Works Agency for Palestine Refugees in the Near East

UN-Women United Nations Entity for Gender Equality and the Empowerment of Women

WFP World Food Programme

Research and Training Institutes

UNICRI United Nations Interregional Crime and Justice Research Institute

UNIDIR[2] United Nations Institute for Disarmament Research

UNITAR United Nations Institute for Training and Research

UNRISD United Nations Research Institute for Social Development

UNSSC United Nations System Staff College

UNU United Nations University

Other Entities

UNAIDS Joint United Nations Programme on HIV/AIDS

UNISDR United Nations International Strategy for Disaster Reduction

UNOPS United Nations Office for Project Services

Subsidiary Bodies

Counter-terrorism committees

International Criminal Tribunal for Rwanda (ICTR)

International Criminal Tribunal for the former Yugoslavia (ICTY)

Military Staff Committee

Peacekeeping operations and political missions

Sanctions committees (ad hoc)

Standing committees and ad hoc bodies

Advisory Subsidiary Body

Peacebuilding Commission

Related Organizations

CTBTO Preparatory Commission Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization

IAEA[1,3] International Atomic Energy Agency

OPCW Organisation for the Prohibition of Chemical Weapons

WTO[1,4] World Trade Organization

Specialized Agencies[1,5]

FAO Food and Agriculture Organization of the United Nations

ICAO International Civil Aviation Organization

IFAD International Fund for Agricultural Development

ILO International Labour Organization

IMF International Monetary Fund

IMO International Maritime Organization

ITU International Telecommunication Union

UNESCO United Nations Educational, Scientific and Cultural Organization

UNIDO United Nations Industrial Development Organization

UNWTO World Tourism Organization

UPU Universal Postal Union

WHO World Health Organization

WIPO World Intellectual Property Organization

WMO World Meteorological Organization

World Bank Group

- **IBRD** International Bank for Reconstruction and Development
- **ICSID** International Centre for Settlement of Investment Disputes
- **IDA** International Development Association
- **IFC** International Finance Corporation
- **MIGA** Multilateral Investment Guarantee Agency

Functional Commissions

Crime Prevention and Criminal Justice

Narcotic Drugs

Population and Development

Science and Technology for Development

Social Development

Statistics

Status of Women

Sustainable Development

United Nations Forum on Forests

Regional Commissions

ECA Economic Commission for Africa

ECE Economic Commission for Europe

ECLAC Economic Commission for Latin America and the Caribbean

ESCAP Economic and Social Commission for Asia and the Pacific

ESCWA Economic and Social Commission for Western Asia

Other Bodies

Committee for Development Policy

Committee of Experts on Public Administration

Committee on Non-Governmental Organizations

Permanent Forum on Indigenous Issues

United Nations Group of Experts on Geographical Names

Other sessional and standing committees and expert, ad hoc and related bodies

Departments and Offices

EOSG Executive Office of the Secretary-General

DESA Department of Economic and Social Affairs

DFS Department of Field Support

DGACM Department for General Assembly and Conference Management

DM Department of Management

DPA Department of Political Affairs

DPI Department of Public Information

DPKO Department of Peacekeeping Operations

DSS Department of Safety and Security

OCHA Office for the Coordination of Humanitarian Affairs

OHCHR Office of the United Nations High Commissioner for Human Rights

OIOS Office of Internal Oversight Services

OLA Office of Legal Affairs

OSAA Office of the Special Adviser on Africa

SRSG/CAAC Office of the Special Representative of the Secretary-General for Children and Armed Conflict

SRSG/SVC Office of the Special Representative of the Secretary-General on Sexual Violence in Conflict

UNODA Office for Disarmament Affairs

UNOG United Nations Office at Geneva

UN-OHRLLS Office of the High Representative for the Least Developed Countries, Landlocked Developing Countries and Small Island Developing States

UNON United Nations Office at Nairobi

UNOV United Nations Office at Vienna

Notes:

[1] The United Nations, its Funds and Programmes, the Specialized Agencies, IAEA and WTO are all members of the United Nations System Chief Executives Board for Coordination (CEB).

[2] UNRWA and UNIDIR report only to the General Assembly (GA).

[3] IAEA reports to the Security Council and the GA.

[4] WTO has no reporting obligation to the GA, but contributes on an ad hoc basis to GA and Economic and Social Council (ECOSOC) work on, inter alia, finance and development issues.

[5] Specialized agencies are autonomous organizations whose work is coordinated through ECOSOC (intergovernmental level) and CEB (inter-secretariat level).

[6] The Trusteeship Council suspended operation on 1 November 1994, as on 1 October 1994 Palau, the last United Nations Trust Territory, became independent.

This is not an official document of the United Nations, nor is it intended to be all inclusive.

Published by the United Nations Department of Public Information DPI/2470 rev.3—13-38229—August 2013

(Chief Executives Board Secretariat, 2014)

ANNEXURE B: INFORMED CONSENT LETTER

Affiliation: University of South Africa (UNISA)

Researcher: JJ van der Merwe

Study Title: AN ANALYSIS OF THE RELATIONSHIP BETWEEN SECURITY RISK MANAGEMENT AND BUSINESS CONTINUITY MANAGEMENT: A CASE STUDY OF THE UNITED NATIONS FUNDS AND PROGRAMMES

Purpose of study: The goal of this research is to investigate the relationship between security risk management and business continuity management and how these two methodologies are applied by the UN Funds and Programmes to enhance their own resilience.

Procedures: Due to the wide distribution of participants globally, the data for this research will be collected through telephonic interviews. A semi-structured interview will be conducted with each participant. The interview should not take longer than 45 minutes to complete. Interviews will be arranged with each participant once the consent form is received by the researcher. Please see Annex 1 for the main questions that will be asked.

Risks and discomforts: Where participants feel uncomfortable answering a specific question they may decline if he/she so wishes. Respondents will have the opportunity to ask for clarification if a particular question is not fully understood.

Benefits: It is my hope that participants partaking in this study will feel the satisfaction of contributing to developing best practices in this field. These best practices will then enable the researcher to make recommendations as to how security risk management and business continuity management can operate in an integrated manner with the goal of increasing the overall resilience of UN Funds and Programmes.

Respondent's rights: Participation in this study is voluntary and may be withdrawn at any time without negative consequences for the respondent. All information is treated as confidential and anonymity is assured by the researcher. The data shall be destroyed should the respondent wish to withdraw. The researcher and his study leader are the only individuals who will have access to raw data from the survey questionnaire, and hereby ensure that data will be treated as stipulated above.

Right of access to researcher: Participants are free to contact the researcher at Johan.vdMerwe@gmail.com in connection with the study, if they so wish.

Thank you for your participation in this study.

I, the undersigned, agree to participate in this study voluntarily without duress.

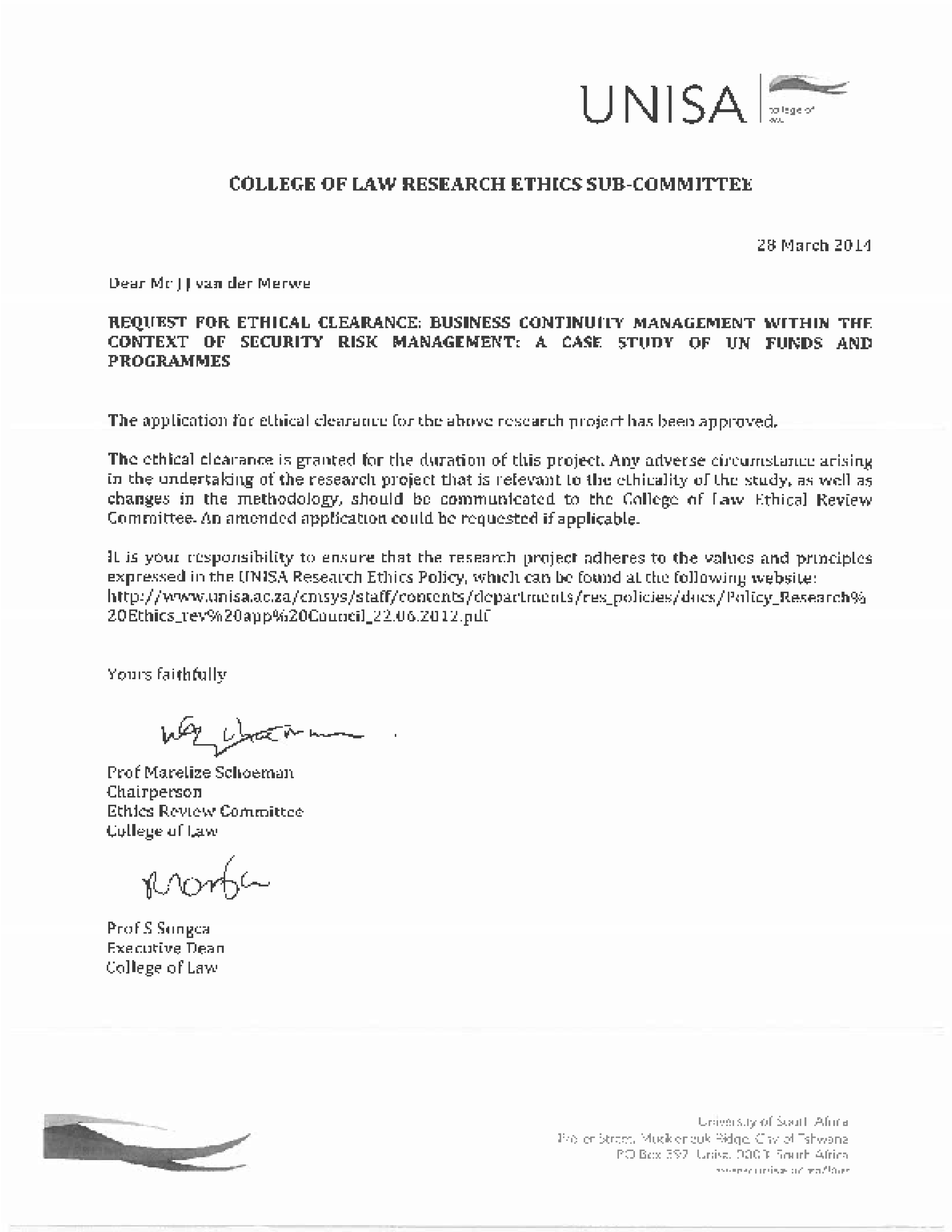
Signed at …………………………….on this…..day of ………………………20…….

……………………………………… ………………………………..

(Print name…………………………)

Organisation: _______________________

ANNEXURE C: ETHICAL CLEARANCE LETTER



UNISA

COLLEGE OF LAW RESEARCH ETHICS SUB-COMMITTEE

28 March 2014

Dear Mr J J van der Merwe

REQUEST FOR ETHICAL CLEARANCE: BUSINESS CONTINUITY MANAGEMENT WITHIN THE CONTEXT OF SECURITY RISK MANAGEMENT: A CASE STUDY OF UN FUNDS AND PROGRAMMES

The application for ethical clearance for the above research project has been approved.

The ethical clearance is granted for the duration of this project. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated to the College of Law Ethical Review Committee. An amended application could be requested if applicable.

It is your responsibility to ensure that the research project adheres to the values and principles expressed in the UNISA Research Ethics Policy, which can be found at the following website:
http://www.unisa.ac.za/cmsys/staff/contents/departments/res_policies/docs/Policy_Research%20Ethics_rev%20app%20Council_22.06.2012.pdf

Yours faithfully

Prof Marelize Schoeman
Chairperson
Ethics Review Committee
College of Law

Prof S Songca
Executive Dean
College of Law

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 Unisa 0003 South Africa
www.unisa.ac.za/law

ANNEXURE D: SEMI-STRUCTURED INTERVIEW QUESTIONS

SEMI-STRUCTURED INTERVIEW QUESTIONS

1. Security risk management
   a. Can you please summarise how your agency manages its security risks? What are the principles and methodologies that underlie your security risk management approach?
   b. What are the most predominant security risks faced by the organisation?
2. Business continuity management
   a. Does your agency have a business continuity programme? Can you please explain it to me?
   b. Where do security risk management and business continuity management functions sit organisationally. What are the reporting lines and areas where they interact?
   c. To what extent are security risk management and business continuity management processes and oversight integrated? Are the outputs from security risk assessments considered as inputs into the business impact analysis, and if so, how?
   d. To what extent are business continuity programmes implemented in offices away from the headquarter locations?