AN EXPLORATION OF RADIOACTIVE SOURCES SECURITY AWARENESS: A CASE STUDY OF FIVE HEALTHCARE FACILITIES IN GAUTENG, SOUTH AFRICA

By

Mafihla Johannes Maleka

Submitted in accordance with the requirements of

MASTER OF ARTS

In

Security Management
School of Criminal Justice

College of Law

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Mrs NP Msimang

CO-SUPERVISOR: Professor SK Jansen van Rensburg

31 JANUARY 2023

DECLARATION

Name: Mafihla Johannes Maleka

Student number: 3687-803-0

Degree: Masters in Security Management

AN EXPLORATION OF RADIOACTIVE SOURCES SECURITY AWARENESS: A CASE STUDY OF FIVE HEALTHCARE FACILITIES IN GAUTENG, SOUTH AFRICA

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references. I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality. I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

MJ Maleka **27 September 2023**

_____ _____

Signature **DATE**

ABSTRACT

The purpose of the research was to explore the level of knowledge regarding radioactive source security that is present among security personnel at healthcare facilities located in the province of Gauteng in South Africa. The level of awareness of radioactive source security that was anticipated among security personnel who work at various healthcare facilities was the focus of the study. The 15 participants who took part in the study were all employed in healthcare facilities registered with the Private Security Industry Regulatory Authority (PSiRA), worked on the level of Grade B security officers or higher and had previous experience in supervisory roles.

A qualitative approach was adopted to research and incorporate case studies to achieve the aim and objectives of the study. Five hospitals in Gauteng, South Africa, were used as case studies. Three security professionals from each hospital made up the unit of analysis in the study. These participants were selected because they were responsible for safety and security at the healthcare facilities. Empirical data were collected through semi-structured interviews that were conducted either in person or over the phone. Data were analysed thematically, and the criteria for assessing the quality of the research were thoroughly addressed. Furthermore, the study adhered to ethical guidelines and was ethically endorsed.

The main findings of the study revealed a significant dearth of knowledge regarding radioactive source security among security personnel. While the participants were aware of the radiology departments at their facilities, they were unaware of radioactive source security. Moreover, the research participants were not able to recall whether radioactive sources are mentioned in both disaster management and security policy. The participants were not trained on the subject under study and were unaware of training opportunities, which has significant implications for radioactive source security at the facilities. The aim of the study was achieved, in that the level of awareness of radioactive source security among security personnel at healthcare facilities was determined. Recommendations based on the findings of the study are detailed for healthcare facilities and security professionals. Furthermore, recommendations for future scientific advancement in respect of radioactive source security at healthcare facilities are proposed.

Keywords: healthcare facilities, nuclear security, radioactive sources, security awareness, security measures

KGUTSUFATSO

Sepheo sa patlisiso e ne e le ho batlisisa ka boemo ba tsebo eo basebetsi ba tshireletso dibakeng tsa tlhokomelo ya bophelo tse porovenseng ya Gauteng Aforika Borwa, ba nang le yona mabapi le mehato e leng teng ya tshireletso ya mohlodi o fanang ka eneji. Boemo ba tlhokomediso ya mehato ya tshireletso ya mohlodi o fanang ka eneji, bo neng bo lebelletswe basebetsing ba tshireletso ba sebetsang dibakeng tse fapaneng tsa tlhokomelo ya bophelo e ne e le ntlha ya sehlooho ya phuputso ena. Bankakarolo ba 15 ba bileng le seabo kaofela ha bona ba ne ba hirilwe dibakeng tsa tlhokomelo ya bophelo tse ngodisitsweng le Private Security Industry Regulatory Authority (PSiRA), ba ne ba sebetsa boemong ba diofisiri tsa tshireletso tsa Mophato wa B kapa bo hodingwana mme ba na le boiphihlelo boo ba tlang le bona ba ho bapala karolo ya bookamedi.

Ho sebedisitswe mokgwa wa ho bokella le ho hlopholla datha eo e seng ya dipalo ho batlisisa le ho kenyeletsa dipatlisiso tse kenelletseng tsa diketsahalo tse itseng ho fihlela sepheo le mehato e totobetseng ya ho fihlela sepheo seo. Dipetlele tse hlano tsa Gauteng, Aforika Borwa, di sebedisitswe e le dibaka tse etswang dipatlisiso tse kenelletseng tsa diketsahalo tse amehang. Basebetsi ba bararo ba nang le bokgoni bo hlokehang ba tswang sepetlele se seng le se seng ba sebetsa e le yuniti ya tlhahlobo phuputsong. Bankakarolo bana ba kgethilwe hobane ba ne ba jara boikarabelo ba polokeho le tshireletso dibakeng tsa tlhokomelo ya bophelo. Datha ya lesedi le itshetlehileng diketsahalong tse bileng teng le maemong a behilweng leihlo e bokelletswe ka diinthaviu tsa dipotso tse hlophisitsweng le tse sa hlophiswang tse tshwaretsweng mohaleng kapa ka ho kopana le bankakarolo ka seqo. Datha e hlahlobilwe ho ya ka mookotaba wa phuputso, mme mokgwa wa ho lekola boemo ba patlisiso o hlophisitswe ka hloko. Ho feta moo, phuputso e entswe ho ya ka ditataiso tsa metheo e amohelehang ya boitshwaro le ho amohelwa ho ya ka melawana e laolang kamoo ho sebetswang ka teng..

Lesedi le ka sehloohong le fumanweng la phuputso le bontshitse hore basebetsi ba tshireletso ba na le kgaello e kgolo ya ho tseba ka mehato ya tshireletso ya mohlodi o fanang ka eneji. Le ha bankakarolo ba ne ba tseba mafapha a radioloji dibakeng tsa bona, ba ne sa tsebe ka mehato ya tshireletso ya mohlodi wa eneji. Ho feta moo, bankakarolo ba patlisiso ba ne ba sa kgone ho hopola hore na mehlodi e fanang ka

eneji e boletswe leanong la taolo le tshireletso ya maemo a koduwa kapa ha e a bolelwa. Bankakarolo ba ne sa rupellwa ka sehlooho se fuputswang mme ba ne sa tsebe ka menyetla ya thupello, e nang le dikameho tse kgolo/bohlokwa mehatong ya tshireletso ya mohlodi o fanang ka eneji dibakeng tse amehang. Sepheo sa phuputso se ile sa fihlelwa, ka hore ho fumanwe hore basebetsi ba tshireletso ba na le tsebo e kae ka mehato ya tshireletso ya mohlodi wa eneji dibakeng tsa tlhokomelo ya bophelo. Ditshisinyo tse itshetlehileng leseding le fumanweng la phuputso di hlaloseditswe dibaka tsa tlhokomelo ya bophelo le basebetsi ba tshireletso ba nang le bokgoni bo itseng. Ho feta moo, ho entswe ditshisinyo tsa ntshetsopele ya nako e tlang e itshetlehileng mekgweng le melaong ya ho etsa dipatlisiso tsa mehato ya tshireletso ya mohlodi wa eneji dibakeng tsa tshireletso.

IQOQA

Inhloso yocwaningo kwakuwukuhlola izinga lolwazi mayelana nokuqashelwa kokulawulwa komthombo wemisebe kubasebenzi bezokuphepha ezikhungweni zokunakekelwa kwempilo ezisesifundazweni saseGauteng eNingizimu Afrika. Ucwaningo lwalugxile ezingeni lokuqwashisa ngokuqashelwa kokulawulwa komthombo wemisebe okwakulindelekile kubasebenzi bezokuphepha abasebenza ezikhungweni zokunakekelwa kwempilo ezihlukahlukene. Ababambiqhaza abayi-15 ababa yingxenye yocwaningo bonke babeqashwe ezikhungweni zokunakekelwa kwempilo ezibhaliswe nePrivate Security Industry Regulatory Authority (iPSiRA). Basebenza ezingeni labasebenzi bezokuphepha beBanga B noma ngaphezulu futhi babenesipiliyoni emisebenzini yokwengamela.

Kwasetshenziswa indlela efanele yokucwaninga kwahlanganiswa nocwaningo olubheke izindawo ezithile ukuze kufezekiswe inhloso nezinjongo zocwaningo. Kwathathwa izibhedlela ezinhlanu eGauteng, eNingizimu Afrika njengezindawo ucwaningo olubheke kuzo. Ochwepheshe abathathu bezokuphepha abavela esibhedlela ngasinye baba yiqoqo elihlaziywayo ocwaningweni. Laba babambiqhaza bakhethwa ngoba kuyibo ababheke ezokuphepha nokuvikeleka ezikhungweni zezempilo. Imininingo yocwaningo olufakazelwe yaqoqwa ngezingxoxo ezihleliwe ezaziqhutshwa siqu noma ngocingo. Imininingo yahlaziywa ngokwezihloko, kwase kubhekwa kabanzi indlela okuyiyo elandelwayo yokuhlola izingabunjalo locwaningo. Ngaphezu kwalokho, ucwaningo lwalandela iziqondiso zenkambo yokulunga futhi lwagunyazwa ngendlela efanele.

Okuqavile okutholakele ocwaningweni kwembula ukuntuleka okukhulu kolwazi lokuqashelwa kokulawulwa komthombo wemisebe kubasebenzi bezokuphepha. Nakuba ababambiqhaza babeyazi iminyango yezemisebe ezikhungweni zabo, babengazi ngokuqashelwa kokulawulwa komthombo wemisebe. Ngaphezu kwalokho, ababambiqhaza bocwaningo abakwazanga ukukhumbula ukuthi imithombo yemisebe yabalulwa yini ekulawulweni kwezinhlekelele nakunqubomgomo yezokuphepha. Ababambiqhaza abazange baqeqeshwe maqondana nocwaningo futhi babengazi ngamathuba okuqeqeshwa, okuthinta kakhulu ukuqashelwa kokulawulwa komthombo wemisebe ezikhungweni. Inhloso yocwaningo yafezeka, ngenxa yokuthi labonakala izinga lokuqwashisa ngokuqashelwa kokulawulwa komthombo wemisebe

kubasebenzi bezokuphepha abasebenza ezikhungweni zokunakekelwa kwempilo. Okunconywayo nokusekelwe kokutholakele ocwaningweni kubalulwe kabanzi ukuze kusizakale izikhungo zokunakekelwa kwempilo nochwepheshe bezokuphepha. Ngaphezu kwalokho, kuphakanyiswa ukuba kube nezincomo zesikhathi esizayo maqondana nokuthuthukisa ezesayensi ngokuphathelene nokuqashelwa kokulawulwa komthombo wemisebe ezikhungweni zezempilo.

DEDICATION

This study is dedicated first and foremost to God, the Father of my Lord and personal Saviour, Jesus Christ of Nazareth, who instilled in me the desire to seek knowledge with everything that I am and everything that I have. Second, this work is dedicated to my late Father, Lerotha Petrus Marakwe, who witnessed me developing and becoming the person I am today long before I began school. He is the impetus for my decision to pursue this qualification. The third person I'd like to thank is my Mother, Anna Mamokete “Sdudla” Moloi, who supported us, her children, through the difficult times following our father's death. Mmangwane, I am very proud of you. The fourth person on this list is my late elder brother, Isaac Manyathi, who took over the family responsibility after my father passed on, your untimely death left us devastated, may your soul rest in peace, Coach. My wife, Popie, and three children, Lerato, Teboho, and Naledi, have all sacrificed 12 years to allow me finish this project. Thanks Popie for your assistance throughout data collection phase, ensuring that I had everything I needed while out in the field; you have been my logistic manager indeed and your support has been phenomenal, to say the least. As for my children, here's to your academic role modelling. It would be a grave mistake on my part not to mention the late Dr Myles Munroe (1954–2014), whose philosophical efforts to discover and maximise one's potential have been an inspiration to me throughout my academic career. When it comes to achieving success in life, he is and will continue to be the person I most admire.

To all my former colleagues at UNISA, and in the security and nuclear industry, the tortoise has finally arrived!

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to the following individuals and entities for their unwavering support throughout this study:

- The late Ms Nomsa Msimang (Supervisor), and Professor Shandré Jansen van Rensburg (Co-supervisor) for believing in me that I have what it takes to complete this study, no matter how challenging it was.
- The South African Nuclear Energy Corporation of South Africa (NECSA): NECSA exposed me to the nuclear sector, which I had no prior knowledge of. Thank you for entrusting me with the responsibility of securing your facilities in the capacity of a physical security manager.
- The World Institute for Nuclear Security (WINS): Without the WINS Academy programme, which certified me as a Certified Nuclear Security Specialised Professional, this study would not have seen the light of day - I will be forever grateful for the sponsorship opportunities that were made available to me in order to complete the entire nuclear security programme and became the first person in the world to achieve this milestone.
- The nuclear industry stakeholders (NNR, PSIF, KPSIF, Nuclear Africa, IAEA) for information sharing.
- The research participants from the healthcare facilities who made up time to slot me into their busy work schedule to be interviewed.
- Mr. Sheperd Moyo a former UNISA colleague who assisted me with academic approaches.
- My colleague at Wits University, Mrs. Prevani Puckaree for her assistance with SmartArt.
- To the Editor, Barbara Shaw, thank you for an outstanding job in editing this dissertation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

^{241}Am	Americium-241
ARS	Acute radiation syndrome
^{252}Cf	Californium-252
CNS	Non-proliferation studies
^{60}Co	Cobalt-60
^{137}Cs	Cesium-137
HEU	High Enriched Uranium
IAEA	International Atomic Energy Agency
ICSRS	International Catalogue of Sealed Radioactive Sources and Devices
IND	Improvised Nuclear Device
^{192}Ir	Iridium-192
ISSPA	International Source Suppliers and Producers Association
^{125}I	Iodine-125
IAEA IPPAS	International Atomic Energy Agency International Physical Protection Advisory Service
ITDB	IAEA Incident and Trafficking Database
KPSIF	Koeberg Public Safety Information Forum
^{85}Kr	Krypton-85
LEU	Low Enriched Uranium
MISS	Minimum Information Security Standards
NATO	North Atlantic Treaty Organisation
NECSA	Nuclear Energy Corporation of South Africa
NNR	National Nuclear Regulator
NRWDI	National Radioactive Waste Disposal Institute
NSS	Nuclear Security Series
NTI	Nuclear Threat Initiative
NTP	Nuclear Technology Products
PAIA	Promotion of Access to Information Act

^{103}Pd	Palladium-103
PPS	Physical Protection System
PSIF	Pelindaba Public Safety Information Forum
PSIRA	Private Security Industry Regulatory Authority
Pu-238	Plutonium-238
Ra-226	Radium-226
RDD	Radiological Dispersion Device
RED	Radiation Emitting Device
^{106}Ru	Ruthenium-106
Se-75	Selenium-75
^{90}Sr	Strontium-90
SASSETA	Safety and Security Sector Education and Training Authority
SAHPRA	South African Health Products Regulatory Authority
S.M.A.R.T.	Specific, Measurable, Attainable, Realistic
TBq	Terabecquerel
Th-232	Thorium-232
UNISA	University of South Africa
U-235	Uranium-235
USA	United States of America
WINS	World Institute for Nuclear Security
WINS BPG	World Institute for Nuclear Security Best Practice Guide
WINS-CPRSSM	World Institute for Nuclear Security Certification Programme in Radioactive Source Security Management
^{169m}Yb	Yterrebium-169

CHAPTER 1
OVERVIEW AND MOTIVATION OF THE STUDY

1.1 INTRODUCTION

This study focused on the security of radioactive sources in healthcare facilities. The purpose of the study was to determine the level of awareness of radioactive sources security among security personnel of these facilities, what they know about radioactive sources, their level of training and awareness of radioactive sources, their awareness of the threat related to radioactive sources and what is being done to address the status quo. Radioactive sources are widely used for a variety of purposes (IAEA Publication 1227, 2005:1). Since most radioactive sources are the product of nuclear, the history and background of nuclear incidents are presented to understand the hazards of nuclear radiation. Radioactive sources produce radiation that can be harmful to humans and the environment if not managed appropriately. Radioactive sources which out of regulatory control are known as “orphan sources” (IAEA Publication 7567, 2007:7). Because of their hazardous nature, radioactive sources must be secured according to prescribed security measures and standards, similar to those used to secure nuclear materials in nuclear facilities and during transportation, to prevent them from falling into the wrong hands and endangering human lives (IAEA Publication 12288, 2018:16).

This chapter addresses the background of radioactive sources, overview of the topic, historical background of the nuclear industry, problem statement, rationale for the study, value of the study, research aims and objectives, research question and sub-questions, key theoretical concepts, and the outline of all chapters. To understand the premise of the study, the significance of the background and an overview of the topic are unpacked.

1.2 BACKGROUND AND OVERVIEW OF THE TOPIC

According to Leavy (2017:46), the choice of topic allows researchers to share their findings with the academic community. In this way, they build a body of knowledge on the topic. Moreover, their study can be extended by acquiring new knowledge or adapting the research methodology. On the other hand, when a topic is under

researched or new, it should be explored in order to fill the knowledge gap (Leavy, 2017:5). The topic of the study was to explore the extent of security awareness of healthcare facilities security personnel in Gauteng, South Africa, regarding radioactive sources. Interest in this topic was stimulated by the radiological incident in Goiania, Brazil, in 1985 (IAEA Publication 3684, 1988:1), the details of which are described in Chapter 3 (see Section 3.10.1.1). Since the Goiania incident occurred in a healthcare facility, the researcher chose to conduct this study at healthcare facilities.

In light of the fact that radioactive sources are a subset of nuclear and emit hazardous radiation, the selection of this topic was motivated by historical nuclear events that had an impact, not only physiologically, but also psychologically, on human beings (Rosoff & Von Winterfeldt, 2007:533).

1.3 HISTORICAL BACKGROUND

A chain of events affected the nuclear industry between 1945 and 2011. These events include the bombing of Hiroshima and Nagasaki (Japan) by the United States of America (USA) during World War II (1945). In 1979, one of the nuclear reactors at Three Mile Island (USA) accidentally melted due to the high temperature. The heat caused a relief valve to fail and shut down the reactor (World Nuclear Association, 2012:np). In 1986, a faulty nuclear reactor in Chernobyl, Ukraine, operated by incompetent personnel, resulted in several people dying from harmful radiation exposure within a few weeks (World Nuclear Association, 2019:np). During the apartheid era in South Africa, a nuclear power plant was bombed by the then-banned African National Congress for political reasons (Public Integrity, 2015:np). According to the IAEA (1988:1), a serious radiological accident occurred in Brazil in which a teletherapy unit containing a radioactive source was left on the grounds of an abandoned hospital. In this accident, 249 people were contaminated, and four people were fatally injured. According to the World Nuclear Association (2018:np), the nuclear accident at Fukushima Daiichi, which occurred in 2011 due to flooding caused by a tsunami, resulted in the explosion of three nuclear reactors, after which residents had to be relocated for fear of harmful radiation and contamination.

The above incidents made the world aware of the dangers of nuclear radiation and its use as a weapon of mass destruction (Fuhrmann & Stulberg, 2013:2). They also

affected people's perceptions of nuclear radiation. Some consider nuclear radiation to be one of the greatest threats to humanity that could end human life (Butler, 2000:xiii). Murray (2001:419) points out that the average citizen is afraid of nuclear radiation because they are not well informed about it. Murray (2001:419) also states that the public also fears that the proliferation of commercial nuclear power plants could lead to nuclear material being diverted from civilian use to nuclear weapons. However, Jagger (1991:159) asserts that the public's fear of nuclear material is based on the belief that radiation emitted from nuclear power plants is dangerous.

The public's fear of nuclear radiation is not unwarranted considering that countries such as the United States, Russia, France, the United Kingdom, China, India, Pakistan, North Korea, and Israel have nuclear weapons (Ferguson & Potter, 2004:47; Tabak, 2009:62). When it became a democratic state, South Africa stopped its nuclear weapons programme and dismantled six nuclear bombs that were developed before 1994 (Fuhrmann & Stulberg, 2013:161).

The presence of radioactive material in any setting and in any form presents both safety and security risks, which need to be mitigated and managed appropriately. The danger posed by radioactive materials is the problem addressed in this study (see Section 3.8).

1.4 PROBLEM STATEMENT

Berg and Lune (2017:33) state that a research endeavour is established by research problems, which in turn drives how the study itself is carried out. The research process is initiated by an idea which is followed by the collection of information.

The security of radioactive sources falls under nuclear security that is a combination of security measures used to safeguard nuclear material. According to the International Atomic Energy Agency (IAEA, 1957:np), nuclear material falls into two categories, nuclear material and other radioactive material. The nuclear material is uranium (U-235 and U-238), plutonium 238 (Pu-238), and thorium 232 (Th-232). Of the three nuclear materials, U-235 is the most commonly used because it is fissionable, meaning it is capable of undergoing a nuclear fission process in a nuclear reactor. A nuclear reactor is a structure in which fissile material undergoes a

controlled, self-sustaining nuclear reaction that results in the release of energy. U-235, i.e., low-enriched uranium (LEU) at 3–5 per cent, is used for domestic purposes, such as electricity generation, while U-235 high enriched uranium (HEU) at 20 per cent or more is used to make nuclear bombs. Nuclear material, in the form of uranium, plutonium and thorium, is not part of this study. This is mentioned only to clarify the background of radioactive material, which in turn generates radioactive sources.

Radioactive sources are a subset of nuclear material. This means that radioactive sources are made from nuclear material or use nuclear material. However, not all radioactive sources are nuclear material. To identify radioactive sources, the IAEA uses two methods. The first is the International Catalogue of Sealed Radioactive Sources and Devices (ICSRS). This catalogue consists of manufacturers' information on sealed radioactive sources and the devices in which they may be used. However, access to the ICSRS catalogue is restricted to IAEA member states and not to the public. The second method for identifying radioactive sources is IAEA Nuclear Security Series (NSS) No. 5 of 2007, which defines how radioactive sources can be identified. IAEA NSS No. 5 is one of the IAEA's nuclear security publications that address the security of radioactive sources. The IAEA is a nuclear-related body established to coordinate and promote the safe and peaceful use of nuclear technologies (IAEA, 1957: np).

Radioactive materials are divided into two categories, namely, enclosed radioactive sources and unenclosed radioactive sources. According to the World Institute for Nuclear Security (WINS) Academy (Enclosed radioactive sources are always sealed in a capsule and are in a solid form (World Institute for Nuclear Security Academy2016a21), 2016a:21). Breaking a capsule to expose a solid form can result in the release of a radioactive substance that could expose people to harmful radiation and contaminate the environment. The IAEA NSS No. 11 (IAEA Publication 8113, 2009) describes uncapped radioactive sources as radioactive substances used peacefully/positively in various applications such as medical applications, e.g., diagnostic procedures and therapeutic nuclear medicine, for scientific research and agriculture, among others.

The security risks associated with radioactive sources stem from their multiple uses by the public, based on their availability, accessibility, size, and portability, which make

them vulnerable to theft. Because of these characteristics, radioactive sources are susceptible to nuclear weapons manufacturing, such as an Improvised Nuclear Device (IND), a Radiological Dispersion Device (RDD) or a Radiation Emission Device (RED) (Ferguson & Potter, 2004:3). IND can be described as a device designed to contain radioactive material to either deliver or disseminate harmful radiation to the public (Robinson & Wood, 2009:6). An RDD is a device in which radiological material and explosive material are stored to disperse radiation and contaminate the immediate environment. On the other hand, an RED is a type of equipment that contains radiological material and could be placed in a public place with the intention of releasing/emitting harmful radiation into the environment without the public's knowledge (Robinson & Wood, 2009:6). The purpose of IND, RDD and RED is to cause harm to people. This means that radioactive sources intended to be used for public benefit, e.g., to treat cancer, can be easily stolen and diverted by individuals with malicious intent to harm, injure or even kill people. Overexposure to nuclear radiation has both short- and long-term harmful effects. For example, radiation from radioactive sources can cause burns, amputations, or mutations of certain body parts that are directly exposed to the radiation.

To gain a more comprehensive view of radiological safety risks, it is essential to understand the historical background of past radiological events that shaped public attitudes and thinking toward nuclear radiation. Earlier radiological events provided the basis and motivation for the researcher to conduct this study.

1.5 RATIONALE OF THE STUDY

According to Hammond and Wellington (2021:442), a rationale is an underlying principle or justification for conducting research. The researcher was motivated primarily by the radiological accident that occurred in Goiania in 1987 (IAEA, 1988:np), where a radioactive source was abandoned and ended up in the hands of civilians. This incident played a critical role in raising awareness of the security of radioactive sources, especially those in healthcare facilities.

Radioactive sources are used in healthcare facilities for a variety of reasons, such as a teletherapy device to treat lumps in the bladder, breast, prostate, lung, or brain (WINS BPG 5.8, 2020:5). In the South African context, the research study aimed to

determine the level of knowledge and awareness of healthcare facility security management staff regarding radioactive sources security in their respective facilities. Public knowledge and awareness of radioactive sources security is essential for safety and to prevent radiological events and incidents. As McIlwraith (2022:7) says, statistics on the number and percentage of security incidents in an organisation suggest that internal users are responsible for at least 70 percent and that most of these incidents are due to user error, mishap, and ignorance.

Robinson and Wood (2009:5) summarised the results of the North Atlantic Treaty Organisation's (NATO) advanced research workshop on international approaches to securing radioactive sources against terrorism, held in the United Kingdom in 2005. The findings of the workshop were that “radiological sources are vital, vulnerable, misunderstood, and largely unregulated” (Wood & Robinson, 2009:4), and that there is therefore a need to educate the public about them. The preliminary literature review revealed that there is no formal security training for nuclear or radioactive sources for the public, such as in healthcare facilities, higher education institutions in South Africa, or in the private security industry regulated by the Private Security Industry Regulatory Authority (PSIRA, 2022:np) or the Safety and Security Education and Training Sector Authority (SASSETA, 2022:np). This lack of training for the public presents a challenge to awareness and security in the handling of radioactive sources used in healthcare facilities where radioactive devices, such as teletherapy devices, are used in oncology departments. They are expected to be secured through access control by traditional security officers who are not trained in this and do not know the security risks associated with securing such a device. This does not mean that security officers working in such healthcare facilities are at risk. Radioactive sources are highly regulated and well secured in their units such as teletherapy devices. Security officers will most likely never see a radioactive source, such as Cobalt 60, in their working lives. However, these devices are part of the assets of healthcare facilities and must be protected by security personnel working around the clock in these facilities. Scaglione (2019:43) underscores the importance of security training, noting that it is an important element of an effective security programme. The author adds that a detailed training programme ensures that security personnel understand their role. Such training would result in officers being competent in all aspects of their duties.

The premise of this study argues that well-trained security personnel will be better equipped to make decisions consistent with security operations in healthcare facilities. This premise forms the foundation of the values of this study.

1.6 VALUE OF THE STUDY

This study is intended to contribute to the nuclear industry, particularly to the security of radioactive sources used in public facilities such as healthcare. The results of the study will also contribute to the body of knowledge in the disciplines of criminology and security science. Various private and public entities and government agencies will benefit from this study. South African citizens in general and the security industry will also benefit from this study by becoming better informed about the benefits, hazards, and precautions to take when securing or coming into contact with radioactive sources that are beyond regulatory control. The value of the study is discussed in more detail below:

1.6.1 The value to Government Departments in South Africa

The Department of Health (DoH) (SA, 2022b:np) which regulates the use of radioactive sources in healthcare facilities, the Department of Energy (DoE) (SA, 2022a:np) which is the competent authority for the nuclear industry in South Africa, and the State Security Agency (SA, 2022c:np) which advises on information security, will all benefit from this study because it will provide information about the security risks of radioactive sources. The study will also provide these agencies with information on radioactive source awareness initiatives.

1.6.2 Value to academia

Because academic institutions use radioactive sources for research, these sources are considered to be part of the academic assets that need to be protected (WINS BPG 2.3, 2011:6). In addition, the academic community is one of the stakeholders in the nuclear business and is tasked with the responsibility of advising governments on the necessity of reform and the issues that are faced by the academic community. The findings of this study will serve as a foundation for additional research on radioactive sources security to be conducted by a variety of scientific groups, and for advisory work to be performed by government agencies that are responsible for radioactive

sources security.

1.6.3 Value to healthcare facilities

It is necessary that healthcare security personnel are trained, educated and aware of radioactive sources security at their respective facilities. Providing educational materials to healthcare security personnel for crime prevention helps the hospital to reduce crime, promote personal safety, and situational awareness (Scaglione, 2019:73). Best practices and general guidelines in securing radioactive sources are necessary to ensure the hospital security personnel are aware of what is expected from them regarding the security of radioactive sources. In addition, there is a need for the implementation of a non-counterproductive security programme which consists of best security practices and general guidelines in securing radioactive sources at healthcare facilities.

1.6.4 Certification in radioactive sources security

Another value of the study is that those responsible for radioactive sources should acquire radioactive sources security certification, which falls under nuclear security (see section 1.1). Radioactive sources security requires specialised knowledge and skills. By obtaining these certifications, offered by both the IAEA and WINS, they demonstrate their competence in securing radioactive sources. The researcher has acquired several such certifications from the above institutions and has can attest to the value and need for such certification.

To achieve the values of the study, the research aims and objectives must be established to guide the study, as indicated below.

1.7 RESEARCH AIMS AND OBJECTIVES

According to Brink, Van der Walt, and Van Rensberg (2018:74), the aim and objectives are specific, measurable goals toward which the research is directed. Research objectives are defined as clear, concise, declarative statements phrased in the present tense. An objective usually focuses on one or two variables and states whether they are to be identified, analysed, or described. Mukherjee (2020:4) defines the research objectives as aiming to add to the existing body of knowledge regarding various

activities in the universe. The author also points out that each research objective must generate new concepts or processes and generalise current measures or techniques to expand their scope and modify existing processes to expand their scope. They refer to the action(s) the researcher will take to achieve the goal.

1.7.1 Aim of the study

The aim of this study was to determine the level of awareness of radioactive sources security among security personnel at healthcare facilities.

1.7.2 The objectives of the study

For the researcher to achieve the above aim, the following objectives were developed:

- To determine participants' level of knowledge about radioactive sources security;
- To verify whether the participants were already informed about the security of radioactive sources;
- To determine the general awareness of criminal activity associated with radioactive sources; and
- To determine whether healthcare facilities are working with government security agencies to assess the threat posed by radioactive sources.

For the researcher to achieve the above aim, the following objectives were developed:

1.8 RESEARCH QUESTIONS

Hammond and Wellington (2021:160) note that the research questions summarise what the researcher is trying to find out and provide the direction and framework for the research. Moreover, the research question(s) are the starting point for establishing the research methodology. Research questions should be carefully crafted and designed to give clear direction to what is being done (Greetham, 2021:30). The following research questions guided the study:

1.8.1 Primary research question

- What is the extent of awareness of radioactive sources security in healthcare facilities?

1.8.2 Secondary research questions

- What is the participants' level of knowledge concerning radioactive security?
- To what extent are the participants informed about the security of radioactive sources?
- What is the general awareness of criminal activity associated with radioactive sources?
- How can the findings of the study provide informed recommendations on the security of radioactive sources in healthcare facilities?

In order to provide answers to the research questions, it was necessary to conduct a literature evaluation that is both comprehensive and pertinent.

1.9 REVIEW OF LITERATURE

Machi and McEvoy (2022:5) explain that a literature review is a written argument that supports the study by building a case from credible evidence derived from previous research. The review of the literature is done in the chapter of this dissertation so that the researcher and the reader can become familiar with the content, nature, and extent of radioactive sources security. The review of literature is expanded in Chapter 3.

The following important theoretical topics are discussed in the literature review:

1.10 KEY THEORETICAL CONCEPTS

The purpose of this study was to generate a shared understanding of the concepts that were employed by identifying the theoretical notions (Jain, 2019:80) as follows:

- **Healthcare facilities:** A healthcare facility is any structure used to provide healthcare services or treatment to four or more people at the same time (York & MacAlister, 2015:39). In this study, healthcare facilities refer to selected public hospitals and universities that use radioactive sources for medical applications and research purposes, respectively.
- **Healthcare security:** This refers to the security that applies and is used in healthcare facilities, such as hospitals (Scaglione, 2019:1). Security can also be defined as a system of safeguards that aims to protect physical property and

achieve relative safety for all individuals interacting within the organisation and its environment (Colling & York, 2010:19).

- **Nuclear security:** This is the prevention of, detection of, and response to criminal or intentional unauthorised acts relating to or directed at nuclear material, other radioactive material, associated facilities, or associated activities (IAEA, 2020:22).
- **Physical protection system** (PPS) refers to the integration of people, technology, and processes used to protect assets and facilities against theft, sabotage, and/or other malicious intent (Garcia, 2008:1).
- **Nuclear Material:** Nuclear material refers primarily to uranium, plutonium, and thorium (IAEA, 1957:np).
- **Radioactive Sources:** These are radioactive materials that are permanently enclosed or closely associated in a capsule in solid form that are not exempt from regulatory control (IAEA Publication 1387, 2009:65).

Next, the outline of the dissertation is presented.

1.11 OUTLINE OF THE DISSERTATION

The dissertation's outline details the activities that need to be carried out in order to realise the intended outcome of the research. The following is a list of each of the five chapters that make up this dissertation:

Chapter 1: The overview and the motivation of the study

The history of radioactive sources, which are a subcategory of nuclear material, is broken down and discussed in this chapter. In order to provide a foundation on nuclear concerns, discussions of previous nuclear events are included. The statement of the problem and its historical context are also covered in this chapter. In addition, the value of the study, research objectives, literature review, key concepts, and outline of the study are outlined in this chapter.

Chapter 2: Research methodology

In this chapter, the research approach that was applied during the course of this study

is presented. The research methodology incorporates the research design and the population and sampling, the selection of participants, the unit of analysis, data collection methods, tools used to collect data, and data analysis, which includes thematic analysis. In addition to this, the criteria that are used to define quality are offered with the intention of assuring transferability, credibility, reliability, confirmability, and objectivity. The concerns of informed consent and the participants' freedom to withdraw from the study are discussed in the final section of the chapter, which is devoted to ethical considerations.

Chapter 3: Literature review

The literature review is discussed in this chapter, with a particular emphasis on case studies of incidents involving radioactive sources. First, the researcher makes use of the South African Health Products Regulatory Authority Code of Practice for Industrial Radiography Gamma Radiation to provide detailed precautions that must be taken in order to maintain security of the storage facilities. The researcher makes use of the Code in an effort to determine the security measures that were considered or not considered during the radiological incidents. Second, the researcher makes use of the WINS Security Threat Assessment Scale, which is organised into five distinct levels, in order to evaluate the case studies from a security point of view (Level 0, 1, 2, 3, 4, 5). The second level of this scale, which indicates that management was ineffective, makes recommendations regarding the security measures of radioactive sources that ought to be put into place based on the scale. Insights into the study of security measures of radioactive sources are addressed.

Chapter 4: **Data analysis**

This chapter provides an overview of the research procedure, which includes the method that was utilised to conduct research and the process that was employed to contact study participants. There are two categories that are shown here. The first group, labelled "A", focuses on the biological information of the participants in the research, while the second category, labelled "B", presents the responses that the participants provided in response to the questions. The questions are arranged in accordance with the study's four objectives (see section 1.5.2).

Chapter 5:

This chapter commences with a summary of the empirical findings. Moreover, the achievement of aim and objectives, as a central aspect of the study, is comprehensively discussed. Thereafter, the chapter provides recommendations for healthcare facilities and security professionals based on the theoretical and empirical findings of the study. The limitations of the study are outlined and recommendations for future scientific advancement are proposed.

1.12 Conclusion

The chapter delivered the introduction and problem statement of the phenomenon, radioactive sources. The rationale of the study based on the researcher's motivation in determining the level of public awareness about radioactive sources was clarified. The historical background of nuclear material as a weapon of mass destruction from 1945 to 2011, while also domestically used, was also discussed. The categories of radioactive sources that are used were also clarified. Given the safety and security risks of radioactive sources, and the historical events related to nuclear radiation, the public fear, concerns and scepticisms based on a lack of information about radioactive sources and nuclear material, were highlighted. Both IAEA and WINS publications related to radioactive sources security were cited throughout this chapter, which provided information about how radioactive sources should be secured.

Applicable regulations governing radioactive sources were also mentioned in this chapter. Both the aim and objectives of the study were described, followed by the key concepts of the study. The last portion of the chapter focused on the outline of the dissertation. Chapter 2 of this study focuses on the research methodology.

CHAPTER 2
RESEARCH METHODOLOGY

2.1 INTRODUCTION

Research methodology is defined as a process that provides clarity about the research activity, which is determined by the nature of the problem to be studied. This means that the problem determines the type of methodology to be used to obtain relevant answers for the research (Bairagi & Munot, 2019:23).

The aim of this study was to examine the need for radioactive sources security awareness by healthcare security personnel (see section 1.1). For the purpose of this study, healthcare facilities refer to selected public hospitals in Gauteng, South Africa, that use radioactive sources for research purposes. To achieve this aim, the specific methods used to identify, select and analyse information about the research topic were implemented. Therefore, this chapter on the research design and methodology shows how the research study was carried out and the research procedures used in order to reach its set objectives.

2.2 RESEARCH METHODOLOGY

Research methodology in qualitative studies broadly refers to the methods used to collect, analyse, and examine descriptive data from research participants' written or verbal accounts (Behar-Horenstein, 2018:1339). Research methodology can be further defined as the framework or pathway that contains the research methods, techniques, and strategies that a researcher deems appropriate for investigating a topic or phenomenon (Zimmerman, 2022:281). As a result, this chapter discusses the relevant research and data collection methods that were used during the research process. Research methodology is more than a set of tools used to collect data. It is a method of engaging with the empirical world by seeking to understand participants' views through their own lived experiences (Bogdan, Devault & Taylor, 2016:7).

In this study, the research methodology incorporated the research design, research approach, population and sampling, data analysis and interpretation, and piloting.

2.3 RESEARCH DESIGN

A research design in its broadest sense refers to the plan for the research study. The researcher selects an appropriate option from a set of logical components to draw up a comprehensive strategy for the study. Thus, the research design functions as a logical blueprint that serves as a rational plan that links the research questions, data collection, and analysis process to the stated research questions. The logic of the plan helps to increase the accuracy of a study (Yin, 2016:83). On the other hand, Bairagi and Munot (2019:70) maintain that a research design is a systematic approach that gives direction to solving the research problem in order to achieve the desired results. A research design answers the "how" questions of conducting research and implementing decisions to achieve desired outcomes. It provides direction for the research and is considered a blueprint for the overall framework of the study. This includes, but is not limited to, the nature of the study and the approaches that will be used to gather information. The research design framework includes the following:

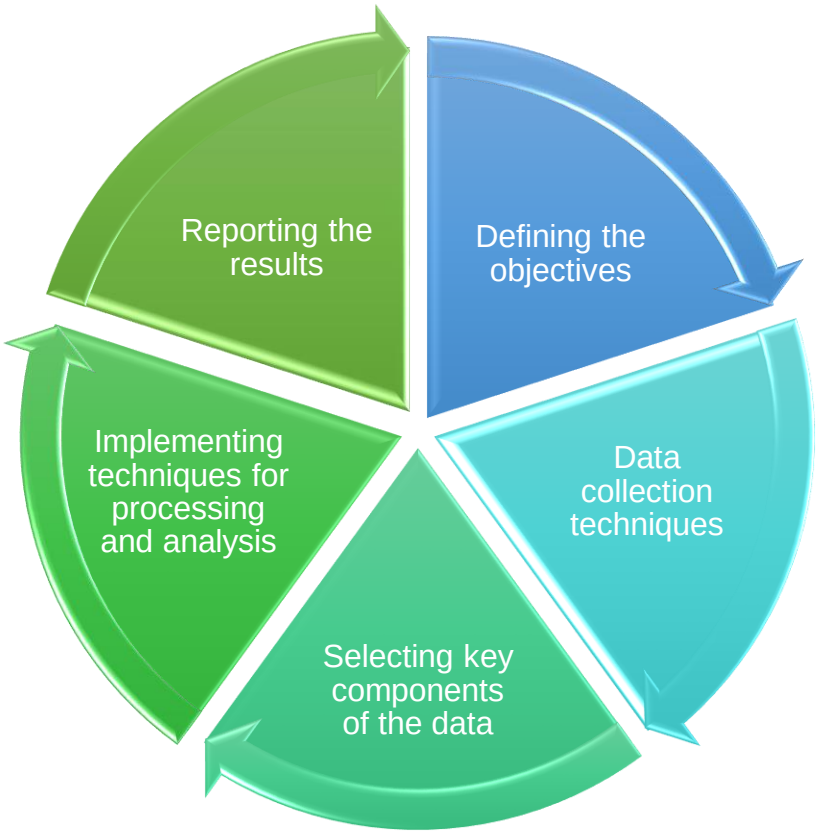

Figure 2.1: Research design

Author's own illustration as adapted from Bairagi and Munot (2019:72)

According to Mukherjee (2020:49), the research design provides for a complete but adaptable structure that includes various activities related to the research method. It considers, among other things, the limits of the study and the characteristics of the study. It also outlines the steps to be taken to conduct the study and specifies how the study will be validated and generalised. Essentially, the research design justifies the evidence that the research purposes, objectives, and questions are met (Cohen, Manion & Morrison, 2018:175).

The objectives of this study were achieved using qualitative research approaches or methods (Bairagi & Munot, 2019:23). This study assumes a case study approach as it focuses on collating data from five public healthcare facilities.

2.4 RESEARCH APPROACH

This study adopted a qualitative approach. Qualitative research can be interpreted as an approach to exploring and understanding the meaning that individuals or groups ascribe to a social or human problem (Creswell, 2014:32). Berg and Lune (2017:12) point out that qualitative research denotes meanings, views, definitions, and representations of things, while Merriam and Tisdell (2016:6) affirm that the goals of qualitative research are to uncover the meaning of an event from people who are involved in it. When conducting a qualitative study, researchers are concerned with discovering how people describe their own experiences, how they construct their world, and the meaning they attach to their experiences. Braun and Clarke (2013:4) offer another explanation, pointing out that qualitative research uses words as data that are collected and analysed in different ways. Rossman and Rallis (2017:38) suggest that qualitative research begins by asking questions for learning purposes and collecting data, such as images, sounds, words and numbers, to answer the question. When the collected data are grouped into patterns, it is called information, and when the information is interpreted and applied, it becomes knowledge. This differs from quantitative studies, which examine the relationship between measured variables to test objective theories. The data from a quantitative study are then statistically analysed to determine the results of the study (Creswell, 2014:45). Qualitative studies are used to determine cause and effect, make predictions, or describe the distribution of a characteristic in a population (Merriam & Tisdell, 2016:5).

2.5 POPULATION AND SAMPLING

The below discussion explains the population and sampling techniques used in this study.

2.5.1 Case study

According to Hammond and Wellington (2021:23), a case study deals with specific units of inquiry and can be understood as a study embedded in a specific context. It provides the researcher with an inductive approach so that he or she can form a holistic picture of a particular case and explain the how and why of a phenomenon. It also allows the researcher to draw on conversations due to its nature of relating to a

specific unit of study. A case study is appropriate for examining a situation by identifying the positive and negative aspects and finally making recommendations. It is useful for getting a detailed overview of a particular case or phenomenon. A phenomenon can be a person, plant, group, process, disease, event, community, or other similar entity (Thomas, 2021:561). In this research, the case study was conducted on five public hospitals in Gauteng Province that use radioactive sources. The selected radiological incidents that have occurred in the past are used as part of the literature review (see sections 3.10.1, 3.10.2, 3.10.4, 3.10.5, 3.10.6). This was done to offer background information that can be used to comprehend the amount of radiological threats to persons and the environment, and to be able to identify the appropriate security measures for safeguarding radioactive sources.

The research approach adopted in this study allowed information to be collected from the selected population and samples to be drawn from the same population.

2.5.2 Population

In research studies, the population represents the total set of objects that are the focus of the study, which may be people, institutions, or events from which an extrapolation is to be drawn (Walliman, 2022:139). The population in this study refers to all the healthcare facilities in Gauteng, South Africa, privy to radioactive sources. However, the researcher did not have the capacity and financial backing to include all these facilities in the study, thus a sample of five facilities was selected.

2.5.3 Sampling design or methods of sampling

Jensen (2021:256) points out that sampling means the selection of entities to be included in or excluded from a study. It is the selection of a subset of a population that characterises the entire population. This subset is selected to replicate the characteristics of the entire population in small numbers (Acharyya & Bhattacharya, 2019:169). The sample consists of a sampling frame that designates the appropriate participants or a specific group of interest for the study (Walliman, 2022:139).

In research, there are two methods of sampling: quantitative and qualitative sampling. Bryant and Charmaz (2019:146) distinguish between quantitative and qualitative sampling by pointing out that quantitative sampling focuses on the population and

relies on random selection to give the population an equal chance of being selected. Qualitative samples, on the other hand, aim to represent the subject of the study based on the researcher's desire to understand the phenomenon. There are two basic types of samples, namely, probability samples and non-probability samples (Bairagi & Munot, 2019:92). Probability sampling (of which simple random sampling is the best-known example) allows the researcher to generalise the results of the study from the sample to the population from which it was drawn. Sampling designs are based on two factors, the basis of representation and the element selection technique. A probability sample has the property that each element in the population has a zero probability of being excluded from the sample. This means that probability sampling gives each element of the population an equal chance of being included in the sample. A non-probability sample is based on a sampling design that does not have this property.

Non-probability sampling does not provide a basis for estimating the probability that each element of the population has the opportunity to be included in the sample. In this study, the author chose a non-probability sample by using purposive and convenient sampling techniques (Patten & Newhart, 2018:115). With this type of sampling, the researcher intentionally selects participants who are most representative of the selected population and are a good source of research information.

To further substantiate purposive sampling, the researcher selected the critical case sample (Acharyya & Bhattacharya, 2019:215; Tavakoli, 2012:508), whose characteristics relate to the element under study and whose study irrefutably decides the research question. The researcher intentionally selected incidents involving radioactive sources that greatly increase the participants' level of knowledge about the security of radioactive sources and determined the nature of the questions to be asked. In addition, a purposive sampling technique was used to achieve even coverage of radioactive sources security (Patton, 2015:475). Finally, when using convenient sampling, the researcher targeted security personnel who are accessible, always at work, and readily available (Tracy, 2020:101). The population and sample guided the researcher in selecting research participants.

2.6 SELECTION OF PARTICIPANTS

Individuals taking part in the research study are called participants, subjects, informants or respondents (Rossman & Rallis 2017:38). Given the nature of this study, which is qualitative, “participant” is the term used to describe individuals who took part in the study. In qualitative research, participants are actively and intentionally selected based on certain characteristics (Bryant & Charmaz, 2019:199) and the method to be used in data generation and collection (Costley & Falton, 2019:233). Three security personnel were purposely selected from five specific healthcare facilities as they are responsible for the safety and security of the healthcare facilities and all assets, including the departments or units where the radioactive sources are stored. Moreover, security personnel are responsible for securing radioactive sources and enforcing prescribed security measures.

The unit of analysis is demarcated below.

2.7 UNIT OF ANALYSIS

Achariyya and Bhattacharyya (2020:184) define a unit of analysis or an observation unit as any entity from which the data or information can potentially be collected. Depending on the research question, the unit may be an individual, a household or part of a household, a business, a school or a hospital (Bachman & Schutt, 2008:104). The participants from whom data are collected are referred to as the unit of analysis. The unit of analysis can also mean "the entire group, the group dynamics, the individual participants, or, usually, the participants' utterances" (Silverman, 2014:309). In other cases, the unit of analysis may also be referred to as the unit of observation, which refers to the thing from which the data are compiled. Five healthcare settings were used to identify the unit of analysis, the security personnel, who were the people selected in the healthcare facilities for data collection. Three security personnel from each facility were selected. The decision to select three participants from each facility was made since the study would be conducted during the day when participants were at work. To ensure that work would be interrupted as little as possible, three participants were selected who were also required to have at least a Grade B (a supervisory level) from the Private Security Industry Regulatory Authority (PSIRA). They were also expected to have at least a grade 10 in school to be able to

communicate in English, as the study was conducted in English. Participants were not discriminated against in terms of gender or ethnicity.

Based on the unit of analysis, a specific method of data collection was used during the interviews.

2.8 DATA COLLECTION METHODS

Data collection methods refer to instruments used to collect data in person (Cohen, et al., 2018:198). In qualitative research, these include semi-structured interviews, observational data, documentary data, and reports. Bairagi and Munot (2019:131) state that an orderly compilation of data allows the researcher to respond to the research questions and correctly evaluate findings. In this study, interviews were used as a data collection method.

Fifteen participants were interviewed. Each participant was asked a total of ten questions which lasted between eight and eighteen minutes. The reason for the different times was that the questions were open-ended, and participants answered according to their level of knowledge about radioactive sources. Participants who answered "No" took less time to participate. English was used as the primary language. However, when participants had difficulty using certain terminology, they were allowed to choose their local language. Participants were interviewed either in their offices, workstations, or any other convenient operational location, considering that the interviews were conducted during operating hours.

2.8.1 Conducting interviews

According to Thomas (2017:337), an interview is a dialogue with a person from whom the interviewer wishes to obtain information. Following Thomas' assertion, Walliman (2022:138) distinguishes three types of interviews: structured interviews, unstructured interviews, and semi-structured interviews:

- **Structured interview:** This type of interview consists of uniformly arranged questions. It does not leave room for flexibility for the interviewee. Structured interviews are occasionally used during fieldwork to supplement the researcher's reflections. This approach is useful in that it gives the researcher more

opportunities to gather additional information (Berg & Lune, 2017:73).

- **Unstructured Interview:** The unstructured interview is also referred to as the "intensive interview" or "in-depth interview" (Yin, 2018:161). It is an accommodative type of interview in which the interviewees are free to respond as they wish.
- **Semi-structured interviews** are the approach "with a predetermined agenda and open-ended questions" (Cohen et al., 2018:199). They are more flexible than structured interviews. In semi-structured interviews, the participant has more latitude to provide information and the interviewer is free to follow up on certain questions or to focus the study more on the topics the researcher deems important to the study. This study used semi-structured interviews. Given the availability of participants and the nature of their work environment, interviews were conducted one on one either by telephone, or via Microsoft Teams. The interviews were carried out in the following ways:

2.8.1.1 In-person interviews

Bachman and Schutt (2018:403) note that an in-person interview is the face-to-face social interaction between the interviewer and the interviewee and has a higher response rate compared to other interview models. In order to have a satisfactory response rate, the researcher opted to drive to the participants' interview places, to deliver the interview questions in order to familiarise himself with the respondents' workplace, distance and to establish a face-to-face rapport with some of the participants before conducting the actual interview. In this study, seven out of ten participants were interviewed in-person. One of the challenges faced by the researcher was delays of participants to avail themselves upon the agreed time, owing to operational reasons. This worked very well as participants, especially the management candidates, ensured that research participants were available as scheduled.

- Telephone interviews

Berg and Lune (2017:78) cite that telephone interviews are an option for data collection and are usually chosen for geographic reasons. To get the best results from telephone interviews, the researcher should have specific questions in mind. One of the reasons for the decision to use telephone interviews was the restriction on

movement due to the Covid-19 pandemic. Most organisations had strict visitor access rules to their premises, and telephone interviewing was a way to communicate with people outside the organisation without entering the participants' premises, so six of fifteen interviews were conducted telephonically. While this method offered the researcher the advantage of being able to interact with participants remotely, it also had its own challenges, one of which was that the researcher was not able to observe the nonverbal cues of the participants. Another challenge with the telephone interviews was that the telephone connection was interrupted during the interviews due to power outages. During this time, either the participant's phone or the researcher's phone was disconnected due to a loss of network connectivity. The recordings had to be paused until connectivity was restored, at which time interviews resumed. Yet another challenge with telephone interviews was that participants were interrupted for operational reasons. Although this occurred occasionally, it was minimal, and interviews could resume after a few minutes. Lastly, a hands-free, office telephone set was used to capture audio through its audible speaker capability. These were all done after informing the participants and gaining their consent.

2.8.2 Procedures during the interview process

The following procedures were undertaken during the interview process.

- Audio recordings

Bordens and Abbott (2018:246) note that audio recordings are used to capture and later analyse more extensive interactions. Durdella (2019:319) points out that participants must be informed about the audio recordings, as they have a right to know that it is taking place, will be stored and used to analyse the data. Biel, Engberg, Ruano and Sosoni (2019:197) point out that one of the advantages of audio recording is to preserve the integrity of the recorded data and to ensure that researchers analyse actual narratives rather than what they remember from the interviews. The researcher used two types of audio recorder instruments (Biel et al., 2019:17), namely, the standard audio recorder and the smartphone voice recorder. The reason for using both instruments at the same time was to have a backup for each instrument in case the other failed.

- Transcriptions

Bryant and Charmaz (2019:196) point out that transcription is the act of translating an oral message into its written form. Biel et al. (2019:103) further indicate that a transcription should be a detailed reproduction of the recorded interaction that accurately reflects such aspects of oral communication such as hesitations, thinking aloud, self-corrections, and dialectal phrasing. Following the audio recordings of the interviews, the researcher listened to the audio recordings multiple times and transcribed the interviews from audio to written format.

Raw data need to be analysed in order to give them meaning.

2.9 DATA ANALYSIS

In data analysis, the researcher describes the step-by-step process used to code the data, identify the categories that emerge, and synthesise and interpret the patterns discovered (Efron & Ravid, 2019:108). In doing so, s/he relies on evidence to support the findings and to increase confidence in the findings. Mukherjee (2020:155) indicates that data analysis requires the cognitive ability to reason logically with facts and figures, to visualise and summarise the data after examining it for relevance, validity, and credibility, to deduce the desired information, and to obtain relevant knowledge from the data by processing them with appropriate qualitative and or quantitative instruments. While conducting this study, data analysis, topics or themes were identified, outlined and categorised.

2.9.1 Thematic analysis

Allen (2017:1756) explains that thematic analysis is conducted to identify recognisable recurring themes, ideas, or patterns in the data that provide insight into communication. This is done to provide a comprehensive understanding of the overall experience of a communication event, series of interactions, or messages in a variety of communication contexts. In this study, themes were generated after recurring patterns were identified from the collected data.

Braun and Clarke (2006:15) concede that thematic analysis involves searching a data set – whether a series of interviews or focus groups or a set of texts – to find recurring

patterns of meaning. This is accomplished through a step-by-step process in which the researcher becomes familiar with the research data, generates codes, identifies a feature of the data that seems interesting to the analyst, searches for themes to focus the analysis on the broader level of themes rather than codes, reviews themes to refine them, identifies the core of what each theme is about, determines the aspect of the data that each theme captures and finally produces the report. Thematic analysis was applied to the study to identify themes within the collected data.

The quality of the data is analysed below.

2.10 CRITERIA FOR ASSESSING QUALITY IN QUALITATIVE RESEARCH

To ensure quality in qualitative research, evaluation methods must be relevant to the context and intentions of the research (Walliman, 2022:8). In research, quality can be achieved through transferability, credibility, dependability, and confirmability.

2.10.1 Transferability

Hammond and Wellington (2021:188) define transferability as the extent to which the results of a study are applicable beyond the scope of the project. It is also used to create an audit trail available to other researchers. Transferability is the way in which the qualitative researcher validates the findings of the research study and their suitability for other contexts. In this case, "other contexts" may mean equivalent circumstances, same populations, parallel phenomena, or beyond the boundaries of the study framework (Given, 2008:886). Thus, transferability refers to the extent to which the findings of qualitative research can be applied to other contexts or settings, meaning that the researcher can transfer the results of the research to other contexts (groups and organisations). In this study, the focus was on the transferability of the recommended measures for securing radioactive sources to the existing measures for securing facilities with the aim of improving them.

2.10.2 Credibility

Credibility is the dependability, plausibility, and integrity of the researcher, which directly affects whether research findings can be believed (Tracy, 2020:289). The degree to which the findings of a research are credible and trustworthy is referred to as

its credibility. Credibility is vital because it ensures that a study's results are legitimate and may be utilised to guide decision-making. It is the methodological procedure and references used to reconcile the participants' expressions and the researcher's view (Given, 2008:138). Credibility is the assurance of the qualitative researcher that the findings of the study are true and accurate. In this study, the researcher used scientifically proven methods to collate data.

2.10.3 Dependability

Dependability indicates the extent to which the study could be repeated by other researchers and the results would be reliable and dependable. In other words, if a person were to attempt to duplicate a study, the information in the research report would be sufficient to do so and produce similar results to the original study. Cohen et al. (2018:271) note that dependability includes member checking, staff interviews, long engagement, and persistent observation in the field. The researcher ensured the dependability of the process by which the research was conducted and documented any methods, approaches, designs, or techniques used.

2.10.4 Confirmability

Confirmability is part of ensuring research quality by reviewing the methods of data collection and analysis (Hammond & Wellington, 2021:50). Confirmability is the step of objectivity in research findings. It means that the findings are based on the responses of the participants and not on possible inclinations or discrete motivations of the researcher. It is associated with reliability and objectivity, which are used to determine the accuracy of the meaning conveyed in the study (Given, 2008:112). Confirmability serves two main purposes, understanding a phenomenon from the perspective of the research participants and understanding the meaning people attach to what they experience. This includes confirming that the researcher's belief does not translate the research participants' views into an account. The researcher ensured confirmability by allowing participants to respond to questions without leading answers and by allowing participants to use their understanding of the phenomenon under study.

2.10.5 Objectivity

Because objectivity is associated with quantitative research, Allen (2017:93) points out that eliminating bias and maintaining the greatest possible objectivity is an important part of academic research (Marcus & Hightower, 2019:102). Hiding bias could lead readers to view the researcher as not objective. To overcome this, the researcher, firstly, made every effort to maintain the objectivity of this study by informing participants that he was aware of their limitations regarding radioactive sources before beginning the interviews. Secondly, the researcher is a certified nuclear security professional who is already aware of these limitations because little is known about radioactive sources security in healthcare facilities. Thirdly, the researcher's preconceptions about the level of knowledge of healthcare facilities security personnel were articulated to the research participants before the interviews began.

During the research process, quality assurance also considered how participants in the study were treated, and any relevant ethical considerations.

2.11 ETHICAL CONSIDERATIONS

Ethical considerations are made when humans or animals are the subject of study. The primary concern is whether the participants will be exposed to any risks and whether or not they are aware of the risks (Thomas, 2021:182). The researcher is expected to take all necessary precautions to meet ethical requirements, such as obtaining the permission to conduct a study. Tracy (2020:270) argues that ethics in research considers procedural, situational, cultural, and relational ethics. Ethical considerations are one of the most important parts of academic research. Cohen et al. (2018:463) believe that the context and nature of the study should influence the ethical considerations. In this study, the researcher followed the ethical considerations prescribed by University of South Africa Ethics Committee, where this research was conducted, and the general ethical considerations required in academic practice.

2.11.1 Informed consent

Hammond and Wellington (2021:165) postulate that obtaining consent is part of the ethical considerations of research. It includes the manner in which individuals are treated and the integrity with which data will be analysed and reported. Given

(2008:128) emphasises that qualitative researchers must adhere to institutional processes related to informed consent. The researcher ensured that participants were fully informed about the research process and gave consent to participate in the research before data collection took place. This means that participants were educated about the details of the research and voluntarily participated in the research (Bordens & Abbott, 2018:200). The researcher ensured that participants were informed of their right to withdraw whenever they wished prior to conducting the interview as explained in the informed consent form (see Annexure A).

2.11.2 Right to withdraw

The right to withdraw is outlined in the consent form of participants in a research project (Acharyya & Bhattacharya, 2019:168). The researcher should ensure that participants feel free to withdraw from participation in the study without consequences. It is also imperative that participants are not coerced or persuaded to participate in the study (Costley & Fulton, 2019:81). In this study, the researcher informed and educated participants, both verbally and in writing, of their right to withdraw from participation at any time (Tracy, 2020:89; Cohen et al., 2018:142). However, none of the participants requested to withdraw from the study.

2.11.3 Guarantee of confidentiality

Protecting the privacy and confidentiality of participants' data should be the researcher's priority. Participation of participants should not, under any circumstances, result in participants having unknowingly or unwittingly consented to participate in another study, whether now or in future research efforts (Yin, 2018:126). The researcher should keep all information about participants obtained during the research process confidential. Confidentiality refers not only to the participants, but also to their organisations or institutions, third parties, or other individuals who were involved in the study (Creswell & Poth, 2018:300). In this study, the researcher followed institutional policies and protocols by intentionally removing any form of the participants' identities from the research documents (Berg & Lune, 2017:48). In addition, the researcher used generic terminology when referring to the institutions where the research was conducted to preserve their anonymity and the participants' responses (Bordens & Abbot, 2018:210).

2.11.4 Potential harm

Bordens and Abbot (2018:203) point out that, in ethical research, the researcher must ensure that the welfare of the participants is protected by not causing harm to the participants. This is referred to as beneficence. The researcher is also aware that unethical research practices can have a negative impact on the public's trust in the results of the research and the credibility of the researcher (Bordens & Abbot, 2018:218). Therefore, the purpose of the research is expected to benefit the individual and reduce the risk of harm to participants (Costley & Fulton, 2019:78). Because of these precautions, the researcher took reasonable steps to uphold the non-maleficence principle, i.e., to ensure that participants were not harmed in any way by their participation in this study by following conventional research procedures during the research process (Costly & Fulton, 2019:80).

2.12 CONCLUSION

This chapter provided an overview of the research methodology followed in the study. First, it defined research methodology and research design and the role they play in guiding the research problem. Based on the design of the study, this study took an exploratory approach based on the researcher's assumption that the respondents knew little about the topic being discussed, which is the participants' knowledge of radioactive sources security in the healthcare facilities where they work. The qualitative research approach was also stated since the study was about meanings, views, definitions, and how things are represented, rather than numbers or figures. The population and sample were also addressed. The researcher explained the reasons for choosing non-probability sampling and purposive sampling for this study. Another aspect that was considered was the selection of participants, namely, where the participants were selected and why they were selected. Then the unit of analysis and the method of data collection was mentioned and defined in detail. To ensure that the study met the required research standards, the elements of the criteria were outlined and discussed. Finally, ethical considerations were made and detailed to ensure the ethical validity of the study.

CHAPTER 3
LITERATURE REVIEW

3.1 INTRODUCTION

Machi and McEvoy (2022:5) define a literature review as a written argument that supports a dissertation by building a case from credible evidence drawn from previous research. It also provides context and background to the current state of knowledge of the subject and presents a logical case to defend the conclusions it draws. In this chapter, the researcher explores the life cycle of radioactive sources, associated activities, and past radiological incidents. Secondly, the chapter focuses on reviewing selected past events related to the loss of radioactive sources in storage facilities and during transportation, with emphasis on appropriate security measures and processes to prevent unauthorised source removal, as specified in the International Atomic Energy Agency Management of Disused Sealed Radioactive Sources (IAEA NW-T-1.3, 2014a:53).

To understand the security of radioactive sources, the process called the "radioactive source life cycle" is reviewed first.

3.2 THE LIFECYCLE OF RADIOACTIVE SOURCES

Both nuclear material and radioactive sources have a specific lifetime. Nuclear material (especially uranium) has a life cycle known as the “nuclear fuel cycle” consisting of various stages known as mining, milling, conversion, enrichment, fuel fabrication, power generation, spent fuel storage, and final disposal (World Nuclear Association, 2021:np). The nuclear material that forms the process from mining to power generation is known as the front end, while the process from spent fuel to storage is known as the back end. In other words, the front-end is primarily raw nuclear material and less radioactive, while the back-end nuclear material is processed nuclear material that is highly radioactive (World Nuclear Association, 2021:np).

The life cycle of radioactive sources includes the process by which radioactive sources are produced, manufactured, distributed, installed and commissioned, used, stored, maintained, recycled, decommissioned, conditioned for storage and disposal, stored, and disposed of (IAEA, NW-T-1.3, 2014a:45). The primary focus of this chapter is on

the security of radioactive sources during storage, whether in storage or in transport. These are reviewed in accordance with the Code of Practice for Industrial Radiography - Gamma Radiography (South African Health Products Regulatory Authority [SAHPRA], 2010:7) issued by the South African Health Products Regulatory Authority (SAHPRA). Although not all radioactive sources are gamma-based, the code is used as a general guideline for radioactive sources security. Because of their inherent hazard, i.e., harmful radiation, various stakeholders are legally responsible for the management and safekeeping of radioactive sources.

The following figure shows the life cycle of radioactive sources (IAEA NW-T-1.3, 2014a:45).

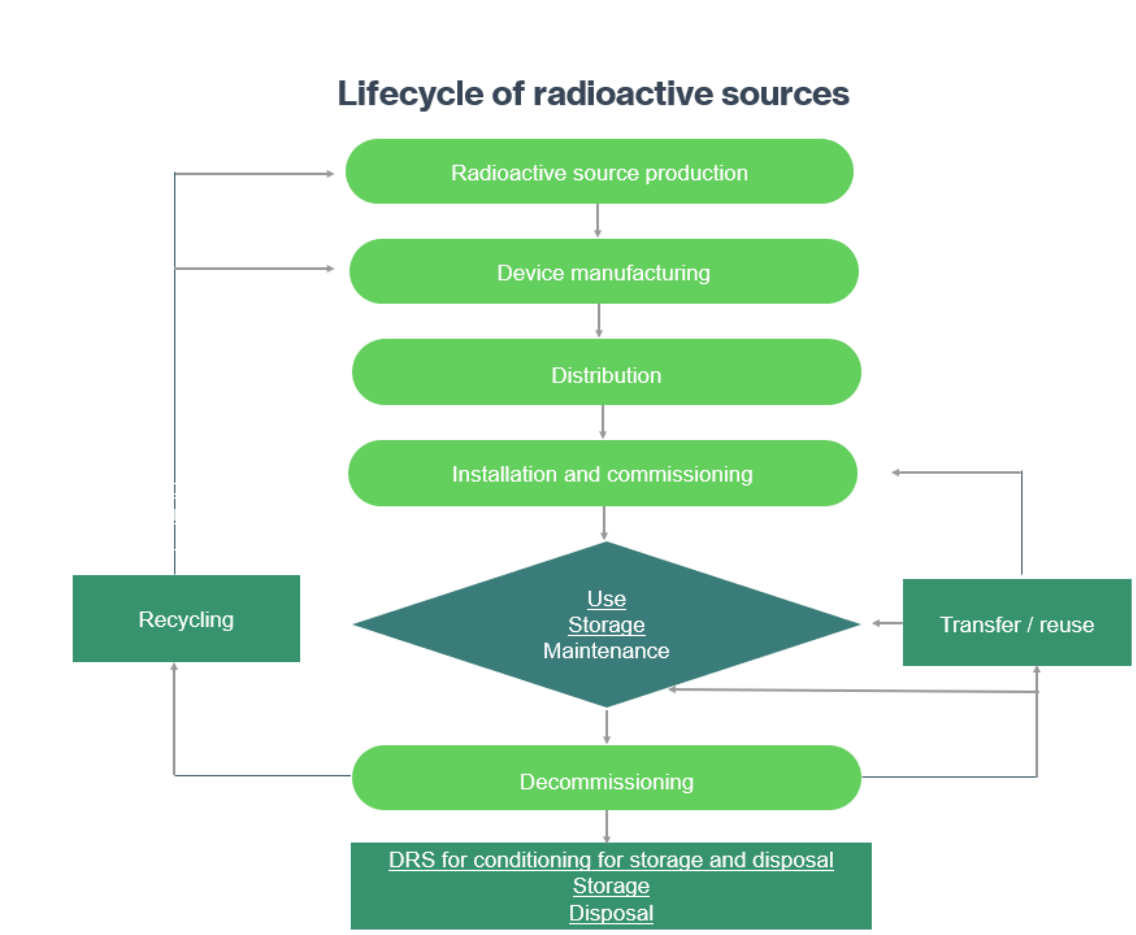

Figure 3.1: The lifecycle of radioactive sources

(Source: Author's own illustration as adapted from IAEA NW-T-1.3 [2014a:45])

During the lifecycle of radioactive sources, there are systematic, step-by-step,

documented phases of radioactive source management that must be followed by all parties that fall within the prescribed radioactive source management. The most vulnerable part is the phase of use, storage, and maintenance. Radioactive sources are produced, manufactured, distributed, installed and/or commissioned so that they can be made available to the user (customer). After radioactive sources are used, the process is reversed, i.e., they should be systematically returned to the manufacturer, who is expected to properly dispose of or recycle them. In South Africa, NTP Radioisotopes SOC Ltd is the producer, manufacturer and distributor of radioactive sources. NTP is the subsidiary of the South African Nuclear Energy Corporation (NECSA) and its security measures fall under nuclear security (NTP Radioisotopes SOC Ltd, 2021:np).

It is vital to determine the correct identification and application of radioactive sources throughout the lifecycle of radioactive sources in order to manage them correctly.

3.3 IDENTIFICATION OF RADIOACTIVE SOURCES AND THEIR APPLICATION

Radioactive sources are used by various institutions, such as hospitals, for medical therapies, to sterilise equipment and devices, in research laboratories, in brachytherapy, to measure thickness and density, and in the oil industry. According to IAEA TECHDOC SERIES 1728 (IAEA-TECHDOC-1728, 2013:92), radioactive sources are identified and used for various purposes as indicated in the table below:

Table 3.1: Identification of radioactive sources and their application

Source	Application	Category
• Cobalt-60 (^{60}Co)	• Medical therapy source • Gamma sterilisation source	Cat 1
• Strontium-90 (90Sr)	• Radioisotope Thermoelectric generator source	Cat 1
• Irridium-192 • ^{60}Co • Cesium-137 (^{137}Cs) • Selenium-75 (Se-75) • Yterrbium-169 (^{169m}Yb)	• Industrial gamma radiography sources (industrial radiography)	Cat 2
• Iridium-192 (192Ir) • ^{137}Cs • ^{60}Co	• HDR Remote after loading brachytheraphy (medical therapy)	Cat 2
• ^{60}Co	• High energy gamma industrial gauging sources	Cat 3
• Americium-241 (^{241}Am) • Californium-252 (^{252}Cf)	• Neutron industrial gauging	Cat 3
• ^{137}Cs • ^{241}Am	• Gamma and neutron oil well logging sources (oil exploration production)	Cat 3
• ^{241}Am • 90Sr • Krypton-85 (85Kr)	• Low energy fixed industrial gauging sources (industrial gauging)	Cat 4
• Iodine-125 (^{125}I) • Palladium-103 (^{103}Pd)	• Permanent implant and low dose rate brachytherapy seed sources (medical therapy)	Cat 5
• Ruthenium-106 (^{106}Ru)	• Eye plagues (medical therapy)	Cat 5

A radioactive source can be used in different categories depending on the application. As indicated in Table 3.1, the same radioactive source can be used for different purposes and in different categories depending on its activity level. For example, cobalt-60 is used as a category 1 radioactive source when used for medical therapy.

Its activity, when used for medical purposes, is measured as 550 terabecquerels (TBq), which is a measure of radiation activity, while the same source can be used as an industrial measurement source and its activity is 37 megabecquerels (MBq), which is a measure of radiation activity. Radioactive sources produce different radiation activities. The higher the activity, the greater the hazard posed by the source. According to the IAEA Publication 7567 (2007:22), radioactive sources are classified into five categories.

The degree of radioactivity emitted by each radioactive source is established by the categorisation of radioactive sources and is dependent on the location in which the source is deployed or utilised.

3.4 CATEGORISATION OF RADIOACTIVE SOURCES

In the IAEA Safety Standards Series No. RS-G-1.9 (IAEA, 2005:6), radioactive sources are classified into different categories based on their level of radioactivity, which determines how dangerous a source may be and what measures must be taken to protect the public from harmful radiation. These categories are listed below:

Category 1: This is a radioactive source classified as extremely hazardous. Exposure to a radioactive source of this level can cause permanent damage to a person who comes into contact with it within minutes to hours, or even death within hours to days.

Category 2: At this level, the radioactive source is considered very dangerous. If someone is exposed to this type of source, they may suffer permanent damage within minutes to hours or die within hours to days.

Category 3: At this level, the source is classified as hazardous and may cause permanent damage if exposed for several hours and may even cause death if exposed for days.

Category 4: This is a not very dangerous category. Sources in this category may cause temporary injury if not handled properly.

Category 5: This source is unlikely to be dangerous and injure someone who handles it improperly.

The categorisation of radioactive sources also adds to the characteristics of a radioactive source, as they have different shapes and sizes (IAEA Publication 1278, 2007:9).

3.5 CHARACTERISTICS OF RADIOACTIVE SOURCES

Radioactive sources pose security risks because of their various properties (WINS Academy, 2016a:40). Security risks in this context refer to theft or sabotage or both:

- **Easily accessible information** – Information about radioactive sources is readily available in the public domain such that people with malicious intent can easily access it.
- **Half-life** – According to Britannica (2022, sv. 'half-life radioactivity'), in radioactivity, the half-life is the amount of time it takes for half of the atomic nuclei in a radioactive section to change into a different type of nucleus by releasing particles and energy, or the amount of time it takes for the number of fragments a radioactive substance makes per second to drop by half. It can also mean the rate at which a radioisotope breaks down, which can take anywhere from a nanosecond to a billion years. The risk is lower when the half-life is shorter, and the risk is higher when the half-life is longer.
- **Attractiveness** – sources are attractive because they are portable and small. This characteristic makes them attractive to those who have malevolent intentions.
- **Usefulness as a weapon** – Radioactive sources can be used as a weapon depending on the degree of their radioactivity.
- **Vulnerability to theft** – radioactive sources are vulnerable to theft, especially by insiders who could steal them protractedly.
- **Weak source as a hazard** – Regardless of the size and radioactivity of the source, a radioactive source still poses a security risk, e.g., through sabotage.
- **Easily dispersed** – Other radioactive sources are easily dispersed. In view of this characteristic, security measures must be considered, especially about the extent of the danger that a radiation source may pose to human life. A graded

approach must be considered for such sources.

- **Aggregation** – Single radioactive sources do not usually pose a major health hazard, but when multiple sources are placed in one location, they produce higher radiation activity. The security measures around such an aggregation need to be reviewed in comparison to the security measures for a single radioactive source.

Because radioactive sources have a variety of distinguishing qualities, it is imperative that the owner or user of the source be accountable and accepts responsibility for their actions.

3.6 THE RESPONSIBILITIES OF THE RADIOACTIVE SOURCES OWNER

The owner of the radioactive sources is referred to as the permit holder and assumes all responsibilities associated with the radioactive sources while they are in their care. The owner/user is expected to take technical and institutional safety and security measures to ensure the safekeeping of the source. The owner assumes legal responsibility for the source until it is transferred to the next legal entity. While the source is in the custody of the owner, the owner is expected to comply with all regulations applicable to the licensee (owner). One of the requirements for the owner is to keep all information about the source, such as the type of source and the manufacturer. This is done so that the source can be traced if it is removed from regulatory control (IAEA NW-T-1.3, 2014b:46). Many radioactive sources have been lost under the care of the licensee that have resulted in several radioactive source incidents. Most of these incidents have resulted from management failures to secure radioactive sources. According to Fay's (2007:492) Incident Causation Model, management failures, which in this case are considered failures of management, form the basis for the deficiencies that lead to the loss, regardless of the size of the organisation or the level at which the failures are committed.

The regulatory framework specifies the procedure through which radioactive source owners are required to fulfil their responsibilities.

3.7 THE REGULATION AND MANAGEMENT OF RADIOACTIVE SOURCES

The IAEA distinguishes between the safety of radioactive material located in nuclear facilities and radioactive sources used mainly in public areas such as public hospitals, industry, well drilling, agriculture, and other purposes. This means that radioactive sources are generally found in many applications “outside” nuclear facilities (IAEA Publication 7567, 2007; IAEA Publication 8616, 2011). Radioactive sources can be either under regulatory control or outside regulatory control. All radioactive sources that are not under regulatory control are usually referred to as “orphan sources”. An orphan source is one that has been abandoned, lost, misplaced, stolen, or otherwise transferred without proper authorisation, poses a sufficient radioactive hazard to warrant regulatory control, and has the potential to harm the public or expose members of the public to harmful (ionising) radiation (IAEA TECHDOC-1388, 2004:np).

Radioactive sources outside nuclear facilities are usually difficult to keep under regulatory control because of their characteristics, physical features or shapes. As shown in the ITDB Factsheet (2019:np), there are a high number of reported cases of losses of radioactive sources each year due to loss, illicit trafficking or theft. Since 1993, a total of 3497 confirmed incidents have been reported by participating IAEA member states. Most thefts and losses reported to the Illicit Trafficking Database involve radioactive sources used in industry or medicine (ITDB Factsheet, 2019:np). In addition to regulatory oversight by the IAEA, radioactive sources are managed internationally by the International Source Suppliers and Producers Association (ISSPA, 2022:np). The association consists of companies that manufacture, produce, and supply sealed radioactive sources or equipment for radiation application processes. ISSPA’s goal is to ensure the continued valuable use of radioactive sources and to promote continuous improvement in safe use and transport – the total management of radioactive sources from cradle to grave (ISSPA, 2022:np). Some of the goals of ISSPA are: to establish a code of conduct for manufacturers and suppliers of radioactive sources; to establish, implement, and maintain a code of conduct for manufacturers and suppliers of radioactive sources; to enhance public confidence in the security of radioactive sources during their life cycle; and to educate stakeholders about the benefits of radioactive sources. Given the goals of ISSPA, it is evident that

the public is one of the most important stakeholders in the use of radioactive sources.

One of the goals of ISSPA is to educate the general public about radioactive sources. As part of this education, participants should learn about the potential threats posed by radioactive sources and how they should be managed.

3.7.1 Radioactive sources security risks and management

According to Ferguson and Potter (2004:3), there are four mechanisms by which nuclear material (including radioactive sources) can be used for destructive purposes:

- The theft and detonation of an intact/complete nuclear weapon;
- The theft or procurement of fissile material resulting in the manufacture and detonation of a crude nuclear weapon – An improvised nuclear device (IND);
- Attacks on and sabotage of nuclear facilities that could result in the release of significant amounts of radioactivity; and
- the illicit procurement of radioactive material that contributes to the production and detonation of a radioactive dispersal device (RDD) – a "dirty bomb" – or RED (Ferguson & Potter, 2004:3).

Like nuclear material, radioactive sources can be used to make IND, RDD for dirty bombs, and deliver radiation in an RED. To mitigate the security risk of nuclear or radioactive material, both the IAEA and WINS have published a series of guidance documents that address the security risks of radioactive sources. The following are IAEA NSS publications that address the security of radioactive materials:

3.7.2 NSS No. 3 – Monitoring for radioactive material in international mail transported by public postal operators

This publication (IAEA Publication 1248, 2009) gives advice on control protocols and equipment that can be used to find gamma and neutron radiation caused by illegal trafficking of radioactive materials through the public mail and private letter carriers. The goal of publishing IAEA NSS No. 3 was to give an overview of the available information and preventative and protective measures to protect postal workers and the public from possible dangers posed by radioactive materials that may have been illegally transported (IAEA Publication 1248, 2009:2).

3.7.3 NSS No. 5 - Identification of radioactive sources and devices

IAEA NSS No. 5 gives basic instructions on how to identify radioactive sources and devices and gives detailed instructions on how to handle and transport containers in an emergency. The scope and purpose of this publication will help in finding radioactive sources and what to do when one is found. This publication can also be used by the public, such as scrap metal processors, to find radioactive scrap (IAEA NSS No. 5, 2007:5).

3.7.4 NSS No. 6 - Combating illicit trafficking in nuclear and other radioactive material

This publication is for persons and organisations involved with identifying and reacting to illicit nuclear or radioactive activity. It also aims to strengthen the worldwide commitment to nuclear and radioactive material security. The nuclear business fears the misuse of nuclear and radioactive materials. This hazard includes building a radiological bomb using radioactive substances. Training and public awareness may prevent illegal conduct by sharing information with law enforcement (IAEA Publication 1309, 2007:92).

3.7.5 NSS No. 9 - Security in transport of radioactive material

Nuclear and radioactive materials are particularly vulnerable during transportation. While there are recommended security measures, security measures differ from case to case with respect to nuclear or radioactive material in transit. It is the responsibility of each state to determine the level of security for radioactive material (IAEA Publication 7567, 2007:7). In establishing the level of security during transport, security measures are applied at three levels: per package (establishing the level of security based on the activity in the package exceeding the established limit), per shipment (establishing the level of security based on the activity in the shipment exceeding the established limit), and per means of transport (establishing the level of security based on the total radioactivity in a means of transport exceeding the established limit) (Publication 7567, 2007:7).

3.7.6 NSS No. 11 - Security of radioactive material in use and storage and of associated facilities

The purpose of this series (IAEA Publication 8113, 2009) is to provide guidance to states on how to establish, enhance, maintain, and support state security measures to secure radioactive materials, associated facilities, and related activities (IAEA Publication 1387 2019:2). The security measures to be established should be capable of deterring (discouraging potential criminals from committing criminal acts), detecting (activating a security system upon intrusion), delaying (reducing the rate at which criminals engage in criminal acts, such as theft), respond (activities performed by a security team after an alarm is triggered), and manage security (which includes establishing security processes, such as security policies and procedures, to ensure no unauthorised access to the facility in question) (IAEA Publication 1387, 2019:42).

WINS best practice guides group five relating to radioactive sources security are:

3.7.7 BPG 5.1 - Security of high activity radioactive sources in use and storage

This BPG is designed to assist individuals in charge of preserving and protecting highly radioactive sources in reducing security concerns (WINS BPG 5.1, 2021:2). It also focuses on the development of adequate physical protection measures for radioactive sources. The establishment of a management strategy and a life-cycle approach, i.e., safeguarding radioactive sources from manufacturing to disposal or from cradle to grave, is one of the BPG's suggestions (WINS BPG 5.1, 2021:31).

3.7.8 BPG 5.4 - Security of radioactive sources in medical applications

Most medical institutions throughout the globe employ radioactive sources for medical purposes such as cancer detection and therapy. This guide explains the many stakeholders' roles and duties in the security of radioactive sources in medical institutions (WINS BPG 5.1, 2021:1). Other topics covered in this tutorial include how to implement a robust and long-term security approach to protect radioactive sources. These include a strong security culture, dealing with internal threats, people competence, security costs, safety and security integration, continuous improvement, and end-of-life planning (WINS BPG 5.1, 2021:24).

3.7.9 BPG 5.5 - Security management of disused radioactive sources

The goal of this BPG is to protect retired radioactive sources (decommissioned radioactive sources). Even when radioactive sources are no longer in use or have reached the end of their useful life, they remain dangerous. As stated in Section 3.1 of this chapter, radioactive sources have a life cycle, which includes safe disposal. This BPG goes into great length into the design and implementation of security measures for decommissioned radioactive sources. Understanding the different roles and duties of the many stakeholders, knowing the targets for malicious activities and their vulnerabilities, and developing an effective and coordinated response plan are all part of the security emphasis (WINS BPG 5.5, 2020:7).

3.7.10 BPG 5.7 - Security of radioactive sources used in industrial radiography and well-logging applications

This group's radioactive sources are often relocated from one location to another. Because they are so mobile, they are vulnerable to loss or theft. The government and users both have a responsibility in maintaining radioactive sources security. The state is in charge of formulating rules, while users are in charge of developing and executing security measures such as security policies and procedures (WINS BPG 5.7, 2021:2). This approach also focuses on limiting access to radioactive sources in storage and at temporary sites by implementing suitable security measures (WINS BPG 5.7, 2021:22).

3.7.11 BPG 5.8 – Security of radioactive sources used in industrial radiation processing

This guidance focuses on the security of gamma irradiation facilities and alerts facility managers to the related security risk, since the radioactive source (60Co) employed in these facilities is very harmful. As with other BPGs, the focus is on strong physical protection systems and security management, and the long-term viability of security measures (WINS BPG 5.8, 2020:1,18).

3.7.12 WINS performance and evaluation series: Peer review guidelines to assess the security of radioactive sources used in medical application

The purpose of this Peer Review BPG is to offer an overview of how industry peers

may perform an effective peer review practice to assess the security programme, i.e., to decide if current security measures are appropriate, inadequate, or excessive. Lessons acquired would aid in the continuing enhancement of the security programme and benchmarking. It is divided into five phases: starting the review, arranging the review, assembling a review team, performing the peer review, and writing the final peer review report (WINS, 2018:9).

The above publications and best practices directly address the security of radioactive sources and are hereby used as the primary reference for the literature review of this chapter. Both the IAEA Nuclear Security Series, which addresses radioactive sources, and the WINS best practice guides, which address radioactive sources, focus fundamentally on securing radioactive sources used for peaceful and domestic purposes. However, securing radioactive sources "outside" nuclear facilities has its own limitations. First, security measures for radioactive sources inside and outside nuclear facilities are not comparable. The reasons for these differences are that security measures inside nuclear facilities generally conform to the IAEA's international regulatory framework, while radioactive sources outside nuclear facilities are subject to individual government security regulations and are regulated by government agencies such as the DoH (as in South Africa and the DoE in the USA). Second, the security of radioactive sources has not been given the same priority worldwide as nuclear safety. It was not until after the hijacking of four commercial airliners in the USA by attackers on September 09, 2001 (which became known as 9/11) that the security of radioactive sources was recognised as a possible next target for terrorists (CNN, 2021:np). The 9/11, 2001 incident was similar to the 1972 hijacking of a U.S. passenger airliner in an attempt to crash the plane into a nuclear facility in Tennessee (Mansfield, 2001:np).

During the use phase, radioactive sources are most vulnerable and the likelihood of them being stolen or lost is high (Korshukim & Emery, 2006:266). The risk arises from the difficulty of always controlling the various areas where radioactive sources are used. For example, the transportation of radioactive sources has resulted in several of them being lost or misplaced. Transporting radioactive sources from one location to another is an essential part of using radioactive sources because they have many applications. At this stage, it is essential that all stakeholders involved in the use of the

sources strictly cooperate and account for the sources to ensure that they are not diverted and used for purposes for which they are not intended (WINS BPG 4.10, 2020:1).

Many radioactive sources have been lost during the use phase, resulting in threats to human life, environmental pollution, radiological injuries, and even death (The Guardian, 2016:np). Many people who have been exposed to a radioactive source that did not comply with prescribed procedures are at risk of being injured or even killed by ionising radiation emitted by the source. Radioactive sources cannot be used to build a nuclear bomb, but they can be used to terrify the public (terrorism) and give bad publicity to the organisation responsible for their safekeeping.

Because of the various stages through which radioactive sources pass, including transportation from one area to another, some radioactive sources have escaped regulatory control at this stage. Cases of theft during the transport of radioactive sources have been reported from various locations (BBC News, 2013:np). Usually, such accidental theft of radioactive sources involves the hijacking of the vehicle by criminals who do not intend to steal radioactive sources. The criminals then abandon the vehicle and leave the source unattended. As a result, the radioactive source escapes regulatory control and becomes a potential hazard to the public and the environment.

There are two security risks associated with radioactive sources: theft and sabotage. Theft of radioactive material can occur either abruptly or over an extended period of time. Abrupt theft involves the theft of large quantities of radioactive sources, while prolonged theft involves the theft of smaller quantities of radioactive sources over an extended period of time. Sabotage occurs when nuclear material is used in such a way that the public lacks confidence in the organisation(s) whose radioactive sources have escaped regulatory control. Due to the characteristics of radioactive sources, theft or sabotage can result in radioactive sources being used as a Radiation Exposure Device (RED), Improvised Nuclear Device (IND), or Radiation Dispersal Devise (RDD). RED, IND and RDD do not have the same scale as a nuclear bomb. Although the use of radioactive sources as a weapon may be minimal compared to a nuclear bomb, they would still cause some injuries in close contact and cause public panic if used malevolently (Ferguson & Potter, 2004:3).

As was the case at the Nuclear Security Summits held in Washington, DC, Seoul, and The Hague, security threats and the management of radioactive sources are an international concern that need to be addressed by both governments and operators globally.

3.8 THE IMPACT OF THE NUCLEAR SECURITY SUMMITS ON THE RADIOACTIVE SOURCES SECURITY

Barack Obama, who was serving as President of the USA at the time, delivered a lecture in Prague in 2009 on the need of ensuring the security of nuclear or radioactive material (Gill, 2020:1). His speech was the impetus for the creation of four nuclear security summits, which took place in Washington, D.C. (2010), Seoul (2012), The Hague (2014), and once again in Washington, D.C. (2016). One of the primary topics discussed at these summits was the protection of radioactive sources. When radioactive sources that need to be secured are hermetically sealed, accounted for, and controlled from cradle to grave, they may be uniquely recognised as needing to be secured.

3.8.1 The Nuclear Security Summit in Washington (2010) Communique

The Nuclear Threat Initiative (NTI, 2010:np) reported that one of the decisions made at this summit included a mention of radioactive material (such as cesium and strontium). Due to the fact that radioactive material has the potential to be used in dirty bombs, it requires the same level of security measures as nuclear material.

3.8.2 The Nuclear Security Summit in Seoul (2012) Communique

The primary reason for attendees' susceptibility to hostile activities is the significant usage of radioactive sources. States were strongly encouraged to increase the security of radioactive sources that are under their care, and to establish mechanisms for the recovery of radioactive sources that have vanished or been stolen, and to retain control over radioactive sources that have been decommissioned (Goon2345, 2012:np).

3.8.3 The Nuclear Security Summit in Hague (2014)Communique

During the course of this summit, a number of nations reported that they had been

successful in enhancing the security of radioactive sources by use of their national registers and by making modifications to their laws and regulations. This was done to conform to the recommendations and guidelines provided by the IAEA (Council of the European Union, 24 March 2014:4).

3.8.4 The nuclear security summit in Washington (2016) communique

One of the decisions that was passed at the summit in 2016 was that the neutralisation of nuclear and radiological terrorism cannot be done only by one country or organisation, but rather only via international collaboration and the exchange of knowledge (The White House Office of the Press Secretary, 2016:np).

The efforts made by the Nuclear Security Summits to secure radioactive sources were informed by earlier radiological accidents, despite the fact that these incidents were not the result of malicious and intentional acts on the part of the perpetrators.

3.9 THE RADIOLOGICAL EVENTS: CASE STUDIES AND SECURITY RISK ASSESSMENT

In evaluating the security measures during the radiological events of the case studies, the researcher refers to the following sources:

- The South African Products Regulatory Authority Code of Practice for Industrial Radiography_Gamma Radiography (standard used for security survey);
- The IAEA reports on previous radiological events (case studies);
- The WINS Security Threat Assessment Scale (threat assessment).

3.9.1 The South African Products Regulatory Authority Code of Practice for Industrial Radiography_Gamma Radiography

The South African Health Products Regulatory Authority (SAHPRA) Code of Practice for Industrial Radiography_Gamma radiography (SAHPRA, 2010:6) specifies the security measures that must be taken in storage facilities and during transport of the radiation source. The Code consists of recommended security measures that must be taken to secure radioactive sources in the facilities or during transport. By making use of the Code, the researcher attempts to identify the security measures that were either

in place or not in place during these events. The recommendations of the Code are as follows:

a) Premises containing storage areas shall be connected to at least a 24-hour security response unit.

b) The storage area must have at least two layers of barriers to provide a delay mechanism.

c) There shall be immediate electronic detection of unauthorised access to the secured area as determined by the designated responsible personnel (e.g., 24-hour security response unit).

d) A 24-hour security response unit should be available to assess the detection of the security breach.

e) Immediate and reliable means of communication must be available to the responsible person to respond immediately to any adverse action discovered.

f) Storage areas must be inspected weekly to detect any possible loss of sources.

g) The security system must be checked weekly for proper operation.

h) Continuous monitoring of portable sources by designated personnel during transport using reliable means of communication.

i) The vehicle must never be left unattended during transport and the container holding the radioactive sources must be securely locked in the vehicle and under constant surveillance.

j) Special security precautions must be taken when the source is being used in high risk areas where there are no security forces in the vicinity.

Since all radiological case studies used in this study were reported by the IAEA, the rating scale consists of the availability or unavailability of security measures based on the IAEA report for each event.

3.9.1.1 The radiological accident in Goiania, Brazil (1987)

The accident occurred in 1985 in the Brazilian city of Goiania (IAEA, 1988) after two citizens entered an abandoned hospital building to collect scrap metal for sale. In the process, they found a teletherapy device containing a cesium-137 (^{137}Cs) source,

which they took home to disassemble. When the device was disassembled, the source was exposed and removed.

Table 3.2: The radiological accident in Goiania

Source name	Accident impact	Security measures according to Code of Practice for Industrial Radiography - Gamma Radiography	Evidence of security measures based on IAEA report
			Yes/No
• ^{137}Cs • Category 1 Extremely dangerous	• 4 x fatalities • About 112 people were monitored for radiation exposure • 249 houses were contaminated • 20 people underwent hospital treatment • Environmental decontamination took more than a year • 85 houses were seriously contaminated • 200 individuals were evacuated from 41 houses • Goiania people discriminated against by other people • Dairy products were also avoided due to environmental contamination	a) 24 hour security reaction?	No
		b) Two layers of barriers to create delay?	No
		c) Immediate electronic detection (alarm) of unauthorised access to the secured area/source location?	No
		d) Availability of detection assessment of a security breach?	No
		e) Immediate and reliable means of communication to initiate response to every detected adverse action?	No
		f) Weekly storage checklist to detect likely source loss?	No
		g) Weekly checklist of security system working condition?	No
		h) Mobile/portable sources continuous surveillance?	No
		i) Continuous surveillance of the source in transit?	No
		j) Special security arrangement of the source in high risk areas where there is no immediate security?	No

3.9.1.2 The radiological accident in Tammiku (1994)

On 21 October 1994, three siblings obtained unauthorised entry to an Estonian nuclear waste storage site in order to search for scrap metal to sell. They obtained a metal

container containing a cesium-137 source. The source dropped to the ground and was picked up by one of the brothers, who carried it home in his jacket. When he returned home, he became unwell and was finally sent to the hospital with terrible injuries to his leg and hip, where he died a few weeks later. Other family members (including a dog that died later) who were exposed to the source were also impacted by the radiation. Authorities eventually collected the source from the residence and returned it to the spot where it had fallen.

Table 3.3: The radiological accident in Tammiku (1994)

Source name and category	Accident impact	Security measures according to Code of Practice for Industrial Radiography - Gamma Radiography	Evidence of security measures based on IAEA report
			Yes/No
• ^{137}Cs • Category 1 • Extremely dangerous	• 2 fatalities • 3 persons got radiation injuries and other health complications	a) 24 hour security reaction?	No
		b) Two layers of barriers to create delay?	No
		c) Immediate electronic detection (alarm) of unauthorised access to the secured area/source location?	No
		d) Availability of detection assessment of a security breach?	No
		e) Immediate and reliable means of communication to initiate response to every detected adverse action?	No
		f) Weekly storage checklist to detect likely source loss?	No
		g) Weekly checklist of security system working condition?	No
		h) Mobile/portable sources continuous surveillance?	No
		i) Continuous surveillance of the source in transit?	No
		j) Special security arrangement of the source in high risk areas where there is no immediate security?	No

3.9.1.3 The radiological accident in Lilo (1997)

On 9 October 1997, the Georgian authorities sought IAEA help with radiological and medical treatment after 11 persons were exposed to ionising radiation at Lilo. The inquiry discovered that the prior owner had left 12 radioactive cesium-137 sources, 1 cobalt-60 source, and 200 radium-226 (Ra) sources unattended (IAEA Publication 1097, 2001:1). As a consequence, nine troops were put under surveillance for radioactive exposure.

Table 3.4: The radiological accident in Lilo (1997)

Source name and category	Accident impact	Security measures according to Code of Practice for Industrial Radiography - Gamma Radiography	Evidence of security measures Based on IAEA report Yes/No
• 12 Cs-137 sources • 1 ^{60}Co source • 200 Ra sources • Category 1 • Extremely dangerous	• 9 soldiers and two more people developed radiological burns on several parts of their bodies and were hospitalised	a) 24 hour security reaction?	No
		b) Two layers of barriers to create delay?	No
		c) Immediate electronic detection (alarm) of unauthorised access to the secured area/source location?	No
		d) Availability of detection assessment of a security breach?	No
		e) Immediate and reliable means of communication to initiate response to every detected adverse action?	No
		f) Weekly storage checklist to detect likely source loss?	No
		g) Weekly checklist of security system working condition?	No
		h) Mobile/portable sources continuous surveillance?	No
		i) Continuous surveillance of the source in transit?	No
		j) Special security arrangement of the source in high risk areas where there is no immediate security?	No

3.9.1.4 The radiological accident in Istanbul (1998; 1999)

Between December 1998 and January 1999, three packages used to carry Co60 teletherapy sources in Istanbul, Turkey, were sold as scrap after the shielding was opened and broken into scrap pieces. Several persons were exposed to radiation, and the person responsible for opening the package had Acute Radiation Syndrome (ARS). This accident occurred as a result of the company's (the user's) failure to return the used radiation sources to the supplier as required under the radioactive source's life cycle.

Table 3.5: The radiological accident in Istanbul (1998; 1999)

Source name and category	Accident impact	Security measures according to Code of Practice for Industrial Radiography - Gamma Radiography	Evidence of security measures Based on IAEA report Yes/No
• ^{60}Co • Category 1 • Extremely dangerous	• 404 people underwent medical observation • 18 people admitted in hospital due to radiation overexposure • 10 people tested positive for acute radiation syndrome • Caused general public panic and anxiety	a) 24 hour security reaction?	No
		b) Two layers of barriers to create delay?	No
		c) Immediate electronic detection (alarm) of unauthorised access to the secured area/source location?	No
		d) Availability of detection assessment of a security breach?	No
		e) Immediate and reliable means of communication to initiate response to every detected adverse action?	No
		f) Weekly storage checklist to detect likely source loss?	No
		g) Weekly checklist of security system working condition?	No
		h) Mobile/portable sources continuous surveillance?	No
		i) Continuous surveillance of the source in transit?	No
		j) Special security arrangement of the source in high risk areas where there is no immediate security?	No

3.9.1.5 The radiological accident in Samut Prakarn (2000)

According to the IAEA assessment on this occurrence, in January/February 2000, 60Co was partly removed from the head of the teletherapy equipment in order to sell the device components as scrap. The device was obtained from a hospital that was replacing its teletherapy system and had no storage space for the replacement device. The hospital is thought to have sold the equipment to an unlicensed receiver who kept it in an insecure storage area, allowing the public unrestricted access to the radiation source (IAEA Publication 1124, 2002:42). The item was brought to a scrap yard and scrapped. The device was further dismantled at the scrap yard, and the 60Co purportedly dropped out of the device, exposing scrap yard personnel to radiation. Doctors who feared radioactive exposure in their patients reported the accident to authorities (IAEA Publication 1124, 2002:1).

Table 3.6: The radiological accident in Samut Prakarn

Source name and category	Accident impact	Security measures according to Code of Practice for Industrial Radiography - Gamma Radiography	Evidence of security measures Based on IAEA report Yes/No
3 ^{60}Co teletherapy head 4 Category 1 **5** Extremely dangerous	6 10 people received high doses from the source 7 3 scrapyard workers died due to radiation exposure	a) 24 hour security reaction?	No
		b) Two layers of barriers to create delay?	No
		c) Immediate electronic detection (alarm) of unauthorised access to the secured area/source location?	No
		d) Availability of detection assessment of a security breach?	No
		e) Immediate and reliable means of communication to initiate response to every detected adverse action?	No
		f) Weekly storage checklist to detect likely source loss?	No
		g) Weekly checklist of security system working condition?	No
		h) Mobile/portable sources continuous surveillance?	No
		i) Continuous surveillance of the source in transit?	No
		j) Special security arrangement of the source in high risk areas where there is no immediate security?	No

3.9.1.6 The radiological accident in Lia, Georgia (2001)

On 2 December 2001, three inhabitants of the Georgian village of Lia set out to gather

firewood in the forest. While looking for wood, they found two metal items containing strontium-90 (90Sr), which produces significant quantities of radiation (IAEA Publication 10602, 2014:1). According to the IAEA report, the sources were used to power generators in Georgia in the early 1980s, when there was no electricity, and were later decommissioned (IAEA Publication 10602, 2014:3). The victims afterwards experienced nausea, headaches, vomiting, and disorientation. They began to feel a burning feeling in some places of their bodies around two weeks later. They were later hospitalised and diagnosed with "acute radiation syndrome" (ARS), which has a detrimental influence on health. As a consequence, one person died after 893 days.

Table 3.7: The radiological accident in Lia, Georgia

Source name and category	Accident impact	Security measures according to Code of Practice for Industrial Radiography - Gamma Radiography	Evidence of security measures Based on IAEA report
			Yes/No
• 90Sr • Category 1 • Extremely dangerous	3 3 residents suffered ARS due to radiation overexposure 4 1 fatality (out of the three who suffered ARS	a) 24 hour security reaction?	No
		b) Two layers of barriers to create delay?	No
		c) Immediate electronic detection (alarm) of unauthorised access to the secured area/source location?	No
		d) Availability of detection assessment of a security breach?	No
		e) Immediate and reliable means of communication to initiate response to every detected adverse action?	No
		f) Weekly storage checklist to detect likely source loss?	No
		g) Weekly checklist of security system working condition?	No
		h) Mobile/portable sources continuous surveillance?	No
		i) Continuous surveillance of the source in transit?	No
		j) Special security arrangement of the source in high risk areas where there is no immediate security?	No

3.9.1.7 Overview of the assessment scale results

The case studies that were chosen do not provide any indication that security precautions were taken in line with the recommendations made in the IAEA report and the Code of Practice for Industrial Radiography - Gamma Radiography. The fact that these findings demonstrate that there were no obligatory security precautions in place at these institutions during the events does not imply that the security status of these facilities has stayed the same up to the present day. This may well be understood as one of the limitations of this study.

All of the chosen radiological incidences serve as proof that there is no evidence to support the fact that radioactive sources have been purposefully targeted by nefarious individuals. In spite of this, the Security Threat Assessment Scale is being applied in this research in order to ascertain the security dangers that were present during these particular occurrences.

3.9.2 Case studies threat assessment: The WINS security threat assessment scale

According to Fay (2007:492), the term "management failure" refers to errors committed by management that serve as the foundation for the shortcomings that ultimately result in a loss. The occurrences that occurred in each of the six radiological case studies that were chosen seem to have been the result of management failure or neglect, particularly in the situations where theft was involved. The researcher proposes to offer the WINS Security Threat Assessment Scale in light of Fay's explanation of the idea of management failure. This scale will be used to identify the severity of each event depending on the features of the occurrence.

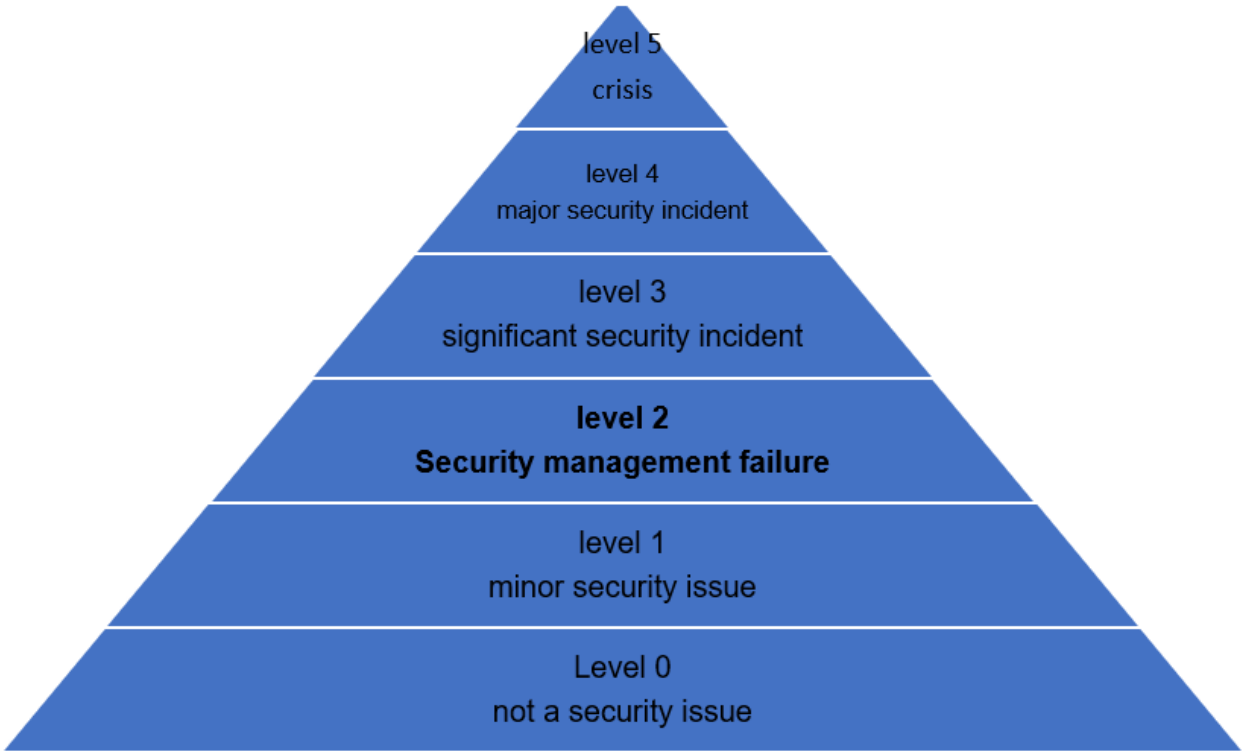

Figure 3.2: The WINS threat assessment scale adopted from WINS Academy (2016b:49)

3.9.2.1 Level 0 – Not a security event

At this point, a security system has been engaged, and the situation is seen as being quite simple to deal with. An example of this would be the situation in which an employee steals from their employer, and the line management responds by applying organisational norms or regulations as a means of disciplining the person for their dishonesty.

3.9.2.2 Level 1 – Minor security event

It is possible that the security system was compromised in a one-time, inadvertent lapse that was not done on purpose. A good illustration of this would be the unintentional disclosure of non-secret security information without adhering to the appropriate organisational norms.

3.9.2.3 Level 2 – Security management failure

This rating indicates that management is not carrying out its responsibilities as it should and is allowing inadequate levels of security. One illustration of this would be a manager's refusal to impose punishment on the security staff members who repeatedly arrive late for work.

3.9.2.4 Level 3 – Signification incident

At this level, people are planning to commit a crime on purpose in order to get some sort of benefit. An example could be a piece of confidential information belonging to the organisation, such as a trade secret, being divulged to third parties in the outside world by accident or on purpose by an employee.

3.9.2.5 Level 4 – Major incident

At this stage, an earnest effort is made to get around the security system, but the activities are stopped by the precautions that are already in place. An example could be an instance during a rally when some protestors may try to pull down the facility's fence in order to gain access to the inside, but the security mechanisms in place can foil such efforts.

3.9.2.6 Level 5 – Crisis

At this point, none of the systems are able to defend the facility against the onslaught. An illustration of this would be when trespassers are successful in entering the institution.

The second level on the scale will serve as the primary focus of this study. On the WINS scale of security threats, level 2 relates to management that is not appropriately executing its function, which leads to a security culture that is lacking. This culture subsequently results in a variety of security shortcomings such as frequent absences of security employees in the place of employment, failure to follow established standards, purposeful failure to notify anomalies, and deliberate inability to react to detected security deficits (WINS-SIM1, 2016:50). If criminal intent was present during these radiological mishaps, it was feasible for radioactive materials to slip into the wrong hands and be utilised for harmful purposes. This was possible based on the

features of the WINS threat rating scale. Case studies demonstrate, among other things, that radioactive sources are widely dispersed and that very few, if any, security precautions are taken to secure them. This also adds to the concern raised by the IAEA in its ITDB information sheet about the rising number of thefts and losses of radioactive sources, particularly during the usage phase. This issue was brought up because of the growing number of thefts and losses of radioactive sources.

Because radioactive sources are utilised on a national scale, sufficient regulatory attention must be paid to the hazard posed by radioactive sources at the national level.

3.10 THE MANAGEMENT OF RADIOACTIVE SOURCES IN SOUTH AFRICA

South Africa is a signatory to a number of IAEA rules on radioactive sources and is also a member of the IAEA. South Africa made commitments at the Nuclear Security Summit in 2014, one of which was to "launch a plan to retrieve, consolidate, and return decommissioned and orphaned radioactive sources across Africa" (Cann, Davenport & Parker, 2016:53). The responsibility for this falls on the Department of Health.

3.10.1 The Department of Health

SAHPRA, acts as the regulatory agency for the Department of Health (SA, 2022b:np). SAHPRA is responsible for regulating and returning disused radioactive sources and equipment from public facilities such as public hospitals. The literature search revealed that there is no evidence of radioactive sources security training or awareness training for the healthcare security personnel. The SAHPRA website has no references to radioactive sources security. Essentially, there is a lack of information on general awareness of radioactive sources security, especially among healthcare facility security personnel.

3.10.2 NTP Radioisotopes SOC Ltd

The NTP is a South African state-owned corporation founded in 1992 to manufacture, process, and distribute radioactive sources to over 60 nations across the globe. Molybdenum-99, which is used in medical imaging, and iodine-131, which is utilised in nuclear medicine to detect and treat thyroid diseases, are among the radioactive elements produced (NTP, 2022). NTP's radioactive source is iridium-192, a sealed

source principally utilised for non-destructive testing based on gamma radiography. The NTP is a member of ISSPA.

Because the NTP is located within the nuclear facility (NECSA, 2022:np) and is subject to the nuclear security of the same facility, the security of the radioactive products is ensured at a nuclear facility while they are being manufactured, processed, and distributed by the NTP. This is the case because the NTP is covered by the same nuclear security as the nuclear facility. However, once these items leave the site of the manufacturer, their security is no longer guaranteed to the same extent as it was when they were first produced. Users of radioactive sources and those working in the field of nuclear medicine may obtain information from these sources. The primary objective of this study was to find ways to improve the security of radioactive sources located both within and outside of nuclear facilities (e.g. in public hospitals).

While it is the responsibility of the government to manage radioactive sources, international cooperation is necessary to ensure that information regarding radioactive sources is disseminated across different countries in order to enhance security awareness and consistency in dealing with them.

3.11 INFORMATION SHARING: NUCLEAR SECURITY VS RADIOACTIVE SOURCES SECURITY (INTERNATIONAL LEVEL)

Every organisation is accountable for ensuring that the classified or sensitive security information it maintains is safeguarded in accordance with the requirements that have been established. On the other hand, it is the responsibility of organisations (especially those that use radioactive sources, such as hospitals) either to explain to the public why certain security information cannot be released or to disclose to the public necessary information regarding the organisation's security. The places where radioactive sources are kept, the people who have the keys to those places, and the employees who are accountable for the radioactive sources are all examples of information that is classified and thus cannot be disclosed to the general public. If information of this kind were to become widely known, it might compromise the security of radioactive materials. According to WINS BPG 2.4 (2011:3), communicating with stakeholders does not mean disclosing confidential information; rather, it means providing information about management systems, governance, and

oversight functions to those who are responsible for carrying out those responsibilities.

3.11.1 THE IAEA Incident and Trafficking Database (ITDB)

The ITDB (IAEA ITDB, 1995:np) was established in 1995 to record and analyse incidents of illicit trafficking in nuclear and other radioactive materials. It covers all incidents involving nuclear and other radioactive material outside regulatory control. Nuclear material that is outside regulatory control may be stolen, lost, or orphaned radioactive sources.

According to the 2016 ITDB Fact Sheet, from the 31 December 2015, ITDB has 2889 confirmed events from participating states. Four hundred and fifty-four occurrences included unlawful possession and associated criminal activity, 762 involved theft or loss, and 1622 involved other unauthorised activities and events.

The fact that reporting of such instances to the IAEA ITDB is entirely voluntary, and the specifics of such incidents are not made accessible to the public, are two issues that plague the database. This also implies that if a member state of the IAEA chooses not to report such occurrences, the ITDB will not chronicle them. This form of reporting is not consistent, and it does not give accurate data on the security of nuclear or radioactive material that has evaded regulatory oversight.

3.11.2 CNS Global Incidents and Trafficking Database

The CNS Global Incidents and Trafficking Database tracks nuclear and radioactive incidents. The Nuclear Threat Initiative (NTI) funds the James Martin Center for Non-proliferation Studies' database. The publicly accessible database is created from public data and news stories. South Africa, Belgium, England, Georgia, India, Israel, and Japan all reported two radioactive source events in 2013, the USA reported 82 incidents and Canada reported 15 incidents. The CNS Global Incidents and Trafficking Database uses official and unofficial sources, including incidents not documented by IAEA ITDB or officially reported by government authorities. The given numbers do not mean that a state has reported these incidents as some information may come from news media (CNS Global Incidents and Trafficking Database, 2017:np).

3.11.3 Canada and the Netherlands IPPAS Mission Reports

In 2005, the IAEA established the International Physical Protection Advisory Service (IPPAS) to assist states in strengthening their national nuclear security measures. The IPPAS advises states on the implementation of international regulations and IAEA guidance on the protection of nuclear and other radioactive materials and associated facilities (IAEA IPPAS Mission, 2005:np). After the IPPAS visit to a state, a confidential report is prepared for the state that was the subject of the IPPAPS review. Such a report is not intended for public release. Nonetheless, in 2016, Canada made its IPPAS mission report available to the public. The mission was conducted in Canada from 19 to 30 October 2015 (WINS, 2016:np). The IPPAS mission report is a top-secret document that IAEA IPPAS missions can share only with the state concerned. It consists of five modules, one of which (Module 4) focuses on the security of radioactive material, associated facilities, and activities.

As indicated by the scope of the IPPAS mission, the IPPAS review consists of sensitive information from both state and the entity reviewed. While sensitive security information was removed from the report, the report contains still has extensive details about the activities conducted by the mission. Another state that has published a similar report is the Netherlands (Follow-up Mission Report: The Netherlands 23 January–3 February 2012). In contrast, there is not much information on the security of radioactive sources that is publicly available, apart from the information provided by the IAEA or WINS. This gap will be filled by this study.

Due to the sensitive nature of radioactive sources, information pertaining to those sources should not only be disclosed on a "need to know" basis, but it should also be supported by government rules that control the disclosure or non-disclosure of classified information.

3.12 SOUTH AFRICAN LEGISLATIONS ON INFORMATION SHARING

3.12.1 The Promotion of Access to Information Act 2, 2000

Section 32(1)(a) of the Constitution of the Republic of South Africa (RSA, 1996) provides that everyone has the right of access to all information held by the State and to all information held by another person that is necessary for the exercise or protection

of rights. The Promotion of Access to Information Act (RSA, 2000:4) is the national legislation enacted to implement the right of access to information enshrined in the Constitution.

The security of a nuclear facility is essential to both the government and the public. Failure to protect information worthy of protection can compromise a nuclear facility and endanger the lives of all if classified information falls into the wrong hands. However, the overprotection of security information that could promote public awareness or increase public confidence in radioactive sources could also have negative consequences, as South Africa is not immune to the loss of radioactive sources. This Act gives effect to the constitutional right of access to all information held by the State and to all information held by another person and is necessary for the exercise or protection of all rights. The Act prescribes the right of access to records of public bodies, the way such records should be made available, and the ground for denying access to records. Based on this Act, the public may request disclosure of radioactive source information for the purpose of public awareness, education, and training, provided that the disclosure of such information will not jeopardise the security of the radioactive source licensee (WINS BPG 2.4, 2011:4).

3.12.2 Protection of Information Act 84 of 1982

The Protection of Personal Information Act (RSA, 2013:14) provides for the protection of certain information from disclosure. Information protected under this Act includes secret and top-secret information, the disclosure of which could jeopardise the security of the State. Based on this Act, not all information can be disclosed to the public. Therefore, the Act provides for withholding certain information, the disclosure of which could have undesirable consequences. The Promotion of Access to Information Act (Republic of South Africa, Protection of Access to Information Act 2 of 2000:4) and the Protection of Information Act (RSA 1982:4) are complementary in that they provide for the disclosure of certain information when necessary.

3.12.3 The Minimum Information Security Standards (MISS)

According to the Minimum Information Security Standards (South African Cabinet, 1996), certain information must be classified for various reasons. The MISS provides

for four classifications of information, namely, restricted, confidential, secret, and top secret. The various classifications define information that cannot be disclosed and information that can be disclosed. This study aimed to maintain the classification of information as stated in the MISS document and to focus on evaluating the need to disclose general radioactive sources security information that will enhance public confidence without compromising the security of radioactive sources in healthcare facilities. The MISS document allows a balance to be struck between promoting access to information and laws protecting information.

Although the government has the ability to make provisions for the sharing of secret and unclassified information, specific legislation is required in order to effectively oversee the nuclear industry.

3.13 THE SOUTH AFRICAN NUCLEAR REGULATORY FRAMEWORK AND STAKEHOLDERS: NUCLEAR VS RADIOACTIVE SOURCES

3.13.1 The Nuclear Energy Act 46 of 1999

This Nuclear Energy Act (RSA, 1999:4) was enacted "to provide for the establishment of the South African Nuclear Energy Corporation Limited ... [and] to define the functions and powers of the corporation". The Act contains, inter alia, provisions relating to the security of the corporation's plant, sites and premises." While this refers to the nuclear sector, it does not include provisions for public participation in nuclear security issues nor is the security of radioactive sources mentioned anywhere in the Act.

3.13.2 The National Nuclear Regulator Act 47 of 1999

The National Nuclear Regulator Act (RSA, 1999:4) was enacted to establish a National Nuclear Regulator to regulate nuclear activities, establish safety standards, and regulatory practices, and to protect persons, property, and the environment from nuclear-related harm and related matters. The NNR has produced a series of regulatory guides for nuclear security.

3.13.3 The National Radioactive Waste Disposal Institute (NRWDI)

According to the National Radioactive Waste Disposal Institute Act (RSA, 2008:4), the

Act provides for the “establishment of the NRWDI to manage radioactive waste disposal at the national level”. Section 5 (m) of the Act states that one of the functions of the NRWDI is to “inform the public living in the vicinity of radioactive waste management facilities about all aspects of radioactive waste management”. Currently, South African radioactive waste is disposed of at Vaalputs, which is considered the national radioactive waste management facility and is managed by NECSA on behalf of the South African government. Transporting waste from NECSA or Koeberg to Vaalputs is both a safety and security issue. Public awareness of road use is primarily a safety issue, but transport security of radioactive material is related to nuclear security.

3.13.4 Department of Energy (DoE)

The Nuclear Energy Act (RSA, 1999:4) and the NNR Act 47 of 1999 are the principal Acts governing the management of nuclear energy in South Africa. The DoE is the authority responsible for the administration of all matters relating to nuclear energy. These matters are divided into three areas: Nuclear Safety, Nuclear Technology, and Nuclear Non-proliferation. Nuclear security falls under non-proliferation.

3.13.5 The Department of Health: South African Health Products Regulatory Authority (SAHPRA)

Nuclear or radioactive materials used outside the nuclear industry, such as those used in healthcare facilities, are regulated by the Department of Health (SA, 2022b:np) through SAHPRA under the Hazardous Substance Act (South Africa [SA], 1973:4). Various Codes of Practice have been published under this Act. The Code of Practice for Industrial Radiography – Gamma Radiography, which was used in this study to evaluate security measures for incidents involving radioactive sources, can be found under SAHPRA.

3.13.6 The National Nuclear Regulator (NNR)

The NNR is the authorised local regulatory authority for the South African nuclear industry, which includes the operators, i.e., NECSA and Koeberg, and the mining industry where uranium is mined. Under the NNR Act xxx(RSA, NNR Act 46 of 1999:4) nuclear power plant operators (e.g., NECSA and Koeberg) are required to establish a

public safety information forum to inform people in their respective communities about nuclear safety and radiation protection issues.

3.13.6.1 The NNR Nuclear Safety Directorate

The NNR, as a regulatory agency, is required to ensure nuclear security or physical protection systems (PPS) at nuclear facilities. According to the NNR website, the licenced or permitted operator must ensure that security measures to protect nuclear or radioactive material meet mandatory international regulatory standards.

The NNR has published two important security-related guidance documents. The RG-0006: Guidance on Physical Protection Systems for Nuclear Facilities provides guidance to licensees on implementing nuclear security measures or physical protection systems at facilities with the goal of preventing criminal activity against nuclear and/or radioactive material. The RG-0014: Guide for Implementing Cyber or Computer Security for Nuclear Facilities provides guidance for implementing cyber or computer security measures at facilities to prevent cyber-attacks and other malicious acts against digital nuclear facilities and associated infrastructure. The nuclear security information provided in the NNR public domain is a practical demonstration that nuclear security information can be discussed with the public without revealing sensitive information. The same approach could be taken in disseminating radioactive sources security information.

In both 2014 and 2016, the WINS conducted a study of regulatory reporting and found that “public reporting by regulators responsible for oversight of nuclear security oversight is neither consistent nor comprehensive”. Based on the WINS Academy (2016c:60), this inconsistency in reporting is attributed to several reasons that include:

- Nuclear security issues are confidential;
- Nuclear security issues are not important;
- Nuclear security is a new regulatory issue; and
- Nuclear safety is more important.

Judging from the above difficulties in public reporting by nuclear regulators, the NNR

has made significant progress in discussing nuclear security issues with the public. This is an essential component of this study and of the attempt to answer the research question. However, the degree of public awareness of radioactive sources security cannot be fully determined until after data collection and analysis (see Chapter 4).

3.13.6.2 The Public Safety Information Forum (PSIF)

In addition to the above, the NNR has established public platforms to engage the public on PSIF, public relations, corporate social responsibility, civil society, public access to information, and fact sheets. During the period between 8 March 2014 and 17 September 2016, nuclear security was discussed in detail at Pelindaba PSIF meetings on only two occasions: during the PSIF meeting which was held on 29 August 2015 and the NECSA Corrective Action Plan: Regulatory Emergency Exercise on 11 October 2014. During these discussions, the following security issues were addressed:

- Access of foreign visitors to NECSA: Statistics were presented on the number of foreign visitors who visited NECSA from 01 April 2014 to 31 March 2015.
- Upgrading security systems: The issue included the fence, cameras, strategic facilities, and security training.
- Corrective Action Plan: NECSA provided information on security noncompliance that occurred during the regulatory emergency exercise at NECSA on 11 October 2014.

The researcher reviewed several PSIF minutes from both NECSA and Koeberg Nuclear Power Plant to determine how frequently radioactive sources security issues were discussed during PSIF meetings. The following observations are based on documented evidence:

- Radioactive sources security is not an integral part of the PSIF agenda;
- Radioactive sources security was never discussed at PSIF meetings;
- The security of radioactive sources is discussed only when there are security-related incidents such as violations of security regulations;

- The security of nuclear/radioactive sources is discussed only when a security issue is raised;

- There is no radioactive sources security awareness programme during PSIF meetings.

3.13.7 The National Radioactive Waste Disposal Institute (NRWDI)

The National Institute for Radioactive Waste Management is established under National Radioactive Act (Republic of South Africa, National Radioactive Waste Disposal Institute Act 53, 2008:4) on the National Institute for Radioactive Waste Management with the aim of managing radioactive waste at the national level. According to Section 5 (m) of the Act, one of NRWDI's functions is to “inform the public living in the vicinity of radioactive waste management facilities about all aspects of radioactive waste management”. Currently, South African radioactive waste is disposed of at Vaalputs (NRWDI Vaalputs, 2021, np), which is considered the national radioactive waste management facility and is managed by NECSA on behalf of the South African government. The South African nuclear industry makes this information available to the public for safety reasons. However, the same cannot be said about the security of radioactive sources.

3.14 CONCLUSION

This chapter focused on the literature review of radioactive sources in terms of their production, use, and security. It also provided an overview of the history of nuclear security and how its use has shaped society's thinking and perceptions about nuclear radiation. In contrast to the public's fears of nuclear radiation are the benefits that accrue from the use of radioactive sources. IAEA and WINS publications on radioactive sources are cited as the primary suppliers of information on radioactive sources from which the public outside the nuclear industry can obtain information on the security of radioactive sources. To fully understand the security risks associated with radioactive sources, one must understand the life cycle of radioactive sources from manufacture to disposal (from cradle to grave). The chapter also addresses how to identify, classify, and characterise radioactive sources. These characteristics are among the reasons why radioactive sources must be safeguarded by radioactive

source licensees or owners. To hold radioactive source licensees accountable, radioactive sources are regulated both internationally and locally. A history of lost radioactive sources is also presented to illustrate the challenge of securing radioactive sources due to their multiple uses in different locations. Both theft and sabotage are cited as security risks for radioactive sources. Even if radioactive sources are not used to build a nuclear bomb, they can be used to build a dirty bomb, which is one of the reasons why they must be secured. The four nuclear security summits held between 2010 and 2016 are also cited as efforts by the international community to secure radioactive sources. A number of case studies on the loss of radioactive sources and the impact on those who have come into contact with them are mentioned. The researcher compares the level of security based on the IAEA report on selected past radiological events with the SAHPRA Code of Practise for Industrial Radiography_Gamma Radiography. The Code includes several recommendations for securing radioactive sources at the facility and during transport. These security measures are then used to determine the presence or absence of security measures during these events. An introduction to the threat rating scale from WINS is provided to determine the failure of management to secure radioactive sources during these incidents. In this chapter, the researcher has taken a closer look at the management of radioactive sources in South Africa and in the international community. The nuclear industry is known for overprotecting security-related information. To demystify the over-classification of security-related information, several sources are used to refute the notion that all nuclear/radioactive sources security information should be classified. The study also shows that less security-related information is shared about radioactive sources than about nuclear safety information. Reference is made to the nuclear industry and radioactive source regulations at the local and international levels.

CHAPTER 4
DATA ANALYSIS AND INTERPRETATION

4.1 INTRODUCTION

Shkedi (2019:98) points out that data analysis is the process of extracting raw data, such as interviews, from the context in which it was originally collected and re-locating it within a context that clarifies its meaning. The aim of this study was to ascertain the level of knowledge regarding the security of radioactive sources that is held by security professionals working in healthcare facilities (see Section 1.7.1). According to the information that was gathered, this objective was accomplished through the responses provided by the participants who took part in the research. The study consisted of four objectives (see Section 1.7.2), which were addressed through the responses from the research participants. This chapter focuses on the presentation, interpretation and analysis of the results of the data collected from the research participants.

In order to provide context for the analysis of the data, the study procedure summary is presented below:

4.2 RESEARCH PROCEDURE OVERVIEW

Data were collected through in-person interviews, i.e., one-on-one interviews and telephone interviews with the participants. Before conducting the interviews, the researcher distributed the interview schedule to the participants in person. In addition, he emailed the interview schedule to participants who could not be reached when the questions were delivered in person. Participants had a choice of one-on-one interviews, telephone interviews, and Microsoft Teams interviews. Three participants were interviewed by phone because they were not available for an in-person interview, and seven participants were interviewed in person. None of the participants were interviewed through Microsoft Teams. Data were collected using a semi-structured interview schedule (See Annexure C). The semi-structured interview schedule consisted of ten questions that were presented to the study participants prior to the start of the interviews to familiarise them with the research questions. All research question schedules were emailed to all participants and then hard copies were handed out to the participants by the researcher. This was done to ensure two things: first, that

the participants actually received the research questions, and second, that the researcher was able to become familiar with the participants' work environments. This would also allow the researcher to relate the participants' responses to the research questions. All interviews were digitally recorded using an audio recorder and then transcribed. Interview recordings were numbered as research Participant 1 to 15 and by the date the interview took place. During the interviews, the most important categories and themes were identified to better understand the data collected. To determine different categories and themes, the researcher analysed the content of the interview transcripts and the participants' responses. Participants' comments were documented and grouped to identify themes. During the interviews, it became clear that the research participants knew very little about radioactive sources security and therefore responded based on their knowledge of traditional security.

The findings of the study are broken down into two categories: Category A comprises the biographical information of the research participants, and Category B comprises the responses provided by the research participants.

4.3 SECTION A: BIOGRAPHICAL DATA

The researcher recognised the importance of obtaining demographic information from research participants. The biographical data was to ensure that all selected participants had relevant and minimal knowledge, experience, and background in the security industry to participate in the study. While information, such as gender, marital status, and others, is normally included in the biographical data, the researcher did not consider this information to be relevant for this study. The biographical information is presented in a tabular format, as indicated below:

Table 4.1: Demographic information of participants

Research participants	Demographic summary					
	Age <30	Race	Employment position	Length of security service	School qualification	Security / equivalent training (min PSIRA Grade B)
1	43	African	Supervisor	18 years	National Diploma	Grade A
2	51	African	Security Manager	30 years	BA Degree	Grade A
3	49	African	Deputy Director	21 years	BA Degree	Grade A
4	40	African	Control Room Operator	13 years	Grade 12	Grade A
5	50	African	Security Manager	26 years	Grade 12	Grade A
6	47	African	Security shift leader	6 years	Grade 12	Grade A
7	36	African	Chief Security Officer	13 years	Advanced Diploma Security	Grade A
8	41	African	Assist. Director	8 years	Grade 12	Grade A
9	47	African	Chief Security Officer	16 years	National Diploma sec	Grade A
10	55	African	Deputy Director	30 years	Grade 12	Grade A
11	38	African	Assistant Director	18 years	Grade 12	Grade A
12	49	African	Investigator	23 years	NQF Level 6 / National Dip	Grade A
13	38	African	Chief Security officer	15 years	Post grade Diploma Sec	Grade A
14	45	African	Chief Security officer	23 years	Advanced Diploma sec	Grade B
15	63	African	Security Manager	43 years	Grade 12	Grade A

4.4 DEMOGRAPHIC DATA INTERPRETATION

4.4.1 Age of participants

Four of the 15 participants were between 30 and 40 years; eight of the study participants were between 41 and 50 years; two of the study participants were between 51 and 60 years, while one of the study participants was between 61 and 70 years old. All participants were older than 30 years and thus had the necessary experience to participate in the study.

Table 4.2: Age of participants

Age group	Number of participants
30–40	4
41–50	8
51–60	2
61–70	1

4.4.2 Race of participants

All fifteen of research participants were African. There was no particular race required. However, given the case studies where this research was conducted, only African males and females were available and responded to participate in the study.

4.4.3 Employment of participants

All research participants were employed in various security-related positions. They are all internal security personnel, that is, they are all employees employed by the institutions. Two were Deputy Directors. Five were Chief Security Officers, two were Assistant Directors, three were Security Managers, one was a Security Leader, one was an Investigator, one was the Control Room Operator, one was the Supervisor, and one was the Security Shift Leader. Work experience in the security industry was a necessity for participating in the study.

4.4.4 Length of security service

All participants had from six to forty-three years of experience working in the security field and were well-versed in the norms and atmosphere of the security industry. Two of the fifteen participants had between six and ten years of experience in the security industry (Participants 6 and 8), six participants had between ten and twenty years of experience (Participants 1, 4, 7, 9, 11, 13), six participants had between twenty-one and thirty years of experience (Participants 2, 3, 5, 10, 12, 14), and one participant had between forty and fifty years of experience in the security industry (Participant 15). Although they were all familiar with the field, it became clear during the course of the research that the participants knew very little about the security of radioactive sources. This was despite the fact that each of the organisations that participated in the study possessed radiological facilities. They referred to the radiological area more commonly as the nuclear medicine or division, but they were unable to make the connection between radioactive sources and nuclear. Only when they were presented with the research questions did they learn about the connection between radioactive sources and nuclear.

4.4.5 School qualifications

Participants' educational qualifications ranged from High School Grade 12 or Standard 10 to Post Graduate Diploma in Security Management. Seven had Grade 12 only (Participants 4, 5, 6, 8, 10, 11); two had a BA degree in security management (Participants 2, 3); one had a post graduate diploma in security management (Participant 13), two had an advanced diploma in security management (Participants 4, 14); two had a national diploma in security management (Participants 1, 9); two had advanced diplomas in security management (Participants 7, 14), and one had a postgraduate diploma in security management (Participant 13). While the participants were not well versed in radioactive sources security, their academic security qualifications played an important role in answering the research questions and understanding the security activities taking place in their respective environments.

4.4.6 PSIRA Grading

The PSIRA (2022:np) Grade B was used as the minimum supervisory requirement,

but all participants had PSIRA grade A, except participant 14 who had Grade B. PSIRA grade A is at managerial level and is the highest among PSIRA grades.

4.5 SECTION B: THE EXAMINATION OF THE NEED FOR PUBLIC AWARENESS OF RADIOACTIVE SOURCES SECURITY

In this section, the researcher determines the participants' need for radioactive sources security awareness. Subsequent to answering the research questions, four themes were developed and matched with the objectives of the study based on the ten questions that were asked of the participants. Themes were generated from the analysis of the ten questions (Patten & Newhart, 2018:20), and similar questions were grouped together to achieve a specific objective. As Rossman and Rallis (2017:455) note, attentive analysis requires a keen awareness of the data and a focused attention on those data and their possible connections. The four themes that were generated were: 1) knowledge of radioactive sources security; 2) awareness of radioactive sources security and the nuclear industry; 3) radiological crime awareness; and 4) radioactive sources threat and risk assessment using the following security concepts:

4.5.1 Knowledge of radioactive sources security

This section addresses the first research objective of the study (see section 1.5.2).

4.5.1.1 Awareness of radioactive sources security

The participants were asked whether they knew about radioactive sources security. All fifteen study participants responded that they did not know about the security of radioactive sources. This initial response to the first question made it clear to the researcher that the study participants were unaware of radioactive sources and their security at their respective facilities. Radioactive sources are common in healthcare facilities and should be properly identified to ensure their security (see Section 3.3). They have different categorisations which determine their level of hazard (see section 3.4). The lack of knowledge of such sources may lead to instances where security personnel can handle the sources and endanger their lives (see sections 3.10.1.1 and 3.10.1.4).

4.5.1.2 Institutional disaster management plan / security policy / plan

Research participants were asked about the existence of a disaster management plan / security policy / plan. Participants 1, 3 and 5 said that they did not have one; Participants 2, 4 and 8 said they were not sure. Nine participants (Participants 6, 7, 9, 10, 11, 12, 13, 14 and 15) confirmed that they had either a disaster management plan or a security policy or plan. The disaster management plan or security policy or plan prescribes a series of actions to be taken in the event of an adverse event. As security personnel work around the clock at the facilities, they must know how to deal with an emergency situation. A lack of such information can mean the difference between life and death. As Bunn and Malin (2009:180) note, international nuclear security organisations (which include radioactive sources security) are weaker than nuclear safety because there has not yet been a significant nuclear security incident. Bunn and Malin (2009) contend that this has led many policymakers and nuclear managers to disregard the potential for nuclear or radiological threats and to assume that existing security measures are adequate. In order to secure radioactive sources, an organisation should have documented internal control measures that address either emergencies or security crises, documented processes in which the security of radioactive sources should be embedded and thus form part of the information about radioactive sources. According to Baillie and Sennewald (2021:95), policies, objectives, and procedures establish what, why and how management wants security for radioactive sources. Once these processes are established, employees are educated (policies), informed (objectives), and trained (procedures). Employees also learn what is expected of them, understand why a particular task is being done, and know how to do it. Having plans or policies in place is part of quality assurance that can contribute to a preventive approach that focuses on early reviews rather than corrective actions. This includes requirements for training, document control and records management, and the identification of deviations, among others (Mohamed, 2009:90). Plans also play an important psychological role in radiological incidents by supporting the actions to be taken during such incidents (Coleman et al., 2012:351).

4.5.1.3 The mention of radioactive sources in the institutional documents

Research participants were asked about the mention of radioactive sources in their respective institutional documents. An-depth probe on this question was conditional

on the answer in question two. If the participant answered no to question two, the researcher skipped question three and proceeded to question four. Only three study participants answered no (Participants 1, 2 and 15). Three participants said they were not sure (Participants 4, 5 and 6). Eight participants (5, 7, 8, 9, 10, 11, 12, 14) said that there was no mention of radioactive sources in either one of the documents. This was also underlined by Participant 3, who said that he had not seen any mention of the radioactive source in any of the organisational documents. Participant 13 also pointed out that radioactive sources are not mentioned in the aforementioned documents. This was another indication that respondents not only said no but were aware of the content of the documents in question. Without mention of radioactive sources, the attitude and behaviour of security personnel toward the security of radioactive sources will be inadequate and will not receive the proper attention that justifies the importance of the radioactive sources (IAEA Publication 7977, 2008:3). No matter where they are situated, radioactive sources are always potentially a danger. For this reason, it is necessary to provide information about them and the risks that are linked with them in some of the documents that are provided by the institution. Those who are counted on to take action in times of crisis can be given access to this information on a "need to know" basis (Shimura, Yamaguchi, Terada, Svendsen & Kunugita, 2015:425).

4.5.2 Awareness of radioactive source and the nuclear industry

This section addresses the second research objective (see section 1.5.2). All fifteen participants stated that they were not aware of the radioactive sources. The information related to radioactive sources, i.e., type, application and category, are open source information (see Table 3.2 and section 3.3). Without this information, it is not easy for the healthcare security personnel to comprehend and manage the threat and risks associated with radioactive sources (see section 3.8). The IAEA provides for the identification, monitoring, and combatting of illicit trafficking of such material (see section 3.8). It is important for security personnel to correctly identify radioactive sources in order to protect themselves and others from the harmful effects of radiation emitted from such sources.

4.5.2.1 Radioactive source awareness training

Participants in the study were questioned regarding their level of education and awareness regarding radioactive materials. Thirteen participants (1, 2, 3, 4, 6, 8, 9, 10, 11, 12, 13, 14, 15) claimed that they had never participated in training on radioactive source awareness, nor did they know anything about such an awareness. Participant 5 revealed an interest in the topic, despite having a limited understanding of the operations that take place within radiological facilities. The participant also made the observation that their radiological facilities have strong security, that confidentiality is preserved, and that information is only disclosed to those who have a "need to know." The organisation's security culture regarding radioactive sources is undermined as a result of this lack of understanding (IAEA Publication 7977, 2008).

Participant 7 shared more about how the security of the institution is related to the nuclear section, where radioactive sources are stored and used. First, the participant claimed that they were informed about the establishment of the nuclear section at the healthcare facility. The participant further emphasised that it was not training but some form of orientation (this may be well construed as a form of awareness to some degree). This means that they were only made aware of the existence of the nuclear section in their healthcare facility. Secondly, when asked how they conduct patrols around the nuclear section, the participant said that security personnel are not deployed at this facility during the night. Further questioning brought to light the types of security measures used to secure the facility, namely, locking with a key and burglar bars. In addition, another question was asked if security measures, such as CCTV (Closed Circuit Television), are used in the facility and the participant answered no.

From the responses of the two research participants (5 and 7), it became evident that security personnel are kept at arm's length when it comes to accessing radiological sections, which is a challenge and reinforces ignorance about the security of radioactive sources. This also illustrates the traditional attitude of keeping all information about nuclear and radiology as far away from the public as possible, including security personnel. According to WINS BPG 2.4 (2011:2), the traditional barriers that have supported secrecy and confidentiality are constantly challenged by legitimate and illegitimate sources. Stakeholders are forced to weigh the need for secrecy against the need for openness. The WINS perspective indicates that the

traditional approach is counterproductive and does not meet both the need-to-know and the need-to-inform. In addition, radiological information seems to be still regarded as only limited to personnel working at the radiology section. Therefore, during emergencies, the security staff at such institutions will not know how to respond to a radiological incident, or worse, they will not know how to protect themselves and others from radiological hazards.

4.5.2.2 Awareness of the nuclear industry organisations

In order to broaden the understanding of radioactive sources and acquire additional information on the subject, the nuclear sector includes a number of different stakeholders who can be contacted. In order to gauge the level of awareness exhibited by the participants, the following institutions were discussed:

a) **Nuclear Industry Association of South Africa** (**NIASA)** – Participants in the study were asked a question regarding their familiarity with NIASA. Fourteen participants who took part in the research (1, 2, 3, 4, 6, 8, 10, 11, 12, 13, 14, 15) reported that they were unfamiliar with NIASA. Participant 5 gave an affirmative response and, when questioned further, indicated that he had heard about it in the school that he had attended. NIASA comprises a number of organisations, groups, and individuals who have an interest in the nuclear industry. Its mission is to advance the standards for the creation and implementation of nuclear technology in South Africa (NIASA, 2022:np). According to WINS BPG 2.1 (2011:5), the nuclear sector includes a number of diverse stakeholders, all of whom, despite operating at various levels, require open and direct communication on security. A greater awareness of radioactive sources among the security personnel working in healthcare institutions can be achieved by knowledge of the relevant stakeholders.

b) **National Nuclear Regulator** (**NNR)** – Participants in the study were questioned regarding their familiarity with the NNR. Nine of the fifteen research participants who took part in the study (1, 2, 3, 4, 6, 8, 9, 11, 13) indicated they were familiar with the NNR, while the remaining five research participants who took part in the study (5, 10, 12, 14, 15) said they were not. The majority of the study participants learned about the NNR from the media, specifically, the television and the internet. Participant 7 showed that he was aware of the NNR by emphasising the fact that

he learned about it on TV while there were debates going on regarding the current national electrical problems. Information about nuclear regulatory announcements, public safety information forums where members of the public can learn about best practices in the nuclear industry, and how to effectively safeguard radioactive sources are all provided by the NNR (see section 3.14.2).

c) **PSIF** – Participants in the study were questioned regarding their familiarity with the PSIF. Twelve of the individuals (2, 3, 4, 5, 6, 9, 10, 11, 12, 13, 14, 15) responded with a no, stating that they were not familiar with the PSIF. Three individuals (1, 7, 8) reported that they had learned about the PSIF through television, the news, or the internet. According to the findings of the researcher, the participants are aware of it and have heard about it, but they have very little knowledge about it. It is possible that the PSIF only targets community members who live within a radius of less than 10 kilometres from the nuclear facility, which would explain the low reaction rate to knowing about it (see section 3.14.6.2). Healthcare security employees can learn a lot about the dangers of radioactive sources and how to protect themselves as members of the public using the PSIF platform, despite the fact that radioactive sources security information is not shared through the PSIF platform. The PSIF meetings are held in the provinces of Gauteng and the Western Cape, and the security staff of the healthcare facilities that were interviewed are welcome and encouraged to participate in order to expand their knowledge base.

d) **WINS** – Participants in the study were questioned regarding their familiarity with WINS. Only Participant 13 mentioned having heard about WINS through the media, both on television and through internet news sources. Based on the low number of responses received, it appears that the healthcare facilities that were interviewed have little understanding regarding the security of radioactive sources. When it comes to ensuring the security of radioactive sources, WINS has a lot to offer (see sections 3.8.6, 3.8.7, 3.8.8, 3.8.9, 3.8.10 and 3.8.11).

4.5.2.3 Awareness of the free online nuclear security discipline courses provided by the IAEA

Participants in the study were questioned regarding their awareness of the IAEA's free online nuclear security courses. None of the fifteen participants were aware that the

IAEA provided a free online course. This comment refers back to the responses that were supplied for question 1 (Annexure C), which stated that the security professionals at the chosen healthcare facilities were not aware of the radioactive sources security. The IAEA's courses in the area of nuclear security include essential information, notably linked to the security of radioactive sources (see sections 3.8.1, 3.8.2, 3.8.3, 3.8.4 and 3.8.5). The IAEA security courses deliver important and instructive security training programmes with an approach to risk management that effectively mitigates risks and influences the attitudes and behaviours of employees (WINS BPG 2.3, 2011:23).

Awareness and training regarding radioactive materials can be useful for healthcare security personnel in determining what to do about security for these areas that include how to: communicate the risk; understand the message that should be communicated; develop a planned communication strategy; and build capacity for risk communication. Awareness and training regarding radioactive materials can also be useful for determining communications (Shimura et al., 2015:426).

4.5.3 Radiological crime awareness

The theme of awareness of radiological crimes was the third objective of the study (see section 1.5.2).

4.5.3.1 Insiders as potential threats to radioactive sources

Study participants were asked whether they were aware of any criminal activity involving radioactive sources in South Africa or elsewhere in the world. None of the participants were familiar with criminal activity involving radioactive sources. Three study participants (Participants 4, 5, 6) answered no to this question. These participants indicated that insider threat is not possible at their institutions because there is a vetting process. Vetting is the thorough investigation of an individual, company, or other entity before a decision is made to undertake a joint project (Kopp, 2021:np). The WINS describes it as human reliability, in which a person's reliability and integrity are tested to determine his or her suitability for a particular position (WINS, 2018:3, 11). Participant 4 described the review process where each employee signs a confidentiality agreement and a follow-up is conducted every three years. This,

according to the participant, should be able to deter possible insider threats. Participant 5 also seemed to have confidence in the vetting process because he had never heard about security events in the radiology department.

The other twelve research participants (1, 2, 3, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15) answered the question in the affirmative, pointing out that there exists the possibility of an insider in their institutions. For instance, study Participant 1 cited challenges from visitors needing access to the facility as a potential threat because their motive for visiting the facility is not fully known while Participant 3 pointed out that those who work with radioactive sources pose a potential insider threat because they have knowledge of radioactive sources, while security personnel do not know about those sources. Participant 5 referred to physicians who work with these devices and have their own practices outside of healthcare facilities as potential insiders. Participant 7 mentioned inadequate technical security measures to prevent insiders and pointed out the challenge of securing information only through the use of security personnel. These participants mentioned the walkthrough metal detectors currently installed at the facility. This observation shows that the participant is able to distinguish the strengths and weaknesses of both human and technical security measures in protecting sensitive information or assets. Participant 8 backed up the facts by mentioning a theft that occurred at the facility where the participant works, where internal parts of the radiography machine were removed and stolen. These thefts may be directly attributed to those working within the radiological facility, as security personnel do not have access to it. Participant 9 concurred with Participant 3 and Participant 8 by saying that those who work with the equipment know about the machines, while security personnel have not been trained on radioactive sources and therefore cannot respond to questions about radioactive sources. In answering this question, Participant 10 focused on the sensitivity of information provided by healthcare clients and laboratories. This is the type of information that potential insiders can acquire and use unlawfully. Participants 11, 12, 13 and 14 pointed to the lack of vetting which could result in the failure to identify insider threats at the institution. Participants 11, 12, 13 and 14 mentioned the lack of vetting that could result in insider threats not being detected at the institution. Participant 15 said that it is not easy to detect people's motives, especially when they are looking for employment. Participant 9 was able to recall a criminal incident but was not sure of the details

thereof.

Some of the radiological events (see sections 3.10.1.1, 3.10.1.2, 3.10.1.3, 3.10.1.4, 3.10.1.5 and 3.10.1.6) point to an insider threat, either intentionally or accidentally. IAEA Publication 1858 (2008:np) addresses the identification of potential threats, situations to consider in insider threat analysis, identification of targets, measures against potential insider threats, and the evaluation of preventive and protective measures against insider threats. Because of the severity of the insider threats, it is essential for the security personnel working in healthcare facilities to be aware of the security threats that originate from within the organisation. These threats can include the actions or inactions of staff, the risks associated with managing major security improvement programmes, and failures in stakeholder engagement and communication (WINS BPG 2.6, 2019:6).

4.5.4 Radioactive sources threat and risk assessment using security concepts

The theme of radioactive source threat and risk assessment was intended to address the objective related to whether healthcare facilities work with government security agencies to assess the threat posed by radioactive sources. This was accomplished through the use of selected security concepts.

4.5.4.1 Awareness of security concepts related to radioactive sources security

There were different responses to security concepts:

a) Graded approach

Study participants were asked whether they were aware of the security concept of the graded approach. Of the fifteen research participants, none were familiar with the concept of the graded approach, as they all answered no. While participants made an effort to answer this question, it was clear that they were not familiar with it. A graded approach is concerned with the implementation of security measures commensurate with the value of the asset being protected. This forms part of the Physical Protection Systems (see section 1.8). If the participants had known about nuclear or radioactive sources security, they would have been familiar with it because it is commonly used in the nuclear industry to determine the level of protection of the asset. Radioactive sources require a certain level of protection based on a tiered approach.

b) Defence/protection in depth

Study participants were asked whether they knew the defence / protection in-depth security concept. Participant 8 showed some knowledge of what the concept means and mentioned that it concerns measures that are used to protect assets. Participant 13 explained that it refers to tools that are used to protect the institution's assets. Participant 14 was aware of the concept and mentioned that it refers to all security measures needed to protect valuable assets. The remaining participants answered no. The security principles that are well integrated include "defence in depth," which is the use of complementary security measures that eliminate single points of failure and integrate people, procedures, and processes (Garcia, 2008:98). Because of their hazardous nature, radioactive sources require several security measures to remain secured. One of the previous radiological incidents was due to a lack of defence / protection in depth and had fatal consequences (see section 3.10.1.6).

c) Security by design

Study participants were asked if they knew security by design. Study Participant 3 answered yes and alluded to the fact that this means a security design based on available resources in place during the design phase. Research Participant 7 believed it to be the security model used at an organisation to protect assets. Research Participant 8 responded by saying that it is a collective security system or security measures that are put in place to mitigate the risk identified. Research Participant 10

claimed that it is a layout concept upon which security is designed. Research Participants 11 and 13 thought it was about crime prevention through environmental design. Research Participant 12 replied that it is the institutional structure together with systems that promote the concept of the application of security. Research Participant 14 said it is the structural design that takes security into consideration. The rest of the research participants answered no. Judging by the participants' responses, not much is known about security by design.

According to WINS BPG 4.1 (2019:4), security by design is based on the concept that security should play an integral role in the design process from the outset. If the security function is not part of the facility design process from the beginning, security decisions will be made in the absence of security practitioners or omitted altogether. This creates a security vulnerability for the facility that may not be revealed until the vulnerability is exploited and requires a security retrofit in the future that may be more costly than if it had been considered during the design phase. Section 3.10.1 is a typical example of a facility where adequate security measures to secure a radioactive source in a public hospital have not been pre-established and designed. The recommended process of security by design includes building an organisation, understanding threats and consequences, establishing design objectives, and developing protection models. The protection model includes protection against theft and sabotage, development of the facility layout, and design for incident response (WINS BPG 4.1, 2014:6).

d) Detection

Study participants were asked if they knew the detection concept. Research Participant 3 alluded to the fact that it an electronic device designed to sense unauthorised motion upon entry at the premises. Participants 4, 5, 7 and 8 responded by referring to the use of metal detectors that could detect firearms and other contrabands. Participants 9 and 10 referred to motion detection of unauthorised persons on the premises by a device or sensor. CCTV was also mentioned by Participant 11 as a form of detection. According to Participant 12, it is an alarm that comes from a device that sends a signal when a security breach occurs. Detection should occur before intruders gain access to the premises or when an intruder approaches the security detection area and when the intruder is in an unauthorised or

restricted area. These were the views of Participants 13, 14 and 15. Most participants answered this question correctly, showing that they understood detection. This was one of the positive responses from most participants and subsequently means that healthcare security personnel will be able to recognise when there is unauthorised movement or entry into a radiology facility and will respond accordingly.

e) Delay

Study participants were asked whether they knew the concept of delay. Participant 3 knew what delay meant when he said that delay can be achieved by building a double fence around a facility. Research Participant 6 explained that security delay is used to reduce the speed at which the public attempts to gain unauthorised access to the facility. Participants 7, 10, and 11 mentioned security delays as a way to slow down intruders or fences that are put up to stop potential intruders. Research Participant 9 demonstrated knowledge of delays by stating that they are any physical measures developed at the facility to deter or delay criminals when they attempt to gain unauthorised access to the premises to conduct criminal activity. Research Participant 10 agreed with Participant 9 when he said that delay is trying to circumvent the adversary over and over again. According to Participant 14, delay is about 'the time it takes an intruder to gain access to or enter a protected area" (Garcia, 2008:187). On average, all participants were familiar with the concept of delay.

f) Response

The study participants were asked whether they were familiar with the response concept. All fifteen participants understood the concept of response. This is because most institutions, including all of the institutions studied, use this form of security service. Furthermore, the armed response course is offered by the PSIRA (2022:np) in addition to the security grades. Knowledge and understanding of response means the timely disruption of an adversary's actions by on-site guards, local police, and others before the target is reached (Garcia, 2008:219).

4.5.4.2 Security risk assessment

Study participants were asked whether they were aware of the risk assessment conducted by the state security agencies at their respective facilities. Of the fifteen

study participants, five study participants (1, 4, 5, 9 and 11) answered no. All other participants answered yes to the questions and confirmed that they observed the authorities conducting the threat assessment. However, none of the study participants confirmed that they were aware of a radioactive source risk assessment or witnessed the assessment in the radiological department. One of the reasons for this is that security personnel are not allowed to enter the radiological department unless there is a request from radiological department personnel, who would then escort security personnel in and out if security is needed in the section. It is essential that security personnel in healthcare facilities be familiar with security risk or threat assessment as a systematic process for identifying and describing the motivation, intentions, and capabilities of a potential or credible threat that may come from either inside or outside the facility and that may attempt to take malicious action against the facility (WINS BPG 2.5, 2010:4).

4.6 CONCLUSION

In this chapter, the research participants' responses from the in-person and telephone interviews were interpreted and analysed. The interpretations and analyses were made by linking the empirical results of the study as sources of information with the researcher's contribution to explaining the findings of the research participants. This chapter discussed the themes that were identified after the transcripts were arranged. Following the interviews, four themes were formulated and the research questions were assigned to the corresponding themes.

CHAPTER 5
SUMMARY OF FINDINGS, ACHIEVEMENT OF AIM, RECOMMENDATIONS AND CONCLUSION

5.1 INTRODUCTION

The purpose of this study was to examine: the need for radioactive sources security awareness in healthcare facilities; the level of knowledge that healthcare security personnel have about radioactive sources; the question of whether or not they have received training or awareness of radioactive sources security in the past; and the radiological security risk that is associated with radioactive sources. The exploratory aspect of the research approach used in this study, which was of a qualitative nature, was utilised by the researcher.

The researcher conducted interviews with security personnel at the selected healthcare facilities in Gauteng, South Africa. As indicated by the data collected (see section 4.4.1.1), the security of radioactive sources was relatively unknown among the healthcare security personnel. The research was conducted in accordance with the objectives of the study. In addition, the limitations of the study, identified by the researcher, are discussed. Based on the findings, recommendations are made to address the deficiencies identified during the research, the development of a radioactive sources security awareness programme for healthcare security personnel, the state security agencies, the service providers and healthcare workers who are responsible for securing radioactive sources in their areas of responsibility and who can work hand-in-hand with security personnel at their facilities. A total of fifteen participants were interviewed from five healthcare facilities and these included Security Investigators, a Control Room Operator, Security Supervisors, Security Managers, Security Shift Leaders, Chief Security Officers, an Assistant Director, a Security Shift Leader and Deputy Directors.

The following is a synopsis of the research findings, the achievement of the study's aim, recommendations, and the conclusion of the study:

5.2 SUMMARY OF RESEARCH FINDINGS

The purpose of this section is to present a summary of the research findings related to the similar and dissimilar findings. These findings are based on the research participants' responses to the themes identified by the researcher.

5.2.1 Similar findings

From the face-to-face and telephone interviews conducted between the researcher and research participants, the following similar findings emerged:

- All research participants were of African descent;
- They all worked in the security industry;
- All, except PSIRA Grade B, were registered as PSIRA Grade A;
- They all had post-matric qualifications with a focus on security management;
- While participants were aware of the radiology department at their facilities, the study participants were unaware of the radioactive sources security;
- All research participants were unable to recall the mentioning of radioactive sources in both disaster management and security policy or plan;
- Research participants were not aware of the Public Safety Information Forum;
- Participants who said that there was no potential insider threat in their institutions, substantiated their responses with the availability of vetting processes in their institutions;
- None of the study participants had taken part in radioactive source awareness training;
- Research participants were not aware of the WINS;
- None of the participants were aware of the IAEA's free online nuclear security courses.

5.2.2 Dissimilar findings

From the face-to-face and telephone interviews conducted between the researcher and research participants, the following dissimilar findings emerged:

- Study participants varied in their knowledge of whether their institutions had disaster management and/or a security policy, with some having disaster management and a few having a security policy. However, some did not know if their institutions had one or both;
- The research participants gave different answers to the question of whether an insider was a potential threat to their organisation and gave different reasons for their answers;
- There were mixed responses when asked about criminal activity or threats against radioactive sources as most had never heard of such threats or thefts of radioactive sources;
- There were also different answers to the question about the application of security concepts;
- Most study participants were unaware of the risk assessment conducted by the state security agencies in their institutions, but a few had some idea, especially those who held higher positions.

5.2.3 General findings

- The responses of the research participants showed that all study participants were unaware of the security of radioactive sources. The responses also showed that the participants did not know what a radioactive source was, even though radioactive sources were present in their radiology departments at their respective facilities. This was concerning because security personnel are amongst first responders during an emergency at these facilities, especially the emergencies with malicious intent.
- All participants indicated that there was no mention of radioactive sources in their emergency planning and/or security policy/plan. The lack of mentioning of radioactive sources adds into the plight of the security in case of an emergency.
- The other finding was that of different responses when it came to insider threats. While some had an understanding of insider threats, other research participants showed more confidence in the vetting programme, which made them believe that it does prohibit or eliminate insider threats. Some believed

that insider threats would mainly be visitors, instead of looking internally at the employees of their organisations, including themselves. According to IAEA Publication 1858 (2008:5), an insider could be someone who has access to, among other things, facility systems, transportation arrangements, physical protection procedures, and technical capabilities. Ciampa (2017:22) gives an example of a healthcare worker upset about an impending layoff who might illegally collect health data from celebrities and sell it to the media.

- Although there are several free online nuclear security courses from the IAEA that are available to the public, whether they work in the nuclear industry or not, not all participants were aware of them. Participants' responses also indicated that the WINS was not fully known, with the exception of a few who happened to hear about it in the news or online.
- In South Africa, there are a number of public actors in the nuclear industry, such as the NNR, NIASA, and PSIF. Although these are local entities, the responses seemed to indicate that participants did not fully understand who these stakeholders are, what they stand for and what their role is with respect to radioactive sources.
- Another finding was the threat and risk assessment by government security agencies. Respondents' answers indicated that such assessments are conducted, but that they were all unaware of the threat assessment for radioactive sources. While the radiological assessment is confidential, higher level security personnel, such as a Deputy Directors, should be aware of such an assessment. The WINS states that overprotection of information is counterproductive and should be prevented at all costs.
- Security concepts also play an important role in securing radioactive sources. In this study, a few security concepts were posed as questions to the research participants. Participant responses were positive, but certain nuclear security concepts were not understood by the participants as they had not participated in nuclear/radioactive source training or awareness. Understanding these concepts would allow security managers to contribute to the risk assessment associated with radioactive sources used at their facilities.
- Theft and sabotage are major risks for radioactive sources. Since the

radiological incident at a hospital in Goiana, Brazil, in 1987 (IAEA Publication 815, 1988) (and several other radiological incidents that occurred thereafter), this information has been in the public domain, but some thirty-five years later (2022), healthcare security personnel are unaware of these incidents. This observation is indicative of the lack of awareness of radioactive sources among stakeholders outside the nuclear field, such as hospitals and higher educational institutions.

The findings of the study were expected to show whether the aim and objectives of the study were achieved.

5.3 ACHIEVEMENT OF AIM AND OBJECTIVES

This study aimed to explore the radioactive sources security awareness at healthcare facilities. To achieve the study's aim (see section 1.5.1), the objectives (see section 1.5.2) needed to be met as detailed below.

5.3.1 To determine participants' level of knowledge about radioactive sources security

To achieve this objective, the primary question of the study was used to guide the study of the level of awareness of radioactive sources security (see section 1.6.1). The primary question was followed by the secondary questions (see section 1.6.2), which were used to further specify the research question to achieve this objective. Fifteen research participant responses indicated a lack of awareness of radioactive sources security, even with publicly available information. The selection of participants (see section 2.6) and the unit of analysis (see section 2.7) assumed that participants worked in an environment where radioactive sources were prevalent and therefore they would be aware of these sources. Fischer, Grau and Roper (2006:89) indicate that security awareness means being aware of potential risks, hazards, or real threats to life, safety, or valuable property, which translates into actions or behaviours that counteract those risks and threats. According to IAEA Publication 1309 (2007:3), the radiological threat has continued to increase since early 1990, and terrorists have attempted to acquire such material. These threats include criminal or unauthorised acts which could result in a radiological incident (see section 1.4).

5.3.2 To verify whether the participants were already informed about the security of radioactive sources

From the outset, the motivation of the study was to determine whether the participants were informed, aware or trained about radioactive sources security (see section 1.1). The rationale for the topic also shows the researcher's efforts to indicate the need for the awareness of radioactive sources security (see section 1.2). This study objective was met in that the study was able to determine whether the participants were aware or not aware of radioactive sources security. According to the participants' responses, none of the participants had been through radioactive sources security training or formal awareness. Security personnel are part of the radioactive source owner (see section 3.6), as they are responsible for the security of radioactive sources on site. South Africa has a Code of Conduct for the Security of Radioactive Sources (see section 3.10.1), which provides educational information on the security of radioactive sources. Failure to train officers on the security of radioactive sources may result in them not knowing they type of threats and risks they are facing and how to counteract them (WINS BPG 2.6, 2019:4).

5.3.3 To determine the general awareness of criminal activity associated with radioactive sources

This study objective was met in that participants were asked about criminality around radioactive sources. The participants did not recall a radiological incident, either locally or abroad. In all chapters of this study, radioactive sources security appeared to be a lesser known phenomenon. This also confirms the claims made in the WINS BPGs (see sections 3.8.6, 3.8.7, 3.8.8, 3.8.9, 3.8.10) that nuclear security information is not readily available to the security departments of the various institutions. Of the fifteen participants, only one (Participant 9) recalled an incident that had occurred at one of the nuclear facilities in South Africa (see section 4.4.3.1). In order to create awareness, the radioactive sources security awareness has been recommended in this study (see section 5.4).

5.3.4 To determine whether healthcare facilities are working with government security agencies to assess the threat posed by radioactive sources

This study objective was met in that the study participants, who were in managerial

positions, were familiar with the threat and risk assessment conducted by government security agencies, even if they could not confirm that the threat and risk assessment included radioactive sources (see section 1.2). The selection of participants (see section 2.6) and the unit of study (see section 2.7) were based on the type of participants who were presumably knowledgeable about radioactive sources and the assessment of their threat and risk. In addition, the threat and risk assessment would highlight the drawbacks of radioactive sources if they fall into the wrong hands (see section 3.8). To address this challenge, this study recommends a radioactive source self-assessment programme (see section 5.4.1.7).

5.4 RECOMMENDATIONS

Based on the literature and empirical findings of the study (see Chapters 1–4), the following recommendations are made:

5.4.1 Radioactive sources security awareness programme for healthcare facilities

Based on the research, this study recommends that a radioactive sources security awareness programme be established and implemented for healthcare facilities that use radioactive sources. It is recommended that the awareness programme includes:

5.4.1.1 Nuclear security

It is imperative that security personnel are able to prevent, detect and respond to criminal activities that are directed at the radioactive sources used at healthcare facilities. Radioactive sources require specific knowledge to secure them appropriately. The IAEA Publication 1481 (2011:5) contains recommendations on the physical protection of nuclear material and nuclear facilities. Garcia (2008:4) provides an in-depth discussion of the components of a physical protection system (PPS), which includes the following: establishing PPS objectives; designing the system to achieve the established objectives; and evaluating the performance of the system in comparison to the established objectives.

5.4.1.2 Identification of radioactive sources

The identification of radioactive sources includes identifying radioactive devices,

radioactive sources, transport packages and the transportation thereof (IAEA Publication 1278, 2007:9). Most of the radiological incidents mentioned in Chapter 3 (see section 3.3) were due to ignorance of radioactive sources by the victims. This is a major risk, considering that radioactive sources can be used to harm people if they fall into the wrong hands or mishandled.

5.4.1.3 Categorisation of radioactive sources

The categories of radioactive sources improve control over radioactive sources, security measures for radioactive sources against the possibility of misuse for malicious purposes, emergency planning and response, and the appropriate categorisation of radioactive sources that are used for medical treatment, academic research, and educational purposes (IAEA Publication 1227, 2005:3). The knowledge of the various categories is helpful for choosing a graded approach to selecting security measures when viewed from a security standpoint. It is important for those who work in the security of healthcare facilities to have an understanding of the many types of radioactive sources and the level of danger posed by each. For instance, $^{CO}60$ and Cesium137 are frequently utilised in healthcare institutions for the detection and treatment of cancer from patients; these two substances are also known for contributing to earlier radiological incidents.

5.4.1.4 Nuclear industry stakeholders

In order to be effective, the awareness programme needs to involve a wide variety of stakeholders from both inside and outside of the nuclear industry. The knowledge base of healthcare security professionals will improve as a result of the awareness of these stakeholders regarding the security of radioactive sources at their particular facilities and the course of action that should be taken in the event of radiological incidents. The WINS BPG 2.4 (2011:5) provides a list of the many stakeholders involved. These stakeholders are as follows:

- **Within the organisation**: These include members of the board of directors and senior management, members of senior management and staff, and professionals in security. In addition, senior management at healthcare facilities needs to be educated about the programme in order to establish a standard for

participation at the highest possible level of the organisation.

- **Communicating with the regulator:** The role of SAHPRA as the regulator needs to be incorporated into the programme.
- **Communicating with government agencies:** In South Africa, the relevant government agencies would be: the State Security Agency (SSA), which is responsible for information security; the South African Police Services (SAPS), which is responsible for physical security threat and risk assessment; the Department of Health, which is responsible for regulating radioactive sources through SAHPRA; and the National Radioactive Waste Disposal Institution, which regulates radioactive waste disposal.
- **Communicating with local communities:** These stakeholders are members of the organisation's staff and have the organisation's best interests at heart. They are an integral part of the organisation.
- **Communicating with peer organisations:** This could be communication between health facilities that use radioactive sources by forming industry organisations that meet to discuss security-related topics and to compare and benchmark their practices
- **Communicating with media:** The establishment of a relationship, trust, and an open exchange of information between the organisation and the media. In the event that something goes wrong, a lack of communication could bring about negative publicity for the organisation.

5.4.1.5 Nuclear security culture

An adequate nuclear security culture should guarantee that the implementation of nuclear security measures receives the attention that is proportionate with the importance of these measures, as stated in the IAEA Publication 1347 (2008:3). It is essential that the awareness programme addresses the culture of nuclear radioactive sources security in order to ensure that the attitudes and behaviours of individuals and organisations support that culture. This can be accomplished by ensuring that the programme addresses the culture of nuclear security.

5.4.1.6 Insider threat

The organisation's employees are among those who can harm the organisation because their loyalty cannot be guaranteed by being the employees of the organisation (Cole & Ring, 2006:4). While it was evident that healthcare facilities have internal procedures in place to verify loyalty, healthcare security personnel need to be more educated about the threat of insiders, namely, their characteristics, advantages, categories and motivations (IAEA Publication 1858, 2008:7–8).

5.4.1.7 Self-assessment

Self-assessment raises security awareness according to the individual's specific roles and responsibilities and may focus on a selected group of employees who have direct relationships with radioactive sources. All WINS BPGs have self-assessment appendices that can assist in designing the self-assessment for this programme.

5.4.2 Personal development of healthcare security professional regarding radioactive sources security

As much as the recommended radioactive sources security programme would help healthcare professionals become familiar with radioactive sources security, personal development is also recommended for individuals to become certified and competent in nuclear security. Below are some of the educational opportunities that healthcare security personnel can take advantage of:

- Register with IAEA free online security courses

  Security management and healthcare facility personnel need to become familiar with nuclear security by taking the initiative to study it online, for free. The information contained in these courses is essential to understanding nuclear security.

- Familiarisation with IAEA NSS publications

  The IAEA NSS publications provide valuable insights into nuclear security but more especially the identification and security of radioactive sources.

- Register free membership with WINS

WINS have several best practice guides regarding nuclear security. Registering with WINS as a member would give access to these best practices.

- Apply for WINS Academy scholarship

  WINS Academy scholarship can be applied for after registering as a member. There are about ten nuclear security modules and specialisations to choose from. The researcher has had the opportunity to register and be certified as a Nuclear Security Professional in all ten modules (WINS Academy, 2018).

The aforementioned recommendations for the contents of the radioactive sources security programme are by no means exhaustive; other topics may be identified and be included in the programme; however, those mentioned would serve as a basis for the education of security personnel on radioactive sources. Publications are available from both the IAEA and the WINS, and they can be explored for additional content to incorporate into the programme.

The limits of the study are one of the factors that may make it more difficult to accomplish the study's aims and objectives than was originally anticipated. The following list presents the limitations that applied to this study:

5.5 Limitations of the study

The researcher needs to be aware of the limitations of the study since they are a weakness of the study itself or the topic being studied (Bairagi & Munot, 2019:50). It is essential for the researcher to be aware of the limitations of the study and to make them known, despite the fact that this may affect his/her credibility (Babbie, 2021:71). Rossman and Rallis (2017:240) postulate that the limitations are about identifying the weaknesses of the study and point out that other disadvantages include having a small sample size, relying on only one method for data collection, and having a selection procedure. As a direct consequence of this, every study produces conclusions that are provisional and conditional. There are certain limitations in the reporting of the findings of this study, which were discovered during the research process. These are described below:

- **Small sample size**

According to Braun and Clarke (2013:80), the scope of the study is restricted by both the size and the number of participants in the research sample. This study was only conducted at certain healthcare facilities and was restricted to the province of Gauteng. As a result, the findings of this research cannot be extrapolated to the entire country of South Africa nor to any of the other provinces in the country where radioactive sources are also employed. It is also important to point out that the scope of the research was restricted to healthcare facilities located within public institutions. Because private medical institutions were excluded from the study, the findings may have been interpreted differently had they been included. Because the researcher chose to conduct the study using a purposeful sampling strategy in order to attain the desired outcomes of the research, private healthcare facilities were not included in the sample.

- **Interviews as limitation:** Creswell (2014:241) points out interviews as having a number of limitations which are:
  - Provides indirect information, filtered through the views of participants:

    The majority of participants were aware of the radiological departments housed within their respective institutions; nonetheless, they were unable to answer questions from either a nuclear or radiological perspective. The researcher attempted to overcome this issue by concentrating on the participants' prior knowledge before they entered the radiology department. This was done in order to have an understanding of the radiology department from their point of view.

  - The presence of the researcher can distort the responses

    During the interviews, it became clear that this was the case since some of the participants exhibited signs of discomfort in response to particular questions, possibly because they did not like to appear embarrassed in front of the researcher. Because this was the first study of its sort to be conducted in South Africa, the researcher reassured the participants on multiple occasions that they should not feel humiliated if they did not know some of the answers to specific questions.

- Not all people are articulate and perceptive

  In the course of the interviews, this proved to be one of the most difficult problems, as the majority of the participants were required to communicate in English, even though it was not their first language. In order to get around this restriction, the researcher made it possible for the participants to communicate in their mother tongue in some situations, which was understood by both the participant and the researcher.

- Interruptions during interviews

  Even though interviews were carried out with all participants until every question was answered, there were interruptions since some participants had to attend official appointments. Power outages also affected telephone interviews that had to be restarted.

- **Lack of radioactive sources security publications**

The IAEA and the WINS are the only two organisations from which the researcher was able to readily access publications and best practices information related to radioactive sources security. This is a problem that is not exclusive to South Africa, but internationally. Because of this, the research utilised data sources, such as radioactive source material that was acquired from the internet.

- **Lack of knowledge of radioactive sources by healthcare facilities' security personnel**

Due to the fact that this qualitative study concentrated on only five healthcare facilities in the Gauteng Province, it is not possible to make any broad conclusions or generalise the findings to other locations. The amount of data provided by healthcare facility security staff was another limitation of the study. The majority of these individuals had not received training or had been formally introduced to radioactive sources security and were unfamiliar with the phrases "radioactive source" and "radioactive sources security". Formal security training that is related to the security of nuclear power plants or radioactive sources is not available at universities in South Africa, the PSIRA (2022:np), or SASSETA (2022:np). The utilisation of outdated sources, in particular those relating to nuclear security, was another obstacle that contributed to the

limitations of the study. The majority of nuclear-related sources, including those from the IAEA, date back to 1988, for instance, the Goiania radiological accident. Other sources that led to restrictions were the IAEA's Techdocs and the NSS that range from 2006 to 2020.

5.6 RECOMMENDATIONS FOR FUTURE RESEARCH AND ADVANCEMENT

The following recommendations are offered for consideration in future research:

- Extend participation to include other provinces in South Africa that use radioactive sources to raise awareness among all healthcare providers.
- Include private healthcare facilities where radiology is widely used, and where security officials are more familiar with radiology departments.
- Include non-security personnel working in radiology departments. Security of radioactive sources should not be the responsibility of the organisation's security department, but the responsibility of all including include facility managers and other radiology staff such as radiographers and medical doctors.
- Include law enforcement officials, i.e., South African Police Service and traffic police as these are outside responders who would be called to the scene during emergencies.
- Security exercises and models should be tested by healthcare workers and the nuclear industry to allow healthcare workers to understand the magnitude of a radiological event and be prepared for related eventualities.
- The University of South Africa needs to explore the possibility of including nuclear security in its security management programme under the module “Industrial Security”. This can start as a chapter and develop into a stand-alone module and a possible academic course that can be pursued as a specialisation. Such development can be achieved by working with Kings College London's Professional Development Course, which is offered with certain colleges in South Africa.

5.7 CONCLUSION

The chapter commenced with a summary of the research findings to remind the reader

of the main empirical findings of the study. The achievement of the aim and objectives were outlined in-depth confirming that the study had achieved its set out goals. Thereafter, recommendations were made for relevant role players and the limitations of the study were declared. To support forthcoming research endeavours, recommendations for future research and advancement were made.

The nuclear industry predicts that a big nuclear or radiological security event will take place in the future. The way an organisation responds to such an event necessitates awareness and training on the part of security officers and professionals in radiological departments. Additionally, individuals who are responsible for radioactive sources need to be competent and have emergency preparedness plans in place. According to the findings of this study, the leading cause of radioactive source injuries and deaths is a lack of awareness of radioactive sources. As a result, the dissemination of information regarding radioactive sources is necessary. A heightened level of awareness can facilitate the proactive protection of facilities against the possibility of criminal activity and the unintentional loss or misuse of radioactive sources. As informed by theoretical and empirical data, this study contributes to academia, healthcare facilities, security professionals and the nuclear industry.

REFERENCES

Acharyya, R. & Bhattacharya, N. 2019. *Research methodology for social sciences*. London: Routledge.

Allen, M. **2**017. *The Sage Encyclopedia of communication research methods* (Vol. 1). Thousand Oaks, CA: Sage.

Arms Control Association. 2015. *Illicit traffickers arrested in Moldova*. [Online]. Available at: https://www.armscontrol.org/act/2015-01/news-briefs/illicit-traffickers-arrested-moldova (Accessed on 05 January 2022).

Babbie, E. 2021. *The practice of social research* (15th ed.). Boston, MA: Cengage.

BBC NEWS. 2013. *Public warning over theft of radioactive items*. [Online]. Available at: https://www.bbc.com/news/world-europe-24365469 (Accessed on 05 January 2022).

Bachman, R. & Schutt, R.K. 2008. *Fundamentals of research in criminology and criminal justice* (2nd ed.). Thousand Oaks, CA: Sage.

Bachman, R.D. & Schutt, R.K. **2**018. *Fundamentals of research in criminology and criminal justice* (4th ed.). Thousand Oaks, CA: Sage.

Baillie, C. & Sennewald, C.A. 2021. *Effective security management* (4th ed.). Oxford: Butterworth-Heinemann.

Bairagi, V. & Munot, M.V. 2019. *Research methodology: A practical and scientific approach*. London: CRC Press.

Bassot, B. 2020. *The research journal: A reflective tool for your first independent research project*. Bristol, UK: Polity Press.

Behar-Horenstein, L.S. 2018. Qualitative research methods. In B.B. Frey (Ed.), *The SAGE encyclopedia of educational research, measurement, and evaluation*. Thousand Oaks, CA: Sage.

Berg, B.L. & Lune, H. 2017. *Qualitative research methods for the social sciences* (9th

ed.). London: Pearson Education.

Biel, L., Engberg, J., Ruano, M.R.M. & Sosoni, V. **2**019. *Research methods in legal translation and interpreting: Crossing methodological boundaries*. London. Taylor and Francis Group.

Bogdan R., DeVault, M.L. & Taylor, S.J. 2016. *Introduction to research methods: A guidebook and resource* (4th ed.). Hoboken, NJ: John Wiley & Sons.

Bordens, K.S. & Abbott, B.B. 2018. *Research design and methods: A process approach* (10th ed.). New York: McGraw Hill Education.

Braun, V. & Clarke, V. **2**006. *Using thematic analysis in psychology*. Auckland, New Zealand: The University of Auckland.

Braun, V. & Clarke, V. **2**013. *Successful qualitative research: A practical guide for beginners*. Thousand Oaks, CA: Sage.

Bricker, M.K. 2014. *The Fukushima Daiichi nuclear power station disaster*. London: Routledge.

Brink, H., Van der Walt, C. & Van Rensberg, G. 2018. *Fundamentals of research methodology for health care professionals*. Cape Town: Juta.

Britannica. 2022. Sv. 'Half-life radioactivity'. [Online] Available at: https://www.britannica.com/science/half-life-radioactivity (Accessed on 10 February 2022).

Bryant, A. & Charmaz, K. 2019. *The SAGE Handbook of current developments in grounded theory*. Thousand Oaks, CA: Sage.

Bunn, M. & Malin, M.B. **2**009. Enabling a nuclear revival – and managing its risks. *Innovations: Technology, Governance, Globalization*, 4(4):173–191. [Online]. Available at: https://doi.org/10.1162/ITGG.2009.4.4.173. (Accessed on 18 December 2022).

Business Research Methodology. n.d. *Formulating research aims and objectives*. [Online]. Available at: https://research-methodology.net/research-

methodology/reserach-aims-and-objectives/ (Accessed on 16 January 2020).

Butler, R. 2000. *The greatest threat: Iraq, weapons of mass destruction, and the growing crisis of global security.* Foreign Affairs. Available at: https://www.foreignaffairs.com/reviews/capsule-review/2000-09-01/greatest-threat-iraq-weapons-mass-destruction-and-growing-crisis (Accessed on 16 January 2020).

Cann, M., Davenport, K. & Parker, J. 2016. *The nuclear security summit: Accomplishments of the process*. Arms Control Association. Available at: https://www.armscontrol.org/reports/2016/The-Nuclear-Security-Summits-Accomplishments-of-the-Process#:~:text=Among%20the%20summits'%20chief%20accomplishments,and%20security%20by%20most%20states (Accessed on 16 January 2020).

Ciampa, M. **2**017. *Security awareness: Applying practical security in your world* (5th ed.). Boston, MA: Cengage Learning.

CNN Editorial Research. 2021. *September 11 hijackers fast facts*. [Online]. Available at: https://edition.cnn.com/2013/07/27/us/september-11th-hijackers-fast-facts/index.html (Accessed on 05 January 2022).

CNS Global Incidents and Trafficking Database. 2017. *Nuclear and other radioactive material incidents reporting*. Available at: https://www.nti.org/analysis/articles/cns-global-incidents-and-trafficking-database-archived-reports-and-graphics/ (Accessed on 05 January 2023).

Cohen, L., Manion, L. & Morrison, K. 2018. *Research methods in education* (8th ed.). London: Taylor and Francis.

Cole, E. & Ring, S. 2006. *Insider threat: Protecting the enterprise from sabotage, spying, and theft*. Oxford: Syngress Publishing.

Coleman, C.N., Adams, S., Adrianopoli, C., Ansari, A., Bader, J.L., Buddemeier, B., … Yeskey, K. **2**012. Medical planning and response for a nuclear detonation: A practical guide. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 10(4):346–371. [Online]. Available at:

https://doi.org/10.1089/BSP.2012.1025. (Accessed on 19 December 2022).

Colling, R.L. & York, T.W. 2010. *Hospital and healthcare security* (5th ed.). Massachusetts. Oxford: Butterworth-Heinemann.

Cooper, J.R., Randle, K. & Sokhi, R.S. 2003. *Radioactive releases in the environment: Impact and assessment.* Hoboken, NJ: John Wiley & Sons.

Costley, C. & Fulton, J. 2019. *Methodologies for practice research: Approaches for professional doctorates*. Thousand Oaks, CA: Sage.

Creswell, J.D., Brown, K.W. & Rian, R.M. **2**017. *Self-determination theory: Basic psychological needs in motivation, development and wellness*. New York: The Guilford Press.

Creswell, J.W. **2**014. *Research design: Qualitative, quantitative, and mixed method approaches*. Thousand Oaks, CA: Sage.

Creswell, J.W. 2018. *Qualitative inquiry & research design: Choosing among five approaches* (4th ed.). Thousand Oaks, CA: Sage.

Creswell, J.W. & Poth, C.N. 2018. *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Thousand Oaks, CA: Sage.

Council of the European Union. 2019. Nuclear Security Summit, The Hague, 24–25 March 2014. [Online]. Available at: https://www.consilium.europa.eu/en/meetings/international-summit/2014/03/24-25/ (Accessed on 22 December 2021).

Durdella, N. **2**019. *Qualitative dissertation methodology: A guide for research design and methods*. Thousand Oaks, CA: Sage.

Efron, S.E. & Ravid, R. 2019. *Writing the literature review: A practical guide*. New York: The Guilford Press.

Eskom. n.d. *Koeberg Nuclear Power Plant*. [Online]. Available at: http://www.eskom.co.za/Whatweredoing/ElectricityGeneration/KoebergNuclearPowerStation/Pages/Koeberg_Power_Station.aspx. (Accessed on 12 October

2020).

Fay, J.J. 2007. *Encyclopaedia of security management* (2nd ed.). Burlington, MA: Butterworth-Heinemann.

Ferguson, C.D. & Potter, W.C. 2004. *The four faces of nuclear terrorism.* Montery, CA: Center for Nonproliferation Studies.

Fischer, L., Grau, J.A. & Roper, C. 2006. *Security education, awareness and training: From theory to practice*. Burlington, MA: Butterworth-Heinemann.

Floyd, J. & Fowler, J. 2014. *Survey research methods* (5th ed.). Thousand Oaks, CA: Sage.

Fuhrmann, M. & Stulberg, A.N. 2013. *The nuclear renaissance and nuclear security*. Stanford, CA: Stanford University Press.

Garcia, M.L. 2006. *Vulnerability assessment of physical protection systems*. Oxford: Butterworth-Heinemann.

Garcia, M.L. 2008. *The design and evaluation of physical protection systems*. 2nd Ed. Massachusetts: Elsevier Butterworth-Heinemann.

George Mason University. 2018. *How to write a research question*. The Writing Center. [Online]. Available at https://writingcenter.gmu.edu/guides/how-to-write-a-research-question (Accessed on 16 July 2020).

Gill, A.S. 2020. *Nuclear Security Summits: A history*. London: Palgrave Macmillan.

Given, L.M. 2008. *The Sage Encyclopedia of qualitative research methods* (Vol. 1&2). Thousand Oaks, CA: Sage.

Goon2345. 2012. 2012 *Nuclear Security Summit* (*Seoul Communique)*. [Online]. Available at: https://goon2345.wordpress.com/2012/03/27/2012-nuclear-security-summit-seoul-communique/ (Accessed on 22 December 2021).

Greetham, B. 2021. *How to write your literature review*. London: Red Globe Press.

Hammond, M. & Wellington, J. 2021. *Research methods: The key concepts* (2nd ed.).

New York: Taylor & Francis Group.

Herzig, T.W. 2010. *Information security in healthcare*. Managing risk. New York: Taylor & Francis.

IGI Global. n.d. *What is higher education institution*. [Online]. Available at: https://www.igi-global.com/dictionary/higher-education-institution/13096 (Accessed on 03 June 2021).

Inside Radiology. 2016. *Radiographer***.** Medical Imaging Technologist. [Online]. Available at: https://www.insideradiology.com.au/radiographer-medical-imaging-technologist/ (Accessed on 11 August 2021).

International Atomic Energy Agency (IAEA). 1957. *The Statute of the IAEA*. [Online]. Available at: https://www.iaea.org/about/statute#a1-20 (Accessed on 15 November 2020).

International Atomic Energy Agency (IAEA). 1988. *The radiological accident in Goiania.* [Online]. Available at: https://www-pub.iaea.org/mtcd/publications/pdf/pub815_web.pdf (Accessed on 13 June 2021).

International Atomic Energy Agency (IAEA). 2005. *Safety Standards Series No. RS-G-1.9.: Categorisation of radioactive sources.* [Online]. Available at: https://www.iaea.org/publications/7237/categorization-of-radioactive-sources (Accessed on 14 October 2021).

International Atomic Energy Agency (IAEA). 2020. *Nuclear Security Glossary Draft.* [Online]. Available at: https://www.iaea.org/sites/default/files/21/06/nuclear_security_glossary_august_2020.pdf. (Accessed on 12 December 2020).

International Atomic Energy Agency (IAEA). 1995. *International Physical Protection Advisory Service.* [Online]. Available at: https://www.iaea.org/services/review-missions/international-physical-protection-advisory-service-ippas (Accessed on 15 December 2021).

International Atomic Energy Agency (IAEA). 2021*. Nuclear Security Series*. [Online]. Available at: https://www.iaea.org/resources/nuclear-security-series (Accessed on 26 July 2021).

International Atomic Energy Agency (IAEA) NW-T-1.3. 2014b. *Regulatory Control for the Safe Transport of Naturally Occurring Radioactive Material: Report of a coordinated research project 2007–2010*. [Online]. Available at: https://www.iaea.org/publications/10582/management-of-disused-sealed-radioactive-sources (Accessed on 25 October 2021).

International Atomic Energy Agency (IAEA) NW-T-1.3. 2014a. *IAEA Nuclear Energy Series: Management of disused sealed radioactive sources*. [Online]. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1657_web.pdf (Accessed on 02 August 2021).

International Atomic Energy Agency (IAEA) Publication 815. **1**988). *The radiological accident in Goiania.* [Online]. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub815_web.pdf (Accessed on 20 July 2022).

International Atomic Energy Agency (IAEA) Publication 1097. 2000. *The radiological accident in Lilo.* Available at: https://www.iaea.org/publications/5968/the-radiological-accident-in-lilo (Accessed on 05 January 2023).

International Atomic Energy Agency (IAEA) Publication 1124. 2002. *The radiological accident in Samut Prakarn.* Available at: https://www.iaea.org/publications/6375/the-radiological-accident-in-samut-prakarn (Accessed on 05 January 2023).

International Atomic Energy Agency (IAEA) Publication 1227. 2005. *IAEA Safety standards for protecting people and the environment: Categorisation of radioactive sources*. [Online]. Available at: STI/PUB/1227 (iaea.org). (Accessed on 05 January 2023).

International Atomic Energy Agency (IAEA) Publication 1248. 2009. *NSS No. 3: Monitoring for radioactive material in international mail transported by public*

postal operators. Available at: https://www.iaea.org/publications/7402/monitoring-for-radioactive-material-in-international-mail-transported-by-public-postal-operators (Accessed on 14 November 2020).

International Atomic Energy Agency (IAEA) Publication 1278. 2007. *NSS No. 3: Identification of radioactive sources and devices*. Available at: https://www.iaea.org/publications/7567/identification-of-radioactive-sources-and-devices (Accessed on 14 November 2020).

International Atomic Energy Agency (IAEA) Publication 1309. 2007. *NSS No. 6: Combating illicit trafficking in nuclear and other radioactive material*. https://www.iaea.org/publications/7806/combating-illicit-trafficking-in-nuclear-and-other-radioactive-materiaL (Accessed on 14 November 2020).

International Atomic Energy Agency (IAEA) Publication 1347. 2008. *Nuclear security culture*. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf (Accessed on 14 November 2020).

International Atomic Energy Agency (IAEA) Publication 1387. 2009. *NSS No. 11: Security of radioactive sources*. Available at: https://www.iaea.org/publications/8113/security-of-radioactive-sources (Accessed on 14 November 2020).

International Atomic Energy Agency (IAEA) Publication 1481. 2011. *Nuclear security recommendations on physical protection of nuclear material and nuclear facilities* (infcirc/225/revision 5). [Online]. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf (Accessed on 14 November 2020).

International Atomic Energy Agency (IAEA) Publication 1858. 2008. *NSS No. 8: Preventive and protective measures against insider threats*. [Online]. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1858_web.pdf (Accessed on 14 November 2020).

International Atomic Energy Agency (IAEA) Publication 3684. 1988. *The radiological accident in Goiania.* [Online]. Available at: The Radiological Accident in Goiânia | IAEA. (Accessed on 05 January 2023).

International Atomic Energy Agency (IAEA) Publication 7402. 2006. *Nuclear Security Series No. 3: Monitoring for radioactive material in international mail transported by public postal operators*. [Online]. Available at: https://www.iaea.org/publications/7402/monitoring-for-radioactive-material-in-international-mail-transported-by-public-postal-operators. (Accessed on 15 November 2020).

International Atomic Energy Agency (IAEA) Publication 7567. 2007. *NSS No. 5: Identification of radioactive sources and devices.* [Online]. Available at: https://www.iaea.org/publications/7567/identification-of-radioactive-sources-and-devices (Accessed on 17 November 2020).

International Atomic Energy Agency (IAEA) Publication 7977. 2008. *NSS No. 7: Nuclear security culture.* [Online]. Available at: https://www.iaea.org/publications/7977/nuclear-security-culture (Accessed on 16 November 2020).

International Atomic Energy Agency (IAEA) Publication 7987. 2008. *NSS No. 9. Security in the transportation of radioactive material.* [Online]. Available at: https://www.iaea.org/publications/7987/security-in-the-transport-of-radioactive-material (Accessed on 21 December 2020).

International Atomic Energy Agency (IAEA) Publication 8113. 2009. *NSS No. 11: Security of radioactive sources.* [Online]. Available at: https://www.iaea.org/publications/8113/security-of-radioactive-sources (Accessed on 19 December 2020).

International Atomic Energy Agency (IAEA) Publication 8616. 2011. *NSS No. 14: Nuclear security recommendations on radioactive material and associated facilities.* [Online]. Available at: https://www.iaea.org/publications/8616/nuclear-security-recommendations-on-radioactive-material-and-associated-facilities (Accessed on 15 November 2020).

International Atomic Energy Agency (IAEA) Publication 8622. 2011. *NSS No. 15: Nuclear security recommendations on nuclear and other radioactive material out of regulatory control.* [Online]. Available at: https://www.iaea.org/publications/8622/nuclear-security-recommendations-on-nuclear-and-other-radioactive-material-out-of-regulatory-control (Accessed on 12 October 2020).

International Atomic Energy Agency (IAEA) Publication 8629. 2011. *NSS No. 13: Nuclear security recommendations on physical protection of nuclear material and nuclear facilities* (INFCIRC/225/Revision 5). [Online]. Available at: https://www.iaea.org/publications/8629/nuclear-security-recommendations-on-physical-protection-of-nuclear-material-and-nuclear-facilities-infcirc/225/revision-5 (Accessed on 15 November 2020).

International Atomic Energy Agency (IAEA) Publication 10353. 2013. *NSS No. 20: Objective and essential elements of a State's nuclear security regime*. [Online]. Available at: https://www.iaea.org/publications/10353/objective-and-essential-elements-of-a-states-nuclear-security-regime (Accessed on 16 November 2020).

International Atomic Energy Agency (IAEA) Publication 10483. 2013. *NSS No. 21: Nuclear security systems and measures for the detection of nuclear and other radioactive material out of regulatory control.* [Online]. Available at: https://www.iaea.org/publications/10483/nuclear-security-systems-and-measures-for-the-detection-of-nuclear-and-other-radioactive-material-out-of-regulatory-control (Accessed on 17 December 2020).

International Atomic Energy Agency (IAEA) Publication 10602. 2014. *The radiological accident in Lia, Georgia*. Available at: https://www.iaea.org/publications/10602/the-radiological-accident-in-lia-georgia (Accessed on 05 January 2023).

International Atomic Energy Agency (IAEA) Publication 12288. 2018. *Regulations for the Safe Transport of Radioactive Material.* Available at: https://www.iaea.org/publications/12288/regulations-for-the-safe-transport-of-

radioactive-material (Accessed on 17 December 2020).

International Atomic Energy Agency (IAEA) Publication 12354. 2020. *Preventive and protective measures against insider threats*. 2020. Available at: https://www.iaea.org/publications/12354/preventive-and-protective-measures-against-insider-threats (Accessed on 17 December 2020).

International Atomic Energy Agency (IAEA). 2019. *Incident and Trafficking Database (ITDB) Factsheet.* Available at: https://www.iaea.org/sites/default/files/19/04/itdb-factsheet-2019.pdf (Accessed on 17 December 2020).

International Atomic Energy Agency (IAEA) IPPAS Mission. 2018. Available at: https://www.iaea.org/services/review-missions/international-physical-protection-advisory-service-ippas (Accessed on 05 January 2023).

International Atomic Energy Agency (IAEA) TECHDOC-1388. 2004. *Strengthening control over radioactive sources in authorised use and regaining control over orphan sources: National strategies*. Available at: https://www.iaea.org/publications/7006/strengthening-control-over-radioactive-sources-in-authorized-use-and-regaining-control-over-orphan-sources-national-strategies (Accessed on 11 August 2021).

International Atomic Energy Agency (IAEA) TECHDOC-1728. 2013. Regulatory Control for the Safe Transport of Naturally Occurring Radioactive Material (NORM): Report of a Coordinated Research Project 2007–2010. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/TE-1728_web.pdf (Accessed on 11 August 2021).

International Source Suppliers and Producers Association (ISSPA). 2022. Available at: https://isspa.com/about-isspa/#:~:text=The%20International%20Source%20Suppliers%20and%20Producers%20Association%20%28ISSPA%29,processing%20or%20treatment%20system%2C%20device%2C%20gauge%20or%20camera (Accessed on 05 January 2023).

Jagger, J. 1991. *The nuclear lion*. New York: Plenum Press.

Jain, S. 2019. *Research methodology in arts, science and humanities*. Oakville, Canada: Society Publishing.

Jensen, K.B. 2021. *A handbook of media and communication research: Qualitative and quantitative methodologies* (3rd ed.). London: Routledge.

Kivunja, C. & Kuyini, A.B. **2**017. Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education*, 6(5). https://doi.org/10.5430/ijhe.v6n5p26. (Accessed on 05 January 2023).

Kopp, C.M. 2021, August. *Vetting.* Investopedia. [Online]. Available at: Vetting Definition (investopedia.com) (Accessed on 07 July 2022).

Korshukim, M. & Emery, R.J. 2006. *Reported events of stolen radioactive sources in Texas from 1956 to 2000: Abstract.* [Online]. Available at: https://journals.lww.com/health-physics/Abstract/2006/03000/REPORTED_EVENTS_OF_STOLEN_RADIOACTIVE_SOURCES_IN.10.aspx (Accessed on 05 January 2022).

Kumar, R. 2019. *Research methodology: A step-by-step guide for beginners* (5th ed.). Thousand Oaks, CA: Sage.

Law Insider. 2021. *Hospital personnel definition*. [Online]. Available at: https://www.lawinsider.com/dictionary/hospital-personnel (Accessed on 23 January 2022).

Leavy, P. 2014. *The Oxford Handbook of qualitative research*. Oxford: Oxford University Press.

Leavy, P. 2017. *Research design: Quantitative, qualitative, mixed methods, arts-based, and community based participatory research approaches*. New York: The Guilford Press.

Leedy, P.D. & Ormrod, J.E. 2021. *Practical research: Planning and design* (12th ed.). New York: Pearson.

Leigh, J. & Brown, N. 2021. *Embodied inquiry: Research methods*. Dublin, Ireland: Bloomsbury Academic.

Lincoln, Y.S. & Guba, E.G. **2**013. *The constructivist credo*. Walnut Creek, CA: Left Coast Press.

Machi, L.A. & McEvoy, B.T. 2016. *The literature review: Six steps to success*. Thousand Oaks, CA: Sage.

Machi, L.A. & McEvoy, B.T. 2022. *The literature review: 6 steps to success* (4th ed.). Thousand Oaks, CA: Corwin.

Mansfield, D. 2001. Tennessee narrowly dodged bullet in tense ’72 hijack episode. *Los Angeles Times*. [Online]. Available at: https://www.latimes.com/archives/la-xpm-2001-sep-23-mn-48746-story.html (Accessed on 02 August 2021).

Marcus, B. & Hightower, W. **2**019. *How to write qualitative research*. London: Routledge.

Mcllwraith, A. 2022. *Information security and employee behaviour* (2nd ed.). London: Taylor & Francis.

Merriam, S.B. & Tisdell, E.J. **2**016. *Qualitative Research: A guide to design and implementation* (4th ed.). San Francisco, CA: Jossey-Bass.

Mohamed, Y.T. **2**009. Quality assurance management system for spent radioactive sealed sources in Egypt. *The Quality Assurance Journal*, 12(2):86–94. [Online]. Available at: https://doi.org/10.1002/QAJ.445. (Accessed on 11 December 2022).

Mukherjee, S.P. 2020. *A guide to research methodology: An overview of research problems, tasks and methods*. New York: CRC Press.

Murray, R.L. 2001. *Nuclear energy: An introduction to the concepts, systems, and applications of nuclear processes* (5th ed.). Oxford: Butterworth-Heinemann.

National Radioactive Waste Disposal Institute (NRWDI) Vaalputs. 2021. *NRWDI Vaalputs*. Available at: https://www.nrwdi.org.za (Accessed on 26 December

2021).

NTP Radioisotopes SOC Ltd. 2022. Available at: https://www.ntp.co.za (Accessed on 06 July 2022).

Nuclear Energy Corporation of South Africa (NECSA). n.d. *About Necsa*. Available at: http://www.necsa.co.za/ (Accessed on 17 October 2020).

Nuclear Energy Corporation of South Africa (NECSA). 2022. *Our Group*. Available at: https://www.necsa.co.za (Accessed on 17 October 2020).

Nuclear Industry Association of South Africa (NIASA). 2022. Available at: https://niasa.co.za (Accessed on 17 October 2020).

Nuclear Threat Initiative (NTI). 2010. *The April 2010 Nuclear Security Summit: One more step toward the mountain top*. [online]. Available at: The April 2010 Nuclear Security Summit: One More Step Toward the Mountaintop - The Nuclear Threat Initiative (nti.org) (Accessed on 30 November 2021).

Onishi, Y., Voitsekhovich, O.V. & Zheleznyak, M.J. 2007. *Chernobyl – What have we learned?* The Netherlands: Springer.

Patten, M.L. & Newhart, M. 2018. *Understanding research methods: An overview of essentials* (10th ed.). New York: Taylor & Francis.

Patton, M.Q. 2015. *Qualitative research & evaluation methods* (4th ed.). Thousand Oaks, CA: Sage.

Petryna, A. 2017. *Life exposed: Biological citizens after Chernobyl*. New Jersey. Princeton: Princeton University Press. Available at: https://wins.org/document/bpg-5-8-security-of-radioactive-sources-used-in-industrial-radiation-processing/ (Accessed on 11 November 2020).

Private Security Industry Regulating Authority (PSIRA). 2021. *About us: Strategic overview*. [Online]. Available at: https://www.psira.co.za/search-joomla/organizational-overview.html (Accessed on 13 December 2021).

Private Security Industry Regulating Authority (PSIRA). 2022. Available at:

https://www.psira.co.za (Accessed on 19 December 2022).

Public Integrity. 2015. Available at: https://archive.publicintegrity.org/national-security/south-african-who-attacked-a-nuclear-plant-is-a-hero-to-his-government-and-fellow-citizens/ (Accessed on 05 January 2023).

Republic of South Africa (RSA). 1973. Hazardous Substance Act No. 15 of 1973. *Government Gazette.* Vol. 94. No. 3834. [Online]. Available at: https://www.gov.za/sites/default/files/gcis_document/201504/act-15-1973.pdf (Accessed on 3 June 2020).

Republic of South Africa (RSA). 1982. Protection of Information Act 84 of 1982. Available at: https://www.gov.za/documents/protection-information-act-20-mar-2015-1202 (Accessed on 05 January 2023).

Republic of South Africa (RSA). 1996. *The Constitution of the Republic of South Africa*. Pretoria: Government Printers.

Republic of South Africa (RSA). 1999. National Nuclear Regulator Act 47 of 1999. Available at: www.gov.za/documents/national-nuclear-regulator-act (Accessed on 05 January 2022).

Republic of South Africa (RSA). 2000. Promotion of Access to Information Act 2 of 2000. Available at: https://www.gov.za/documents/promotion-access-information-act

Republic of South Africa (RSA). 2008. National Radioactive Waste Disposal Institute Act 53, 2008. Available at: https://www.gov.za/documents/national-radioactive-waste-disposal-institute-act (Accessed on 05 January 2022).

Republic of South Africa (RSA). 2013. Protection of Personal Information Act 4 of 2013. Available at: https://www.gov.za/documents/protection-personal-information-act (Accessed on 05 January 2023).

Republic of South Africa (RSA). 2022a. Department of energy, mineral resources and energy. Available at: https://www.energy.gov.za (Accessed on 05 January 2023).

Republic of South Africa (RSA). 2022b. Department of Health. Available at: https://www.health.gov.za (Accessed on 05 January 2023).

Republic of South Africa (RSA). 2022c. State Security Agency. Available at: https://www.gov.za/state-security-agency-0 (Accessed on 05 January 2023).

Robinson, D.M. & Wood, W.D. 2009. *International approaches to securing radioactive sources against terrorism*. Washington, DC: Institute for Applied Science.

Rossman, G.B.N. & Rallis, S.F. 2017. *An introduction to qualitative research: Learning in the field* (4th ed.). Thousand Oaks, CA: Sage.

Rosoff, H. & Von Winterfeldt, D. 2007. A risk and economic analysis of dirty bomb attacks on the Ports of Los Angeles and Long Beach Risk Analysis. In A.E. Abbas, M. Tambe & D. von Winterfeldt (Eds.), *Improving homeland security decisions* (pp.111–133). Cambridge: Cambridge University Press.

Safety and Security Sector Education and Training Authority (SASSETA). 2021. *National Government: Overview.* [Online]. Available at: https://nationalgovernment.co.za/units/view/156/safety-and-security-sector-education-and-training-authority-sasseta (Accessed on 05 January 2023).

Safety and Security Sector Education and Training Authority (SASSETA). 2022. Available at: https://www.sasseta.org.za (Accessed on 05 January 2023).

Scaglione, B.J. 2019. *Security management for healthcare: Proactive event prevention and effective resolution*. London: Routledge.

Shimura, T., Yamaguchi, I., Terada, H., Svendsen, E.R. & Kunugita, N. **2**015. Public health activities for mitigation of radiation exposures and risk communication challenges after the Fukushima nuclear accident. *Journal of Radiation Research*, 56(3):422–429. [Online]. Available at: https://doi.org/10.1093/JRR/RRV013. (Accessed on 19 December 2022).

Shkedi, A. 2019. *Data analysis in qualitative research: Practical and theoretic methodologies with optional use of software tool*. Published by A. Shkedi.

Silverman, D. 2014. *Interpreting qualitative data* (5th ed.). Thousand Oaks, CA: Sage.

Simon, M.K. & Goes, J. 2018. *Dissertation and scholarly research: Recipes for success*. CreateSpace Independent Publishing Platform.

South African Cabinet. 1996. Available at: https://www.sita.co.za/sites/default/files/documents/MISS/minimum%20Information%20Security%20Standards%20(MISS).pdf (Accessed on 05 January 2023).

South African Health Products Regulatory Authority (SAHPRA). 2010. *IRCP91-2-Industrial radiography-gamma*. Available at: https://www.sahpra.org.za (Accessed on 05 January 2023).

South African Health Products Regulatory Authority (SAHPRA). 2021. *Radiation control guidelines and codes of practice: Code of practice for industrial radiography: Security measures at storage facilities*. [Online]. Available at: https://www.sahpra.org.za/wp-content/uploads/2020/01/IRCP91-2-Industrial-radiography-gamma-radiography-May19-rev-0b-2.pdf (Accessed on 23 June 2022).

Tabak, J. 2009. *Nuclear energy*. New York: Facts on File, Inc.

Tavakoli, H. 2012. *A dictionary of research methodology and statistics in applied linguistics*. Iran: Rahnam Press.

The Guardian. 2016. Radioactive material stolen in Iraq raises security fears. [Online]. Available at: https://www.theguardian.com/world/2016/feb/17/radioactive-material-stolen-in-iraq-raises-security-fears (Accessed on 05 January 2022).

The White House, Office of the Press Secretary. 2016. *Nuclear Security Summit 2016 Communique*. [Online]. Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/04/01/nuclear-security-summit-2016-communiqu%C3%A9 (Accessed on 05 January 2022).

Thomas, C.G. 2021. *Research methodology and scientific writing* (2nd ed.). Kerala. India. Springer.

Thomas, G. 2017. *How to do your research project: A guide for students* (3rd ed.).

Thousand Oaks, CA: Sage.

Tracy, S.J. 2020. *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Vanderstoep, S.W. & Johnston, D.D. 2009. *Research methods for everyday life: Blending qualitative and quantitative approaches*. San Francisco, CA. Jossey-Bass.

Volders, B. & Sauer, T. 2016. *Nuclear terrorism: Countering the threat*. London: Routledge.

Walliman, N. 2022. *Research methods: the basics* (3rd ed.). London: Routledge.

World Institute for Nuclear Security (WINS) Academy. 2016a. *Nuclear security incident management. Version 1.* Available at: https://www.wins.org/wins-academy/ (Accessed on 05 January 2023).

World Institute for Nuclear Security (WINS) Academy. 2016b. *Radioactive sources security management. Revision 1*. https://www.wins.org/wins-academy/ (Accessed on 05 January 2023).

World Institute for Nuclear Security (WINS) Academy. 2016c. *Security regulation. Revision 1.* Available at: https://www.wins.org/wins-academy/ (Accessed on 11 October 2021).

World Institute for Nuclear Security (WINS). 2016. *Canada publishes IPPAS mission report.* [Online]. Available at: https://www.wins.org/canada-publishes-ippas-mission-report/ (Accessed on 11 October 2021).

World Institute for Nuclear Security (WINS). 2018. *Peer review guidelines to assess the security of radioactive sources used in medical applications*. [Online]. Available at: https://www.wins.org/document/peer-review-guidelines-to-assess-the-security-of-radioactive-sources-used-in-medical-applications/ (Accessed on 05 January 2022).

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 2.3. 2011. *Information security for operators: Challenges and opportunities. Revision 1.*

Vienna, Austria: WINS.

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 2.4. 2011. *Communicating Security Information: Striking the balance.* [Online]. Available at: https://www.wins.org/document/2-4-communicating-security-information-striking-a-balance/ (Accessed on 23 January 2022).

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 2.5. 2019. *Engaging with external stakeholders on nuclear security. Version 1.1*. Available at: https://www.wins.org/document/2-5-engaging-with-external-stakeholders-on-nuclear-security/ (Accessed on 05 January 2023).

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 2.6. 2019. *Assessing and communicating nuclear security threats*. Available at: https://www.wins.org/document/2-6-assessing-and-communicating-nuclear-security-threats/ (Accessed on 05 January 2023).

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 4.1. 2019. *Implementing security by design at nuclear facilities.* Available at: https://www.wins.org/document/4-1-implementing-security-by-design-at-nuclear-facilities/ (Accessed on 05 January 2023).

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 4.10. 2020. *Nuclear transport security.* [Online]. Available at: https://www.wins.org/document/4-10-nuclear-transport-security/ (Accessed on 05 January 2022).

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 5.1. 2021. *Security of high activity radioactive sources*. [Online]. Available at: https://wins.org/document/5-1-security-of-high-activity-radioactive-sources/. (Accessed on 15 February 2020).

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 5.4. 2019. *Security of radioactive sources used in medical applications.* [Online]. Available at: https://wins.org/document/5-4-security-of-radioactive-source-used-in-medical-applications/. (Accessed on 16 September 2020).

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 5.5. 2020. *Security management of disused radioactive sources.* [Online]. Available at: https://wins.org/document/5-5-security-management-of-disused-radioactive-sources-2/. (Accessed on 12 September 2020).

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 5.7. 2021. *Security of radioactive sources used in industrial radiography and well-logging applications.* [Online]. Available at: https://www.wins.org/document/5-7-security-of-radioactive-sources-used-in-industrial-radiography-and-well-logging-applications/ (Accessed on 05 January 2022).

World Institute for Nuclear Security Best Practice Guide (WINS BPG) 5.8. 2020. *Security of radioactive sources used in industrial radiation processing*. [Online]. Available at: https://www.wins.org/document/bpg-5-8-security-of-radioactive-sources-used-in-industrial-radiation-processing/ (Accessed on 04 March 2022).

World Nuclear Association. 2012. Available at: https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/three-mile-island-accident.aspx (Accessed on 05 January 2023).

World Nuclear Association. **2**018. Available at: https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-daiichi-accident.aspx (Accessed on 05 January 2023).

World Nuclear Association. 2019. Available at: https://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx (Accessed on 05 January 2023).

World Nuclear Association. 2021. *Nuclear fuel cycle overview*. [Online]. Available at: https://world-nuclear.org/information-library/nuclear-fuel-cycle/introduction/nuclear-fuel-cycle-overview.aspx (Accessed on 04 March 2022).

Yin, R.K. 2016. *Qualitative research: From start to finish* (2nd ed.). New York: The Guilford Press.

Yin, R.K. 2017. *Case study research and applications: Design and methods* (6th ed.).

Thousand Oaks, CA: Sage.

Yin, R.K. 2018. *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, CA: Sage.

York, T.W., MacAlister, D. 2015. *Hospital healthcare security (6th ed.).* Butterworth-Heinemann, USA: Elsevier.

Zimmerman, A.S. 2022. *Methodological innovations in research and academic writing*. Hershey, PA: IGI Global.

ANNEXURE A: INFORMED CONSENT FORM

PARTICIPANT INFORMATION SHEET

PARTICIPANT INFORMATION SHEET

Ethics clearance reference number: ST131
Research permission reference number:

2022-03-31

TOPIC: PARTICIPANT IFORMATION SHEET AND INFORMED CONSENT

Dear Prospective Participant

My name is Mafihla Johannes Maleka, student no 36878030 and I am doing research under the supervision of Ms NP Cebekhulu, Senior Lecturer, Department of Criminology and Security Science, College of Law at the University of South Africa. I am inviting you to participate in a study entitled:
"An examination of the need for public awareness and nuclear security information dissemination: a case study from SA"

WHAT IS THE PURPOSE OF THE STUDY?

The purpose of this research study is to examine whether is there a need for the healthcare facilities (hospitals and institutions of higher learning) security personnel, to be aware of radioactive sources security.

WHY I AM BEING INVITED TO PARTICIPATE

You are being invited to participate in this study because you form part of the healthcare facilities where radioactive sources are used for academic research purposes and you are expected to be aware of how to secure them while at your facility.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves semi-structured interviews using an interview schedule. The semi-structured interview schedule consists of open ended-questions that require you to give flexible answers according to your own knowledge and experience as it relates to the radioactive sources security.

The researcher will conduct one-on-one interviews with participants: these may also be conducted in an online format, should a need arise. The interview will be audio recorded so that the researcher can transcribe the data more accurately. You will be provided with a transcript of this so that you can ensure that what has been captured is a true reflection of what you shared with the researcher during the interview. The expected duration of each interview is approximately 30 minutes.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Participation in this study is voluntary and there is no penalty or loss of benefit for non-participation. You are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time of the interview process and without giving a reason; however, it will not be possible to withdraw after the interview process has been completed. Please note that the interview questions will not require you to personally identify yourself.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

The potential benefits for the participants as a group, the scientific community and/or society is that the new knowledge has a potential to contribute to developing good practices in addressing the security of radioactive sources. Furthermore, this study will add value to the discipline of nuclear security and radiology since it will supply insight into the topic being studied. The radiology Radiation and Health Physics Unit at the

University of the Witwatersrand will benefit from insight gained into the sharing of best practices in the security of radioactive sources.

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

There is no foreseeable risk of harm from taking part in this study. In the unlikely event that the participant feels inconvenienced, the researcher will stop the interview and if it suits the participant, reschedule to a more convenient date/time. If there is any discomfort, the interview will also be stopped and the participant will be given time to refresh themselves and perhaps take a walk outside, if it is safe to do so. Only once this has been concluded, and IF the participant feels that they would like to still take part in the research, will the researcher reschedule another interview. The participants will be reminded that they are free to withdraw their participation at any stage if they feel not comfortable to continue.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

The researcher has familiarised himself with the relevant Unisa policies that underpin ethical research. As such he undertakes to ensure that the privacy and confidentiality of information is protected and maintained. Your name will not be recorded anywhere in the research report or the data gathering instruments, and no one, apart from the researcher will know about your involvement in this research and no one will be able to connect you to the answers you give. As a participant, you will be given a code number and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings. Your answers may be reviewed by people responsible for making sure that research is done properly, including the supervisor and members of the Research Ethics Review Committee. Otherwise, records that identify you will be available only to the researcher, unless you give permission for other people to see the records.

Also note that as a participant, your anonymous data may be used for other purposes, such as a research report, journal articles and/or conference proceedings. Your privacy as a participant will be protected in any publication of the information. Example: A report of the

study may be submitted for publication, but individual participants will not be identifiable in such a report. Please keep in mind that it is sometimes impossible to make an absolute guarantee of confidentiality or anonymity, e.g. when focus groups are used as a data collection method. This study will not use focus group as a data collection method.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a period of five years in a locked cupboard/filing cabinet at his private residence. For future research or academic purposes; electronic information will be stored on a password protected computer. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. Information on hard copies will be destroyed by shredding the papers and electronic copies will be permanently deleted from the hard drive of the computer through the use of a relevant software programme.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

Participants will not be offered inducements or incentives to encourage their involvement in the research and will not incur financial obligations as a result of their participation in the research. The researcher will not anticipate financial gains from involvement in the research.

HAS THE STUDY RECEIVED ETHICS APPROVAL?

This study has received written approval from the Research Ethics Review Committee of the College of Law, Unisa. The Ethics approval number is ST131.
A copy of the approval letter can be obtained from the researcher upon request.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

If you would like to be informed of the final research findings, please contact Mr Mafihla Johannes Maleka, email: 36878030@mylife.unisa.ac.za.

Should you have concerns about the way in which the research has been conducted, you may contact Mrs. NP Cebekhulu at Cebeknp@unisa.ac.za.

Thank you for taking time to read this information sheet and for participating in this study.

_____ Mafihla Johannes Maleka

CONSENT TO PARTICIPATE IN THIS STUDY Participant number #.....

I, _____ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation. I have been allocated the participant number #.....

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the audio recording of the interview.

I have received a signed copy of the informed consent agreement.

Participant Signature……..Date……

Researcher's Name & Surname ……(please print)

Researcher's signature…….Date……

ANNEXURE B: ETHICAL CLEARANCE CERTIFICATE

UNISA college of law

COLLEGE OF LAW RESEARCH ETHICS REVIEW COMMITTEE

Date: 2016/11/25

Reference: ST131

Applicant: Mr. M. J. Maleka

Dear Mr. M. J. Maleka
(Supervisor: Prof A. Minnaar)
(Co-supervisor: Prof K. Pillay)

DECISION: ETHICS APPROVAL

Name	Mr. M. J. Maleka
Proposal	An examination of the need for public awareness and nuclear security information dissemination: a case study from SA
Qualification	MTech

Thank you for the application for research ethics clearance by the College of Law Research Ethics Review Committee for the above mentioned research. **Final approval is granted.**

The application was reviewed in compliance with the Unisa Policy on Research Ethics.

The proposed research may now commence with the proviso that:

1. *The researcher will ensure that the research project adheres to the values and principles expressed in the Unisa Policy on Research Ethics 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

2. *Any adverse circumstances 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 in writing to the College of Law Ethical Review Committee.*

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392, Unisa, 0003, South Africa

An amended application could be requested if there are substantial changes from the existing proposal, especially if those changes affect any of the study-related risks for the research participants

3. *The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study.*

Note:

The reference number (top right corner of this communique) should be clearly indicated on all forms of communication (e.g. Webmail, E-mail messages, letters) with the intended research participants, as well as with the URERC.

Kind regards

PROF B W HAEFELE
CHAIR PERSON: RESEARCH ETHICS
REVIEW COMMITTEE
COLLEGE OF LAW

PROF R SONGCA
EXECUTIVE DEAN:
COLLEGE OF LAW

ANNEXURE C: INTERVIEW SCHEDULE

UNISA

INTERVIEW SCHEDULE

AN EXPLORATION OF RADIOACTIVE SOURCES SECURITY AWARENESS: A CASE STUDY OF FIVE HEALTH CARE FACILITIES IN GAUTENG, SOUTH AFRICA

Interview Number: .....

Date: ..... Time: ..... Place.....

Section A: Biographical data

Age (not younger than 30 years): .....

Race: .....

Position (At least Supervisory level): .....

Length of service (in the security industry): .....

School qualification (minimum Grade 10 or Std 8): .....

Security/equivalent training (minimum training – PSIRA Grade B) .....

Section B: interview questions

1. Do you know what is radioactive sources security?
2. Does this institution have a disaster management plan / security policy / plan (yes/~~no~~)
3. If yes, does it contain any specific mention of the disaster management in relation to radioactive sources?
4. Have you ever attended a radioactive source security awareness training?
5. Do you think an 'insider' is a potential threat to this institution in terms of the radioactive sources or sensitive information?
6. Have you heard of criminal activities/threats of theft of radioactive sources or its equipment that took place in South Africa or anywhere else in the world?
7. Are you aware of the application of the following security concepts; graded approach, defence/protection-in-depth, security-by-design, detection, delay and response?
8. Do you know whether the security department of this institution previously engaged with State Security Agencies to conduct threat assessment related to radioactive sources?
9. Have you heard of the following ~~organisations~~:
   - Nuclear Industry Association of South Africa (NIASA)
   - National Nuclear Regulator (NNR)
   - Public Safety Information Forum (PSIF)
   - The World Institute for Nuclear Security (WINS)
10. Are you aware of the free online nuclear security discipline courses provided by the IAEA?

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: TURNITIN REPORT

turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Mj Maleka
Assignment title:	MA (Criminal Justice)
Submission title:	Final Dissertation
File name:	Maleka_Draft_dissertation_09012023.docx
File size:	574.12K
Page count:	135
Word count:	37,267
Character count:	217,047
Submission date:	09-Jan-2023 02:41PM (UTC+0200)
Submission ID:	1990187201

feedback studio | Mj Maleka | Final Dissertation | -- /null | 2 of 3

AN EXPLORATION OF RADIOACTIVE SOURCES SECURITY AWARENESS: A CASE STUDY OF FIVE HEALTHCARE FACILITIES IN GAUTENG, SOUTH AFRICA

By

Mafihla Johannes Maleka

Submitted in accordance with the requirements of

MASTERS OF ARTS

In

Match Overview

12%

1	Submitted to University... Student Paper	2%
2	Submitted to Mancosa Student Paper	<1%
3	"Nuclear Law", Springer... Publication	<1%
4	Ibrahim Alrammah, Ab... Publication	<1%
5	Submitted to University... Student Paper	<1%
6	Submitted to University... Student Paper	<1%
7	Submitted to University...	<1%

ANNEXURE E: CERTIFICATE OF EDITING

Barbara Shaw
Editing/proofreading services
18 Balvicar Road, Blairgowrie, 2194
Tel: 011 888 4788 Cell: 072 1233 881
Email: barbarashaw16@gmail.com
Full member of The Professional Editors' Guild

To whom it may concern

This letter serves to inform you that I have done language editing, reference checking and formatting on the thesis

AN EXPLORATION OF RADIOACTIVE SOURCES SECURITY AWARENESS: A CASE STUDY OF FIVE HEALTHCARE FACILITIES IN GAUTENG, SOUTH AFRICA

By

Mafihla Johannes Maleka

Barbara Shaw

05/02/2023