ORGANISATIONAL RESILIENCE: A PARADIGM SHIFT FOR MANAGING SECURITY RISKS USING A MATURITY MODEL

by

JOHAN DIEDERICK DU PLOOY

submitted in accordance with the requirements

for the degree of

MAGISTER TECHNOLOGIAE

In the subject

SECURITY MANAGEMENT

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF A deV MINNAAR

CO-SUPERVISOR: DR C J MORRISON

June 2012

COPYRIGHT DECLARATION

DECLARATION FORM

Student Number: 03304949

I, **JOHAN DIEDERICK DU PLOOY,**

Declare that this dissertation:

ORGANISATIONAL RESILIENCE: A PARADIGM SHIFT FOR MANAGING SECURITY RISKS USING A MATURITY MODEL

Is my own work and that all the sources that I have quoted have been indicated and acknowledged by means of complete references.

JOHAN DU PLOOY

SIGNATURE: DATE: 15-06-2012

(J.D. DU PLOOY)

TABLE OF CONTENTS

FIGURES AND TABLES

FIGURES

TABLES

ACKNOWLEDGEMENTS

Firstly I would like to thank God for the ability, energy and wisdom He gave me to do this work.

I would like to thank my supervisor and co-supervisor, Professor Anthony Minnaar for his guidance and Professor Cherita Morrison for her patience and guidance in the development of this research document. I will miss the many debates we had to reach agreement on the differences between Security Risk Management and Criminology. Also to Professor Kris Pillay who has always been a keen supporter of my personal development.

Thanks also go to my many friends and colleagues who over the years have given me guidance and support to improve the profession that I have now been involved in for more than forty years. I need to however highlight some of these: Rynier Keet, Peter Grant, Dirk Ackerman (Snr), Basie Smit, Francois Marais, George Skinner and Charles Rogers among a number of others. As my interest into the new field of Standards grew, I have been very fortunate to have been able to work with and be guided by the following people: Dr Marc Siegel who gave me an opportunity to grasp this new field of expertise for the security professional, Dr Gert Cruywagen who had the insight to allow the first implementation of the Organisational Resilience Management System (ORMS) Maturity Model, Colin Ackroyd who was a slave driver but helped to ensure the best project deliverable that I have worked on in recent years, my business partner at Temi Group, Roger Warwick for sharing his knowledge and giving guidance, and Giel Burger who did so much to ensure we were able to achieve our goals during the implementation at Tsogo Sun Group. The Tsogo Sun Group for allowing me to use their case study for this research document. Also to Dr Alice Mare who at very short notice helped refocus my mind when revising the first two chapters. Raymond van Staden, my friend and colleague who drowned while doing an unselfish deed, saving the life of a young boy. Also to the many people who I have not mentioned here but to whom I will be ever grateful to for their assistance and support.

My family have always been very supportive in whatever I have undertaken, but in this instance my wife Eleanor has to be singled out for her patience while I spent many hours doing research and typing up this research document. Also to my son Craig and his wife Tracey, my daughter Michelle, my grandchildren, Joshua, Kayla, Lilly and Taya for their ongoing support and the love I receive from each one of them.

This work is dedicated to all of you.

LIST OF ABBREVIATIONS

ANSI	American National Standards Institute
ASIS	ASIS International (formerly American Society for Industrial Security)
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CCM	Capability Maturity Model
CCMI	Capability Maturity Model Integration
CMU	Carnegie Melon University
EMS	Environmental Management System
FDIS	Final Draft International Standard
FIFA	Fédération Internationale de Football Association
ILO	International Labour Organisation
IS	Intervention Schedule
ISO	International Organisation for Standardisation
KPA	Key Performance Area
OFI	Opportunity For Improvement
OR	Organisational Resilience
ORMS	Organisational Resilience Management System
PAS	Publicly Available Specification
PDCA	Plan-Do-Check-Act Model
QMS	Quality Management System
PWC	PricewaterhouseCoopers
RA	Risk Assessment
RABQSA	Registrar Accreditation Board Quality Society of Australasia
RIMS	The Risk Management Society (Australia)
REAG	Resilience Expert Advisory Group (Australia)
SABS	South African Bureau of Standards
SOP	Standard Operating Procedures
SPC	Security, Preparedness and Continuity
TC	Technical Group
TSG	Tsogo Sun Group
WG	Working Group
WHO	World Health Organisation

ABBREVIATED SUMMARY

This study, within the sphere of security risk management, aimed to ascertain whether the concept: '*Organisational Resilience*' would create a paradigm shift for managing security risks when using a Maturity Model. It is foundationally based on the American National Standards Institute-ASIS International's Security, Preparedness and Continuity (SPC) standard *(ANSI/ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with guidance for use)* and a Maturity Model for an Organisational Resilience Management System. The latter was implemented in a case study which allowed for on-site tailoring and cost-effective maintenance within certain resource constraints. It was found that, by using this Maturity Model, all levels of management were able to experience a constant understanding of what level of resilience existed within the organisation. Implementation also minimised the probability of potential disruptive events and other risk threats from occurring, as well as, in all likelihood, mitigating the consequences should these actually occur.

KEY TERMS

ANSI/ASIS SPC.1-2009: Maturity Model; Security Risk Management: Organisational Resilience, ISO 27000: 2007; ISO 28000: 2007; ISO 31000: 2009; ISO 19011: 2002; Security related standards; Management Systems.

EXECUTIVE SUMMARY

The word '*resilience*' is used in a multitude of contexts as we refer to corporate, business, enterprise, emotional, individual, organisational, medical, sectoral or social environments. Each of these environments or contexts has a very different application for the word '*resilience'* as it reflects common core elements such as the ability to absorb change gracefully while remaining stable in a turbulent environment. For organisations, it measures their ability to and agility with which they can avoid being affected by potentially disruptive events, as well as returning to predetermined performance levels following a high impact/low probability disruption.

The aim of this research study was, within the sphere of security risk management, to ascertain if the concept of Organisational Resilience would create a paradigm shift for managing security risks when using a Maturity Model. The study was based on the American National Standards Institute and ASIS International's Security, Preparedness and Continuity (SPC) standard, namely: the *ANSI/ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with guidance for use* and the Maturity Model that was developed to complement its cost effective implementation and maintenance.

The framework of the research was based on the following main elements:

- The use of standards in security risk management;
- Background to Organisational Resilience;
- Using a Maturity Model;
- Auditing the system; and
- A case study.

The case study was based on the first ever implementation of the Organisational Resilience Standard using a Maturity Model which was specifically designed for the project. This was done to expedite implementation and allow for tailoring the implementation process to the resource constraints of each facility.

One of the challenges in the formulation was converting a generic standard and customising it for use by the hospitality industry. An important lesson learnt was the

need to engage people in the process, since buy-in from all levels was the key to achieving the required results. The phased approach taken in the case study provided a manageable path for implementation.

The research study found that putting into practice the Organisational Resilience Standard as a Management System, using the Maturity Model for the hospitality sector, had distinct advantages. The maturity model proved viable as a risk management tool and improved the manner in which the different elements of the SPC.1 standard were implemented and maintained by the organisation. This finding was based on the case study as implemented at the Tsogo Sun Group prior to the FIFA World Cup in 2010 and the subsequent audits over the past two years.

The effectiveness of the implementation of the Maturity Model based on the SPC.1 proved to be successful in the case study. The resilience approach enabled the organisation to better allocate resources and priorities. By simultaneously considering minimising likelihood and consequence, it was possible to build a layered approach of technical and administrative measures, balancing strategies to minimise the likelihood of consequences. The maturity model used a phased implementation approach that created the culture of “risk ownership” with employees and other stakeholders.

It was further found that, by using the Maturity Model, all levels of management were allowed to have and experience a constant understanding of what level of resilience existed within the organisation. It also gave management and other stakeholders the confidence to know that the organisation could have a positive impact on and extensively minimise the likelihood of potential disruptive events and other risk threats occurring. It was also found that in implementing the Maturity Model, would, in all likelihood, also mitigate the consequences should these actually occur and thereby enhance recovery time by allowing recovery to occur in an orderly and rapid fashion.

A paradigm shift in Security Risk Management using the Maturity model is thus possible in most resilient organisations willing to implement the Model.

CHAPTER 1
INTRODUCTION AND MOTIVATION FOR THE RESEARCH

1.1 INTRODUCTION

Organisations manage and maintain infrastructure and contribute to society by providing employment and essential goods and services to communities. Events, such as unexpected or unplanned for major hazardous incidents, natural disasters causing infrastructural damage and deliberate attacks on an organisation including crime threats impact on the ability of organisations to continue to function. They also have an influence on the length of time that essential services are unavailable and on the duration of recovery for the community as a whole. There is a need to critically evaluate the consequences that such events may have on organisations and their resilient capability to survive these events. In this context 'resilience refers particularly to organisations ability to survive and continue all operations in a profitable manner. A significant challenge to achieve this goal lies within the complexity of organisations and the ever changing context within which they operate (Stephenson, Seville, Vargo & Roger, 2010: i)

The ability of organisations to avoid and respond effectively to adverse events depends on the organisational structure, management and operational systems, and the combined resilience of these to address such an event. This research study explores how the concepts of systems may be used to understand specific areas of complexity, and suggests a potential framework for implementing a 'Maturity Model' that contributes to the resilience of organisations.

A case study was used which encompassed the known threat elements in an audit survey matrix allowing for security professionals to re-evaluate the way in which organisations should prepare for unexpected and disastrous incidents. In 2009 the publication of the American National Standards Institute and ASIS International's Security, Preparedness and Continuity (SPC) standard, namely: the *ANSI/ASIS SPC.1-2009 Organizational Resilience*: *Security, Preparedness and Continuity Management Systems – Requirements with guidance for use,* allowed for such a new approach.

The researcher used the methodology from the *ANSI/ASIS SPC.1-2009* organisational resilience standard as the foundational approach for this research. The implementation of the standard was undertaken at the Tsogo Sun Group (TSG), a major enterprise in the African Hospitality Sector. A Maturity Model that was specifically developed for the project at TSG formed the main framework for the implementation. This was the first time that such an implementation was done by security professionals anywhere in the world. This dissertation documents and tracks the implementation and impact thereof.

1.2 PROBLEM STATEMENT

The problem that forms the foundation of this research is the following research question:

> *Is it possible to bring about a paradigm shift in security risk management using a Maturity Model based on the main elements required in the ANSI/ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with guidance for use.*

1.3 RATIONALE FOR THE STUDY

This study is an extension of the implementation of the Organisational Resilience Management System (ORMS) at Tsogo Sun Group, where the researcher was the project leader from inception to the delivery, auditing, impact evaluation and full implementation. Approximately eight months before the start of the 2010 FIFA (Fédération Internationale de Football Association) Soccer World Cup that was held in South Africa, the Director of Risk at TSG wanted a single risk management system tool to streamline the various risk elements faced by the group. The Tsogo Sun Group wanted a process that would be relevant and cost effective for them to consolidate their various risk management efforts under a single control mechanism in the organisation.

The FIFA Soccer World Cup of 2010 presented the challenge for a range of risks, due to natural, intentional and unintentional events. Given the limited timeframe and resources available to prepare for the FIFA tournament, was necessary to devise a

comprehensive approach to risk management that consolidated Tsogo Sun's previously fragmented (often isolated in 'silos' or separate compartments) methodological approach into a single strategy of identifying gaps and avoiding duplication. The identification and roll-out used the SPC.1 as the basis for the project along with the Maturity Model to evaluate a methodology that eliminated risk silos while tailoring the implementations to drive the cultural change and affect a 'paradigm shift' in risk management practitioners.

The following disciplines are part of the Resilience Management system:

- Risk Management;
- Security Management;
- Emergency Management;
- Disaster Recovery Management;
- Business Continuity Management; and
- Occupational Health and Safety Management.

The Maturity Model combines the strategies of managing identified risks and providing an enhanced ability to respond quickly and effectively when a crisis occurs, irrespective of whether the event was previously identified as a risk or not.

1.4 RESEARCH OBJECTIVES

The objective of this research was to evaluate the effectiveness of using the Maturity Model with the SPC.1 standard to manage security risks within the context of a Security Risk Management approach.

1.5 RESEARCH QUESTIONS

The following questions formed the framework of this research:

1.5.1 *Do International Organisation for Standardisation (ISO) standards contribute to forming an organised framework for security risk management*?

1.5.2 *Are there any benefits in implementing the ORMS in an organisation?*

1.5.3 *Does the Maturity Model for the ORMS have any measurable benefits for an organisation?*

1.5.4 *How does the use of recognised audit systems or procedures add value to the achievement of the paradigm shift in security risk management using the Maturity Model?*

1.5.5 *Does an organisation's agility improve the possibilities of identifying and dealing with risk incidents, improve after implementing the ORMS using the Maturity Model?*

1.6 AIM OF THE RESEARCH

The primary aim of this research was to study the transition of an organisation's risk management approach from a fragmented approach to a comprehensive strategy using the Organisational Resilience Standard in tandem with a Maturity Model.

The secondary aim was to:

- establish if resilient organisations are able to make a paradigm shift in order to improve the management of risks for the future using the ANSI/ASIS SPC.1 which included the development of plans to reduce risks that had not yet been established; and

- examine whether resilient organisations are more agile in managing risks and better prepared to face the risks of unexpected events.

1.7 KEY THEORETICAL CONCEPTS

The key theoretical concepts for this study focussed on Organisational Resilience and the Maturity Model since these applied to the issues that are covered by risk management components. This included the following focus areas:

Risk Management: "Coordinated activities to direct and control an Organisation with regard to risk" (International Organisation for Standardisation (ISO) ISO Guide 73: 2009: 2).

Emergency: “Sudden, urgent, usually unexpected occurrence or event requiring immediate action” (International Organisation for Standardisation Publicly Available Specification (ISO/PAS) 22399:2007: 2).
Disaster: “Event that causes great damage or loss” (ISO/PAS 22399:2007: 2).

Continuity: “Strategic and tactical capability, pre-approved by management, of an organisation to plan for and respond to conditions, situations, and events in order to continue operations at an acceptable predefined level” (American National Standards Institute/ASIS International (ANSI/ASIS) SPC.1-2009: 45).

Security Risk Management: “The condition of being protected against hazards, threats, risks, or loss” (ANSI/ASIS SPC.1-2009: 47).

Occupational Health and Safety: When the Occupational Health and Safety Assessment Series (OHSAS) 18001:2007 uses the term occupational health and safety, it refers to all of the factors and conditions that:

> ….affect health and safety in the workplace, or could affect health and safety in the workplace. Occupational Health and Safety (OH&S) factors affect employees (permanent and temporary), contractors, visitors, and anyone else who is in the workplace (OHSAS 18001:2007: 3.12).

The **Organisational Resilience** (OR) management programme is more fully described in a later chapter of this dissertation. However, the base definition is to be found in the standard itself:

> Ongoing management and governance process supported by top management; resourced to ensure that the necessary steps are taken to identify the impact of potential losses; maintain viable recovery strategies and plans; and ensure continuity of functions/products/services through exercising, rehearsal, testing, training, maintenance, and assurance (ANSI/ASIS SPC.1-2009: 47).

Maturity Model: The definition of a Maturity Model for this specific standard was published in January 2010 (Siegel & Siegel). The first implementation test anywhere in the world by security professionals of the model was done as described in the case study. The definition by Siegel and Siegel (2010: 3) describes the model as:

> The Maturity Model for the phased implementation of the *ANSI/ASIS SPC.1-2009* is a series of steps designed to help organisations evaluate where they currently are with regard to resilience management and preparedness, set goals for where they want to go, benchmark where they are relative to those goals, and plot a business sensible path to get there. Standards are designed to promote managed and repeatable performance. This will be achieved by moving up the phases of the model.

Organisational Resilience as a science, linked to security risk management, is a relatively new concept. It is an examination of many unknown factors and could be classified as a futuristic perception in applying the practices highlighted in this chapter.

1.8 RESEARCH PLANNING (CHAPTER LAYOUT)

Chapter 1: Introduction and motivation for the research. This chapter covers the problem statement, rationale for the study, research problem, research questions, aim and key theoretical concepts.

Chapter 2: Methodological exposition of the research design

The methodological exposition for this research is discussed in this chapter. It creates the framework for the research that was done to see how effective the use of a Maturity Model would be in creating a paradigm shift in security risk management.

Chapter 3: Background to international standards and their use in security risk management

This chapter looks at the traditional standards that have been used to improve security risk management from both an international and national perspective.

This was followed by the work being done by Technical Committee (TC) 223: Societal Security, in the development of ISO 22300 which is expected to be published in 2012. The last part of this chapter was used to give a brief description of *ANSI/ASIS SPC.1-2009.*

Chapter 4: Background to Organisational Resilience

This chapter takes a deeper look at Organisational Resilience: how it compares to traditional risk management, resilience and corporate governance, what the benefits are of Organisational Resilience, what resilient organisations appear to be and the reliance on stakeholders and society to make it work. It investigates Resilience Management as it applies to changing security risk management. The application of risk management models to manage the components that make up Organisational Resilience are discussed. In summary, the discussion is focussed on elements that are required for the focus areas that organisations may use to become more resilient.

Chapter 5: Using a Maturity Model

This chapter defines and discusses some previously used Maturity Models before specifically discussing the Maturity Model as it applies to Organisational Resilience in this research document. This included the development of Maturity Models, their structure through the five or six levels as applied in practice.

Chapter 6: ISO 19011: 2002 guidelines for quality and/or environmental management systems auditing

This chapter deals with the auditing tools necessary for the implementation of management system. The audit methodology used and specifically developed for the case study is outlined, as well as the audit guidelines according to ISO 19011: 2002 in respect to security systems.

Chapter 7: Case Study: implementation of an organisational resilience management system using a Maturity Model

The findings of a functional case study where the Maturity Model was used to implement the ANSI ASIS.SPC.1 Organisational Resilience Management System at Tsogo Sun Group. The chapter covers the research that lead to the implementation

through to the reaction and impact in respect of the implementation at group and unit level.

Chapter 8: Findings, recommendations and conclusions

This chapter is a summary of the results of the research as it relates to the Case Study. Recommendations are made which may, in the future, serve companies in a positive manner in order to deal with these identified issues under a single methodological approach to risk management.

CHAPTER 2
METHODOLOGICAL EXPOSITION OF THE RESEARCH DESIGN

2.1 INTRODUCTION

The methodological exposition for this research is discussed in this chapter. It creates the framework for the research that was done to test the effective use of the Maturity Model in Security Risk Management.

As point of departure, a literature study was conducted, enhanced by an empirical study and the case study. The mixed method approach was used incorporating qualitative, quantitative and evaluative components. The data collection technique used included interviews, observations and corporate documents, complemented by a practical evaluation of impact of the implemented Maturity Model.

The various methods will be explained, whereafter the mixed method design based on the work of Mouton (2009: 160-162) will be discussed and evaluated as the research framework for this study.

2.2 RESEARCH APPROACH AND DESIGN

2.2.1 Literature study

A literature study was conducted. Search criteria such as resilience, organisational resilience, standards, standards approach, risk management and resilience, security risk management sciences, paradigm shift, were used during the literature research.

No reference was found on how these standards may be applied to the managing of security risks in the Private Security Industry in South Africa. The researcher divided the research into different concepts which applied to the elements of Security Risk Management as these could be applied to the fuller concept of Risk Management based on the broader requirements as stated in *ISO 31000:2009 - Risk Management* and the other relevant management standards.

In doing this, the researcher found literature relevant to the study. Literature was studied to explore the national and international arena for current practices in the

collection, analysis and utilisation of security risk information as it pertains to the "Organisational Resilience Management System" and the use of a "Maturity Model" in managing security risks (ANSI/ASIS SPC.1:2009).

2.2.2 Empirical study

Scientific statements are subject to and derived from personal experiences or observations (Anon., Nd). Patton, M.Q. (2008: 544) states that an empirical approach means gathering data on actual programme activities. The collection of the data has to then be presented in a fair and balanced way. The users of the information should be able to use the data to make their own judgements about its usefulness or not. Thomas Khun has promoted the concept that these methods, namely observation, experience, and experiment, are influenced by prior beliefs and experiences (Khun as cited in Patton, 2012: 286).

Although two scientists may look at the same thing, they may literally not see the same thing because of their different theoretical perspectives, assumptions or ideology-based methodologies. This process helps researchers inquire into the empirical nature of the world that produces objective findings (Patton 2012: 286).

To enhance the empirical study conducted by the researcher, a literature study was conducted. The American Heritage Dictionary of the English Language (Online Edition - 2012), defines the word empirical as results that support the hypothesis, and secondly as information gained by means of observation or experiments. Empirical data is data produced by an experiment or observation and not by theory.

For the purposes of this study the empirical research design was used to investigate the nature and extent of the problems experienced by organisations to make a paradigm shift when using the Maturity Model. The research included the understanding of, and resistance to, establishing resilience protocols in an organisation. Social science is said to be empirical, when knowledge is based on what one experiences (Mouton, 2009: 140). This research is a case study with mixed-method research approaches and contains elements of both the qualitative and quantitative methodologies along with an evaluative component.

The researcher was able to document data/information from first-hand experience. The description of some of the aspects of this research came from practical experiences of Organisational Resilience and the use of the Maturity Model. An analysis of the data/ information was done and categorised into specific themes and categories. This allowed the researcher to study selected issues in depth, transparency and detail. The researched information allowed for a better understanding of the main themes and sub-categories as these apply to both the Organisational Resilience Standard as well as the Maturity Model.

The research was flexible and data collection was less structured but more accessible. The researcher was able to make changes in the investigation of the possibilities of a paradigm shift in managing security risks by using the SPC.1 standard and the Maturity Model. This allowed for the study to be more flowing, naturalistic, participatory and interpretive (De Vos, Strydom, Fouché, Delport, 2009: 264, 268, 269 & 271).

2.2.3 Case Study

Stake (1995: 5) states that the sole criterion for selecting cases for a case study should be the 'opportunity to learn'. Imas (2010: 5) defines a case study as: "…a method of learning about a complex instance, based on a comprehensive understanding of that instance obtained through extensive description and analysis of that instance taken as a whole and in its context". Flyvbjerg (2011: 301), also describes a case study as an intensive analysis of an individual unit (e.g. a person, group, or event) stressing developmental factors in relation to context. For the purposes of this study, the unit of analysis is therefore, the implementation (event) of the ANSI/ASIS SPC.1 standard and the Maturity Model.

According to Stake (1995: 8-9) the purpose of a case study is particularisation, and not generalisation when a particular case is taken and become well-known. The emphasis is on uniqueness and this is obtained by placing an observer in the field to observe the workings of the case, one who records objectively what is happening but simultaneously examines its meaning and redirects observation to refine or substantiate those meanings. During this study, the researcher also fulfilled the role of an observer when conducting research with the business units, the groups and

during the implementation of the Maturity Model. The researcher had the opportunity to observe, amongst others, how the General Managers prepared the monthly set of reports as required by their head office. This assisted with understanding how the implementation of the Maturity Model could assist in improving or refining the processes.

With regard to the methodology used, Imas (2010: 5) postulates that the methodology used in a case study is a form of descriptive and evaluative research which has a qualitative outcome. Imas (2010: 10) further states that the approach to be taken should be one with a holistic view of complex instances where the following would provide part of the results: observation, progressive focussing, searching for patterns, and developing assertions.

Case studies can thus be categorised as follows:

Descriptive

- The intervention is described and the context in which it occurred;
- Realism is added as well as in-depth examples to other information about a programme, project or policy;
- The present situation is described fully to indicate what a situation is like and why something specific may be happening;
- Assists with the interpretation of survey data; and
- Small numbers are used for survey purposes. These are all aspects that were covered in this specific Case study.

Explanatory

- Causal links in interventions are explained from the links in the programme to what the effects could be:
- Explore little known situations about a specific intervention or its likely results and effects.

Combined

- Findings from several case studies are brought together to answer an evaluation question
- Findings from a number of case studies are consolidated to find an answer to an evaluation question, as to whether it is descriptive, normative, or cause and effect (Imas, 2010: 21-26).

Although these are depicted as separate items, in practical terms these overlap during programme implementation, where case studies investigate operations at numerous sites and frequently in a normative manner.

The research design used in this study poses the 'why' or 'how' of the programme implemented in the case study. The key elements are descriptive and explanatory.

2.3 METHODOLOGICAL PATH OF THE STUDY

An exposition of the methodological sequence includes the following aspects: demarcation, data collection, data analysis and validity.

2.3.1 Demarcation: Population and sampling procedures

Sampling refers to the process used to select a portion of the population for study. Qualitative research is generally based on non-probability and purposive sampling. Purposive sampling means that participants are selected because of some defining characteristics that make them the holders of the data needed for the study. Purposive sampling decisions are not only restricted to the selection of participants but also involve the settings, incidents, events and activities to be included for data collection (Nieuwenhuis, 2010: 79).

For the purpose of this research stratified purposeful sampling was used as it means that participants are selected according to preselected criteria relevant to a particular research question. In this case, participating businesses units and individuals were sampled. Sampling was conducted via workshops with individuals and groups at the various business units. One-on-one discussions with the general managers and Heads of Departments which included finance, food and beverage, housekeeping,

maintenance and security where these formed part of the business unit's organisational structure were held. Use was made of a structured interview schedule that will be discussed in chapters seven and eight and attached as Annexure B). Not all business units had such a full complement of staff members, as structure was dependent of the business units' size and requirements for such positions. Adaptations were thus made in those specific instances.

The sample size pertaining individuals was not fixed prior to data collection as it depends on the resources and time available to the researcher, while the sample size with regard to the business units was fixed.

2.3.1.1 Sample size

Business units

From a total of 114 business units five were selected by the Director of Risk of the Tsogo Sun Group (TSG) as the 2010 FIFA World Cup participating teams, also referred to as the "FIFA Family" would reside there. The units are also known for their efficient administrative practices and senior level management who would be able to assist with the refinement of the documentation and existing Standard Operational Procedures (SOPs). The selected business units were:

- Five-star hotel in Sandton (Gauteng);
- Three-star hotel in Morningside, Sandton;
- Four-star hotel in Durban (KwaZulu-Natal);
- Casino in Durban
- Casino in Emalahleni (Mpumalanga), which also has a three-star hotel attached to the same building (Only used for the initial document review).

The choice of the facilities in Sandton was based on the fact that the specific five-star hotel would serve as the base for the "FIFA Family" which consisted of the executive and support staff of the organisation, invited VIPs (Very Important People), including heads of state, and media representatives from around the world. The casino facility that was chosen was in Durban. This facility was chosen since it had a very good support capacity that would be able to assist with the timely

implementation and roll-out of the programme. The casino is close to the Moses Mabhida Stadium (Durban FIFA World Cup match stadium) and was extensively frequented during the 2010 FIFA World Cup.

Participants

The initial discussions were held at the selected business units with stakeholders at all levels, keeping in line with the requirements of the resilience programme. The briefing consisted of a PowerPoint presentation on what Organisational Resilience was all about and how TSG would like to roll it out over the next few years. The presentation included an outline of the requirements of the programme, the implementation methodology and the ongoing audit and reward programmes.

Stratified purposeful sampling was conducted via workshops with individuals and groups at the various business units. One-on-one discussions with the general managers and Heads of Departments which included finance, food and beverage, housekeeping, maintenance and security where these formed part of the business unit's organisational structure were held. A structured interview schedule was used. Not all business units had a full complement of staff members, as structure was dependent of the business units' size and requirements for such positions. Adaptations were thus made in these specific instances.

All internal stakeholders were included in the second and third rounds of discussions and workshops held at the facilities. In the initial research of the documentation and SOPs, the attendees numbered approximately four to eight which later grew to larger numbers of 32 depending on the size of the unit and the availability of staff during these sessions.

For this study, twelve interviews were conducted and a total of 71 participated.

2.3.2 Documentation review

A documentation review was undertaken and workshops were conducted with staff at all levels. During the initial evaluation process, samples of the documentation, such as security and safety policies and procedures, emergency planning, business continuity plans and disaster management plans were perused. This was done in

order to establish whether these documents were relevant to the process of organisational resilience and fitted into the Maturity Model.

A document review was undertaken at each business unit. Existing systems and operational procedures were evaluated against the requirements of the ORMS. Documents that weren't required were taken out of the system and a new index created that satisfied the TSG requirements, measured against the criteria of the Maturity Model. The documentation that is now used by the business units serves as the foundation of their ORMS. The gaps were identified and solutions sought to bring the documentary proof in-line with the requirements of the ORMS and the Maturity Model.

2.3.3 Pilot Projects

The researcher conducts a pilot study to ascertain whether the selected database was correct and where gaps in the data occur. The pilot study was conducted at the five selected units.

The documents at these facilities were reviewed and the usefulness of each document was evaluated against group security and corporate governance policies as well as other legal requirements for effective management. Discussions were held with staff members and contractors at all levels to ascertain the practicality of some of the documentation and processes. This was done so that the most effective system for the group could be devised and where required, documentation was discarded and reporting mechanisms realigned. Contractors included specialists in the fields of fire safety, sprinkler maintenance, air conditioning, electrical, water maintenance and sewerage. Meetings were also held at each of the centres with the local municipal Health Inspector and Fire Protection Liaison Officer, as life safety is of the utmost importance in any emergency plan, as it also forms one of the main pillars of resilience planning.

2.3.4 Data collection

A number of different collection methods were used to collect data for this research project. These included an interview schedule, questionnaires, documentation

reviews (hard copy information) and the collection of physical artefacts, interviews, and observation.

2.3.4.1 Hard copy information

Each business unit already had some form of security, safety and business continuity programme in place that had been developed and updated over many years. The result was that most of the existing documents, monthly/quarterly/six monthly/annual reports were robotically filled in and sent in as required by the group's operating procedures and compliance requirements. In general, the system looked as if it was working, but gaps were found which indicated that the processes required a review and update.

TSG selected the ORMS as the vehicle to refine the existing system and bring the operations in line with international best practice and ensure compliance where applicable.

2.3.4.2 Interviews

Number of interviews: Twelve interviews were conducted with 71 interviewees. Three one-on-one interviews were held with TSG Risk Executives and six group interviews were held with other TSG executives and staff. A tenth interview was held at the closing of the training course held in Centurion in July 2011 and two follow-up interviews on 14 June 2012.

Interview schedule: For these 71 interviews, a structured interview schedule (Appendix 'B') was used. The structured interview schedule consists of a set of 21 questions, covering aspects such as corporate security policy, risk management Plan, security plan, business continuity plan, fire safety plan, occupational health and safety program, updates and revisions of the plans. These questions were posed to all the individuals and groups during the interviews. The questions were closed and required either a 'yes' or 'no' answer.

The researcher made use of one-on-one interviews and group interviews. Nieuwenhuis (2010: 90) explained a group interview as the asking of a set of semi-structured or structured questions to a group of participants without debating or

arguing about the responses being generated. Group interviews were in contrast with focus group interviews when the discussion was focussed on a particular topic. Debate and even conflict were encouraged and group dynamics assisted in data generation.

Four levels of discussions can be distinguished.

- The first level of group interviews centred on the applicability of utilising a management system to enhance and refine the existing risk management portfolio, which included security, emergency planning, disaster management, business continuity and occupational health and safety. On completion of the discussions it was agreed that all of these elements were to be combined under a group Organisational Resilience Plan. These discussions also created the opportunity to fully brief each of the unit General Managers on the TSG Policy decision to implement the Organisational Resilience Management System (ORMS) in the company. On completion of these briefings, the General Managers all individually gave their full support to assist with the implementation and delivery of the programme.

- Informal one-on-one discussions were also held with other specialists [e.g. maintenance, housekeeping, food and beverage, etc.). based on the questions formulated in the structured interview schedule (Appendix 'B') at each unit in the various disciplines that were covered in the organisational resilience project. These respondents assisted with the clarification of some of the practical operational barriers that they encountered, as well as giving some practical guidance where avenues had not previously been adequately covered.

- Group interviews were held with staff and contractors at all levels to ascertain how practical some of the documentation and processes were. This was done so that the most effective system for the group could be devised and where required, documentation and reports realigned for practical implementation.

- The final level of group interviews was with non-management staff members, using the structured interview schedule (Appendix 'B') at all operational levels. These included the security, maintenance, finance, front desk, guest services, cleaners, housekeeping, kitchen, beverage and, garden and landscaping staff.

Their replies were documented and contained in the field notes.

2.3.4.3 Observation

Four types of observation can be identified (Nieuwenhuis 2010: 85), namely complete observer, observer as participant, participant as observer and complete participant. For the purpose of this research the type of observation used was the participant as observer, because the researcher becomes part of the research process with the aim to gain an insider perspective of the setting (emic perspective). Observations were documented in the field journal.

2.3.4.4 Field notes (journal)

An informal field journal was kept. Notes on meetings were written and filed in the applicable section that was researched or worked on at the time. Decisions that were taken during the research and implementation of the project at Tsogo Sun Group resulted in the changing the document requirements. The documents that were refined and eventually reintroduced into the revised ORMS were then filed in specially developed files and in a specified format and order. This assisted with the enhancement of the management system at both an executive level for good corporate governance and at an operational level to ensure a functional operational system and an audit trail.

At the outset of this study, the concept of Organisational Resilience was difficult for the staff members to understand. Initially this was quite a challenge as it was noticed that the theory that we were trying to impart, was not making any sense to them. This meant going back to basic communication and developing communication mechanisms that would explain to them exactly what would be influenced in their specific environment to ensure that they would participate more fully in the roll-out of the management system. This meant developing different communication presentations to ensure that they understood what was required from them. This

worked well and assisted with a smooth roll-out as the project continued within the group.

However, the following has to be borne in mind during the research: Campbell and Stanley (1963: 5) provide a framework for evaluating the limitations that various types of research studies pose with respect to inferring a causal link between independent (treatment) and dependent (outcome) variables. They suggest a necessary relationship between the validity of an individual research study and the generalisation of results from this study to wider populations. No major issues were encountered during the research or implementation phases of the project. The TSG Project Team, consisting of the researcher, five risk managers from TSG and another consultant from Temi Group,[1] worked well together and management had given its full support, in many aspects, to ensure that the implementation could be done effectively in the short time that was available.

2.3.5 Data analysis

Creswell (2008: 7-15) discusses the views of Merriam (1988) and Marshall and Rossman (1989) who contend that data collection and data analysis must be a simultaneous process in qualitative research. He also mentions the claims that were made by Schatzman and Strauss (1973) that qualitative data analysis primarily entails classifying things, persons, and events and the properties which characterise them. He further implies that researchers seek to identify and describe patterns and themes from the perspective of the participant(s), then attempt to understand and explain these patterns and themes (Agar, 1980).

Data analysis and interpretation were based on the basis of Creswell's model (2008: 7-15) and included the following circles: collecting and recording data, managing data, reading and writing memos, describing, classifying and interpreting, and representing and visualising. Data was collected through different types of sources (documentation reviews, interviews, and observation) at various stages of the project at the TSG business units. The initial collection was done during the gap analysis phase. A second phase of information was collected during the pilot studies which

[1] Temi Group is a global security risk management company with a subsidiary company in South Africa.

were conducted on the same dates and places where the interviews were held, whereafter the researcher organised the data while making them easily retrievable and manipulatable.

Once the implementation started, all business units were obliged to follow the group policy as set down by the TSG Executive Board which supported the implementation of the project and required all stakeholders to participate in the implementation of the Maturity Model for the ORMS.

Existing reports made at all operational levels relating to any of the risk management processes connected to the ORMS were reviewed. These reports consisted of checklists and incident reports that were required in the SOPs. The analysis of the data was done at business unit level. A gap analysis was conducted at each level based on the requirements of the project plan and the revised index of documents was developed and implemented (See Chapter 7). This was used to refine the existing systems and required reports. Some of the reports and checklists had become redundant and others had become too cumbersome and were not adding any value other than that of wasting time and resources. Some reports were updated and refined as they were necessary for insurance risk management as well as compliance issues which needed fixed-time reports to stay compliant. On completion of this level of data review, the final list of future reports and documents were decided on. These would then form the framework of the implementation of the ORMS programme within TSG.

2.3.6 Reporting the findings

Lofland 1974: in Creswell (2008: 7-15) suggests that although data collection and analysis strategies are similar across qualitative methods, the reporting methods are diverse. Miles and Huberman 1984: in Creswell (2008: 7-15) address the importance of developing and displaying the data. They further state that narrative text is the most frequent form of display for qualitative data. The reader thus gains first-hand experience as to the challenges that were encountered during the research and how the outcomes were achieved Creswell (2008: 7-15).

The results are presented in a descriptive, narrative form rather than as a scientific report. The researcher's experiences and the meanings he attaches to these will be included mainly in the research findings chapter.

2.4 RELIABILITY AND VALIDITY

Fouche and De Vos (2009: 101) make the following comparisons in respect of the assessment and suitability of the research approach:

> In some instances the choice of topic will be the main determinant of the approach selected, but sometimes the researcher might still be able to change the focus of the selected topic to better suit one or the other approach. It is important that the researcher ignore his bias towards either if the topic does not lend itself to a certain approach.

They further state that in the practical environment of human sciences research both quantitative and qualitative methodology is occasionally knowingly used but at other times intuitively (Fouche & De Vos, 2009: 103). Neuman (2000: 16-17) is of the opinion that each has its own strengths and limitations, topics or issues where it excels, and classic studies that provide remarkable insights into social life. By understanding both styles, the researcher will be able to distinguish from a range of research that can be used in both contemporary ways.

Campbell and Stanley (1963: 5) argue that internal validity is the basic minimum without which any experiment is un-interpretable and question if in fact the experimental treatments make a difference in this specific experimental instance.

Typical of potential threats to internal validity are:

- Uncontrolled, extraneous events occurring during the study (called a 'history' threat);

- Failure to randomise interviewers or raters across comparison groups (called an 'instrumentation' threat);

- Biased or differential selection of cases as occurs when groups are self-selected in a case-control study (call a ‘selection’ threat); and

- Differential loss of cases from comparison groups when there is no pre-test to assess the impact of the loss (called an ‘experimental mortality’ threat).

Towards the end of the two-week training course that was delivered by Dr Siegel, Standards Commissioner, ASIS International, USA, a discussion was held on how the project would be able to set proper guidelines for implementation and measurement which were reliable and valid. The group of six students attending the course were of the opinion that the existing measurement tool, a self-assessment checklist, would not adequately provide an in-depth analysis of the real situation. As the researcher was leading the implementation project at TSG, a discussion was held between himself and Dr Siegel to find a solution.

There was no valid measurement capability in the Maturity Model and the researcher made suggestions to TSG on how this could be done. The proposal was accepted and implemented. A refined measurement capability was then added by the implementation team to evaluate the level of the capability of the business unit while also identifying the gaps that existed in their ORMS. This measurement system has now been used in the recently published *ANSI/ASIS.SPC.4-2012: Maturity Model for the Phased Implementation of the Organizational Resilience Management System*, standard. This measurement system is discussed in Chapter six of this research report.

2.5 LIMITATIONS OF THE RESEARCH

This study had a short timetable during the research and implementation of the project at TSG before the FIFA World Cup of 2010. The study was limited to the implementation of the ORMS at five properties within TSG and the research that was done in the initial pilot study of the five other business units. The researcher would have preferred to have been involved in a bigger sample, but time was limited due to the project scope that was agreed to with TSG prior to the World Cup.

2.6 VALUE OF THE RESEARCH

The following organisations, institutions and individuals may gain from implementing and considering the expected recommendations emanating from this research:

- The Programme: Security Management in the Department of Criminology and Security Science in the School of Criminal Justice of the College of Law at the University of South Africa (UNISA), for the results obtained and also the integrated approach to the security risk management process and training of professional security risk managers. The research findings could also possibly be utilised by this Department for inclusion in either short courses for study material for professional security risk managers.

- Any type of business entity, from the smallest business to the largest global enterprise, could utilise the guidelines and the Maturity Model.

- The changing trends of securing businesses across a number of disciplines relating to risk management, would allow for the implementation of the ORMS standard as a tool to ensure that such businesses can quickly respond to threats and incidents in a resilient manner.

2.7 ETHICAL CONSIDERATIONS

Ethical considerations in the research were addressed by adhering to the *Policy on Research Ethics at UNISA* (UNISA, 2007: 1-16).

This research was based on a case study where the individual participants mostly formed part of workshop groups. Where individual interviews were held, these were mostly with the general managers of the individual business units and/or their heads of departments. All respondents were informed that information received would be treated as strictly confidential although this formed part of their job analysis. In addition, high standards in the research were maintained by means of focusing on implementing the proper referencing an acknowledgement of sources of information, avoiding plagiarising of information and of obtaining the consent of the respondents

to participate and permission to undertake the research from the relevant organisations. These factors all aimed at increasing the acceptance of the information received by respondents, as well as to enhance the validity of the research conducted.

As the case study is based on the project at Tsogo Sun Group, they gave permission for the implementation to be used in this study with the proviso that their specific intellectual property (IP) be protected and that none of their confidential data was to be used in the study. A non-disclosure agreement was entered into between the researcher and TSG in this regard. The result has been that actual results have not been used to show the real impact of the roll-out and implementation of the ORMS in TSG. The full extent and description of some documents have also not been used.

The tables used for reference in this section are used with the permission of ASIS International who is the copyright holders.

The researcher has been involved in security for the past forty two years and in the Organisational Resilience discipline for the past three. Organisational Resilience is a relatively new methodology as the first standard on this subject was only published in 2009 and has taken some time to enter the market.

2.8 SUMMARY

The mixed-method approach of research methodologies which was used in this research and the expected outcomes was explained in this chapter.

Chapters one and two have set the context for the academic outline of the research. The next chapters will describe how ISO standards are developed, the development of the Maturity Model used in the Case Study for this research and how these can be used in determining whether a paradigm shift is possible in Security Risk Management using a Maturity Model.

CHAPTER 3
BACKGROUND TO THE DEVELOPMENT OF INTERNATIONAL STANDARDS AND THEIR USE IN SECURITY RISK MANAGEMENT

3.1 INTRODUCTION

The British Standards Institute defines a standard as an:

> …agreed, repeatable way of doing something. A standard is a published document that contains a technical specification or other precise criteria designed to be used consistently as a rule, guideline, or definition (British Standards Institute (BSI), 2011).

In brief standards assist in making life simpler by having a set 'benchmark' as a guideline for everyone to subscribe to and follow for any product and/or activity following established 'best practices'. This ultimately increases the reliability and the effectiveness of many goods and services. Standards are created by bringing together the experience and expertise of all interested parties such as the producers, sellers, buyers, users and regulators of a particular material, product, process or service.

The latest edition of The ISO Survey of Certifications, for 2010, underlines the global market relevance of ISO's management system standards for quality, environment, medical devices, food safety and information security revealing a 6.23% increase in the number of certificates for a worldwide total of 1 457 912 certificates and users of one or more of the standards in 178 countries (ISO, Nd(a)).

The biggest increases in certification has occurred in the sector-specific ISO 22000:2005 food safety management system standard, which is up by 34% The issue-specific ISO/IEC 27001:2005 information security management system standard has also experienced an increase of 21%. ISO/IEC 27001:2005 sets the requirements for information security management systems. By the end of 2010, at least 15 625 ISO/IEC 27001:2005 certificates had been issued in 117 countries. The 2010 total represents an increase of 2 691 (+21%) over the 2009 total. The three

countries with the highest number of total of certificates are Japan, India and the United Kingdom, while the top three for growth in 2010 were Japan, China and the Czech Republic (ISO, Nd(b)).

A prudent Chief Executive Officer (CEO) of a company or an organisation will understand that the market value of the organisation does not lie in its reporting capabilities but in the manner in which it uses its assets to generate business (Stimson, 2012: 3). The impact that systems can have on organisations is both positive and negative depending on the manner in which these are implemented, managed and controlled as organisations try to achieve 'best practice'.

In an undated open letter to Stevan Breeze, CEO of the British Standards Institute (BSI), Prof John Seddon, an anti-ISO9000 proponent, says that the only reason that he believes that organisations register for ISO9000 is because of coercion from the market-place where it is said that 'you comply [with ISO standards], we buy'. At the time of him writing the letter to Breeze, only one percent of all registered companies had registered for ISO9000.

He further states that:

> Clearly our ideas about 'best practice' differ. You seem to think 'best practice' is the result of people sharing opinions, I think 'best practice' should be deteremined empirically. The same problemis occurring currently with what is called the Call Centre Associaiton's 'best practice' standard. People in the call centre industry have written a standard and your people will happily take fees for assessing conformance to it, but no one is concerned about determing wether this standard is worthy. I maintain this standard [ISO9000] ought to be called the 'sweat shop' standard, for it contains all of the features that have created the sweat shop phenomenon (Seddon, 2012: 1).

An expanded discussion about the positive or negative aspects of management systems based on ISO9000 does not form part of this research. It has been introduced to show that not all elements of management systems have a positive

impact on an organisation. Organisations should also be aware of the negative elements that could influence their businesses during such implementations.

The ISO or non-ISO standards as these apply to the Security Risk Management environment are mostly based on the principles of:

- ***ISO 9001:2008****: Quality management systems - Requirements;*
- ***ISO 9004:2000****: Quality management systems: Guidelines for performance improvements; and*
- ***ISO 14001:2004****: Environmental management systems -- Requirements with guidance for use.*

Management systems standards that have a specific impact on security risk management include the following:

- ***ISO 19011: 2002:*** *Auditing system guidelines;*
- ***ISO 22301:2012****: Societal security - Business continuity management systems - Requirements;*
- ***ISO/PAS 22399:2007****: Societal security - Guidelines for incident preparedness and operational continuity management;*
- ***BS 25999-1:2006****: Business continuity management;*
- ***ISO 27001:2005****: Information technology -- Security techniques -- Information security management systems - Requirements;*
- ***ISO 28000:2007****: Specification for security management systems for the supply chain;*
- ***ISO 28001:2007****: Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance;*
- ***ISO 28002:2011****: Security management systems for the supply chain -- Development of resilience in the supply chain - Requirements with guidance for use;*
- ***ISO 28004:2007****: Security management systems for the supply chain - Guidelines for the implementation of ISO 28000;*

- ***ISO 31000:2011****: Risk management - Principles and guidelines;*
- ***ISO/IEC 31010:2009****: Risk management - Risk assessment techniques;*
- ***ANSI/ASIS SPC.1-2009:*** *Organizational Resilience: Security, Preparedness, and Continuity Management Systems - Requirements with guidance for use;*
- ***ANSI/ASIS SPC.4-2012:*** *Maturity Model for the Phased Implementation of the Organizational Resilience Management System;*
- ***OHSAS 18001: 2007:*** *Occupational health and safety management;*
- **Guide 73:2010**: Risk management: Vocabulary; and
- **PD 25888:2011**: Published Document: Business continuity management - Guidance on organisation recovery following disruptive incidents.

Management systems are about creating improvement. The *ANSI/ASIS SPC.1-2009 - Organizational Resilience: Security, Preparedness, and Continuity Management Systems - Requirements with guidance for use,* formed the base of the research along with the initial Maturity Model document which was developed by Dr Siegel. The initial Maturity Model has now been superseded by *ANSI/ASIS SPC.4-2012: Maturity Model for the Phased Implementation of the Organizational Resilience Management System.* This document was published in April 2012. Both of these standards are described more fully later in this research report.

Chaos would ensue if there was no standard set whatsoever in so many of the things in everyday life that are taken for granted. These include technologies, goods and services. ISO lists the following examples:

- Standardisation of screw threads helps to keep chairs, children's bicycles and aircraft together and solves the **repair and maintenance** problems caused by a lack of standardisation that was once a major headache for manufacturers and product users worldwide.

- Standards establish an international consensus on **terminology,** and make technology transfer easier and safer. They are therefore an important stage in the advancement of new technologies and dissemination of innovation.

- Without the standardised **dimensions** of freight containers, international trade would be slower and more expensive.

- Life would be more complicated without the Standardisation of **telephone and banking cards**.

- A lack of Standardisation may even affect the **quality of life** itself: for **the disabled**, for example, when they are barred access to consumer products, public transport and buildings because the dimensions of wheel-chairs and entrances are not standardised.

- **Standardised symbols** provide danger warnings and information across linguistic frontiers.

- Consensus on grades of various materials gives a **common reference** for suppliers and clients in business dealings.

- Agreement on a sufficient number of variations of a product to meet most current applications allows **economies of scale** with **cost benefits** for both producers and consumers. An example is the Standardisation of paper sizes.

- Standardisation of **performance or safety requirements** of diverse equipment makes sure that users' needs are met while allowing individual manufacturers the freedom to design their own solution on how to meet those needs.

- Standardised **computer protocols** allow products from different vendors to ‘talk’ to each other.

- Standardised **documents** (and identifying label pictures/posters on packaged goods for instance) speed up the transit of goods, or identify sensitive or dangerous cargoes that may be handled by people speaking different languages.

- Standardisation of connections and interfaces of all types ensures the **compatibility** of equipment of diverse origins and the **inter-operability** of different technologies.

- Agreement on **test methods** allows meaningful comparisons of products, or plays an important part in **controlling pollution** - whether by noise, vibration or emissions.

- Safety standards for machinery **protect everybody** whether at work, at play, at sea... and even, for example, at the dentist.

- Without the international agreement contained in ISO standards on **metric quantities and units**, shopping and trade would be haphazard, science would be unscientific and technological development would be handicapped (ISO, Nd(c)).

When products, systems, machinery and devices work well and safely, it is often because they meet standards and the organisation responsible for many thousands of the standards which benefit the world is the International Organisation for Standardisation (ISO). When standards are absent, it is soon noticed and their absence has an impact on all spheres of life.

To gain experience in the field of Standards, the researcher has served on a number of committees both locally and internationally. The development of Standards through the South African Bureau of Standards (SABS) for the security environment is driven through the Technical Committee, TC 179, and for Emergency Planning and Disaster Recovery TC 223. SABS is also a member of the international TC223 committee, Working Group 4. The researcher served on the technical and advisory committee of *ANSI/ASIS SPC.4-2012: Maturity Model for the Phased Implementation of the Organizational Resilience Management System.*

3.2 TYPES OF STANDARDS

Standards are divided into two different types. For the purposes of this research only '*International Standards'* and '*National Standards'* will be discussed.

3.2.1 International standards

International standards are developed by international standards organisations. International standards are available for consideration and use, worldwide. The most prominent organisation is the International Organisation for Standardisation (ISO).

ISO is the world's largest developer and publisher of international standards. ISO was established in 1946 when delegates from 25 countries met in London and decided to create a new international organisation. The objective was to facilitate the international coordination and unification of industrial standards. The new organisation, ISO, officially began operations on 23 February 1947, in Geneva, Switzerland. ISO is a network of the national standards institutes of 163 countries, one member per country, with a central secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organisation that forms a bridge between the public and private sectors. Member organisations are part of governmental structures of their countries, or are mandated by their government. There are also other members from the private sector, having been set up by partnerships with industry associations. Such an example in South Africa is the gaming industry where the implementation of technology is tested by the SABS before it is approved for implementation in casinos or other gaming venues by the National Gaming Board.

ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society. Because "International Organisation for Standardisation" would have different acronyms in different languages ("IOS" in English, "OIN" in French for *Organisation internationale de normalisation*), its founders decided to give it a short, all-purpose name. They chose "ISO", derived from the Greek *isos*, meaning "equal". Whatever the country, whatever the language, the short form of the organisation's name is always ISO (ISO, Nd(d)).

ISO has developed over 18 000 International Standards on a variety of subjects and some 1100 new ISO standards are published every year (ISO, Nd(e)).

3.2.2 National standards

International standards may be used either by direct application or by a process of modifying an international standard to suit local conditions. The adoption of

international standards results in the creation of equivalent, national standards that are substantially the same as international standards in technical content, but may have (i) editorial differences as to appearance, use of symbols and measurement units, substitution of a point for a comma as the decimal marker, and (ii) differences resulting from conflicts in governmental regulations or industry-specific requirements caused by fundamental climatic, geographical, technological, or infrastructural factors, or the stringency of safety requirements that a given standard authority considers appropriate (ISO, Nd(f)).

3.3 ROLE OF STANDARDS

Standards are important, as they make a positive contribution to most aspects of daily living. Standards ensure desirable characteristics of products and services such as quality, environmental friendliness, safety, reliability, efficiency and inter-changeability at an economical cost.

When products and services meet user expectations, it is normally taken for granted and the user is unaware of the role that standards would have played in the design and manufacture. However, when standards are absent, it is soon noticed. The user soon notices when products turn out to be of poor quality, do not fit, are incompatible with equipment that is already in use and are unreliable or dangerous.

ISO states that standards:

- Make the development, manufacturing and supply of products and services more efficient, safer and cleaner;
- facilitate trade between countries and make it fairer;
- provide governments with a technical base for health, safety and environmental legislation, and conformity assessment;
- share technological advances and good management practice;
- disseminate innovation;
- safeguard consumers, and users in general, of products and services; and
- make life simpler by providing solutions to common problems *(*ISO, Nd(g)).

ISO standards provide technological, economic and societal benefits. The main beneficiaries of this standards system include businesses, innovators, customers, governments, trade officials, developing countries, customers, everyone and the planet. These beneficiaries include the following:

Businesses: The widespread adoption of International Standards means that suppliers can develop and offer products and services meeting specifications that have wide international acceptance in their sectors. Therefore, businesses using International Standards can compete on many more markets around the world.

Innovators of new technologies: International Standards on aspects such as compatibility, terminology and safety speed up the dissemination of innovations and their development into manufacturability and marketable products.

Customers: The worldwide compatibility of technology which is achieved when products and services are based on International Standards gives them a broad choice of offers. They also benefit from the effects of competition among suppliers.

Governments: International Standards provide the technological and scientific bases underpinning health, safety and environmental legislation.

Trade officials: International Standards create "a level playing field" for all competitors on those markets. The existence of divergent national or regional standards can create technical barriers to trade. International Standards are the technical means by which political trade agreements can be put into practice.

Developing countries: International Standards that represent an international consensus on the state of the art are an important source of technological know-how. By defining the characteristics that products and services will be expected to meet on export markets, International Standards give developing countries a basis for making the right decisions when investing their scarce resources and thus avoid squandering them.

Consumers: Conformity of products and services to International Standards provides assurance about their quality, safety and reliability.

Everyone: International Standards contribute to the quality of life in general by ensuring that the transport, machinery and tools we use are safe.

The planet we inhabit: International Standards on air, water and soil quality, on emissions of gases, radiation and environmental aspects of products can contribute to efforts to preserve the environment (ISO, Nd(h)).

3.4 THE INTERNATIONAL ORGANISATION FOR STANDARDISATION (ISO) SYSTEM

The following section's information is based on the researcher's own personal experience gained from serving on various SABS TCs and ISO standards setting committees from 2006 to 2012.

The ISO system is viewed as a democratic system. Every full member of ISO has the right to take part in the development of any standard which it judges to be important to its country's economy. No matter what the size or strength of that economy, each participating member in ISO has one vote. Each country is on an equal footing to influence the direction of ISO's work at the strategic level, as well as the technical content of its individual standards (ISO, Nd(i)).

ISO standards are voluntary. As a non-governmental Organisation, ISO has no legal authority to enforce the implementation of its standards. ISO does not regulate or legislate. However, countries may decide to adopt ISO standards – mainly those concerned with health, safety or the environment – as regulations or refer to them in legislation, for which they provide the technical basis (ISO, Nd(j)).

In addition, although ISO standards are voluntary, they may become a market requirement, as has happened in the case of ISO 9001 quality management systems, or of dimensions of freight containers and bank cards.

ISO only develops standards for which there is a market requirement. The work is mainly carried out by experts from the industrial, technical and business sectors which have asked for the standards and which subsequently put them to use.

ISO standards are based on international consensus among the experts in the field. Consensus, like technology, evolves and ISO takes account both of evolving technology and of evolving interests by requiring a periodic review of its standards at least every five years to decide whether they should be maintained, updated or withdrawn. This process allows ISO to keep the standards as effective as possible.
ISO standards are technical agreements which provide the framework for compatible technology worldwide. They are designed to be globally relevant and thus useful everywhere in the world.

3.5 MEMBERSHIP OF THE ISO

ISO membership is open to one member per country. The members are normally the national standards institutes most representative of standardisation in their country. In South Africa it is the South African Bureau of Standards (SABS).

- Full members are known as **"member bodies"**. Each has one vote, whatever the size or strength of the economy of the country concerned.

- **"Correspondent members"** pay reduced membership fees. This category is entitled to participate in any policy or technical body as observers, with no voting rights.

- **"Subscriber members"** also pay reduced membership fees. These are institutes from countries with very small economies that nevertheless wish to maintain contact with international Standardisation.

Although individuals or enterprises are not eligible for membership, both have a range of opportunities for taking part in ISO's work:

- Individuals may be selected by national member institutes to serve as **experts on national delegations** participating in ISO technical committees.

- Individuals and enterprises may provide their input during the process of developing a national consensus for presentation by the delegation. This may be done through national **mirror committees** to the corresponding ISO technical committee.

- International organisations and associations, both non-governmental and representing industry sectors, can apply for **liaison** status to a technical committee. They do not vote, but can participate in the debates and the development of consensus (ISO, Nd(k)).

3.6 MANAGEMENT OF THE ISO SYSTEM

All strategic decisions are referred to the ISO members, who meet for an annual General Assembly. The proposals put to the members are developed by the ISO Council, drawn from the membership as a whole, which resembles the board of directors of a business organisation.

The ISO Council meets twice a year and its membership is rotated to ensure that it is representative of ISO's membership.

ISO's operations are managed by a Secretary-General, which is a permanent appointment resembling the chief executive of a business enterprise. The Secretary-General reports to the ISO Council, the latter being chaired by the President who is a prominent figure in Standardisation or in business, elected for two years.

The Secretary-General is based at ISO Central Secretariat in Geneva, Switzerland, with a small staff complement which provides administrative and technical support to the ISO members, coordinates the decentralized standards' development programme, and publishes the output (ISO, Nd(l)).

3.7 FINANCING OF THE ISO SYSTEM

ISO's national members pay subscriptions that meet the operational cost of ISO's Central Secretariat. The subscription paid by each member is in proportion to the country's Gross National Income and trade figures. Another source of revenue is the sale of standards.

The operations of ISO Central Secretariat represent only about one fifth of the cost of the system's operation. The main costs are borne by the member bodies that manage the specific standards development projects and the business organisations that provide experts to participate in the technical work. These organisations are, in effect, subsidizing the technical work by paying the travel costs of the experts and allowing them time to work on their ISO assignments (ISO, Nd(m)).

3.8 ISO DECISION PROCESS TO DEVELOP A STANDARD

A new standard’s development is launched by ISO in response to the sectors that express a clearly established need for them. An industry or business sector communicates its requirement for a standard to one of ISO's national members. The latter then proposes the new work item to ISO as a whole. If accepted, the work item is assigned to an existing technical committee. Proposals may also be made to set up technical committees to cover new scopes of activity.

At the end of 2010, there were 3 274 technical bodies in the ISO system, including 214 ISO technical committees (ISO, Nd(n)).

The focus of the technical committees is specialised and specific. In addition, ISO has three general policy development committees that provide strategic guidance for the standards' development work on cross-sector aspects. These committees ensure that the specific technical work is aligned with broader market and stakeholder group interests. They are:

- CASCO (conformity assessment)
- COPOLCO(consumer policy), and
- DEVCO (developing country matters)

3.9 TECHNICAL COMMITTEES

ISO standards are developed by experts from the sectors which have asked for them. ISO standards are developed by technical committees comprising experts from the industrial, technical and business sectors which have asked for the standards, and which subsequently put them to use. These experts may be joined by representatives of government agencies, testing laboratories, consumer associations, non-governmental organisations and academic circles (ISO, Nd(o)).

The experts participate as national delegations, chosen by the ISO national member institute for the country concerned. These delegations are required to represent not just the views of the organisations in which their participating experts work, but of other stakeholders too. According to ISO rules, the member institute is expected to take account of the views of the range of parties interested in the standard under development. This enables them to present a consolidated, national consensus position to the technical committee (ISO, Nd(p)).

3.10 THE STANDARDS DEVELOPMENT PROCESS

The national delegations of experts of a technical committee meet to discuss, debate and argue until they reach consensus on a draft agreement. This is circulated as a Draft International Standard (DIS) to ISO's membership as a whole for comment and balloting.

Many members have public review procedures for making draft standards known and available to interested parties and to the general public. The ISO members then take account of any feedback they receive in formulating their position on the draft standard. If the voting is in favour, the document, with eventual modifications, is circulated to the ISO members as a Final Draft International Standard (FDIS). If that vote is positive, the document is then published as an International Standard (ISO, Nd(q)).

Every working day of the year, an average of eight ISO meetings take place somewhere in the world. In between meetings, the experts continue the standards' development work by correspondence. Increasingly, their contacts are made by electronic means and some ISO technical bodies have already gone over entirely to

working electronically, which speeds up the development of standards and cuts travel costs (ISO, Nd(r).)

3.11 ISO'S INTERNATIONAL PARTNERS

ISO collaborates with its partners in international Standardisation, the International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU). The three organisations, all based in Geneva, Switzerland, have formed the World Standards Cooperation (WSC) to act as a strategic focus for collaboration and the promotion of international Standardisation.

ISO has a close relationship with the World Trade Organisation (WTO) which particularly appreciates the contribution of ISO's standards to reducing technical barriers to trade. ISO collaborates with the United Nations (UN) Organisation and its specialized agencies and commissions, particularly those involved in the harmonization of regulations and public policies, such as:

- CODEX Alimentarius, on food safety measurement, management and traceability;
- UN Economic Commission for Europe (UN/ECE), on the safety of motor vehicles and the transportation of dangerous goods;
- World Health Organisation (WHO), on health technologies;
- International Maritime Organisation (IMO), on transport security; and
- World Tourism Organisation (UNWTO), on the quality of services related to tourism.

In addition, ISO cooperates with UN Organisations that provide assistance and support to developing countries, such as the United Nations Conference on Trade and Development (UNCTAD), the United Nations Industrial Development Organisation (UNIDO) and the International Trade Centre (ITC).

ISO's technical committees have formal liaison relations with over 600 international and regional organisations. ISO has reinforced its links, too, with international organisations representing different groups of stakeholders, including:

- World Economic Forum (WEF);
- Consumers International (CI);
- World Business Council for Sustainable Development (WBCSD), and
- International Federation of Standards Users (IFAN).

ISO also collaborates regularly with the major international organisations for metrology, quality and conformity assessment (ISO, Nd(s)).

3.12 ISO'S REGIONAL PARTNERS

Many of ISO's members also belong to regional Standardisation Organisations. ISO has recognised regional standards organisations representing Africa, the Arab countries, the area covered by the Commonwealth of Independent States, Europe, Latin America, the Pacific area, and the South-East Asia nations. The regional bodies, listed below, commit themselves to adopt ISO standards as the national standards of their members.

- African Regional Organisation for Standardisation (ARSO)
- Arab Industrial Development and Mining Organisation (AIDMO)
- European Committee for Standardisation (CEN)
- Pan American Standards Commission (COPANT)
- Euro Asian Council for Standardisation, Metrology and Certification (EASC)
- Pacific Area Standards Congress (PASC)
- ASEAN Consultative Committee for Standards and Quality (ACCSQ)

3.13 STANDARDS DEVELOPMENT PRINCIPLES

ISO standards are developed according to the following principles.

Consensus: The views of all interests are taken into account: manufacturers, vendors and users, consumer groups, testing laboratories, governments, engineering professions and research organisations.

Industry: Global solutions to satisfy industries and customers worldwide.

Voluntary: International Standardisation is market driven and therefore based on voluntary involvement of all interests in the market-place.

There are three main phases in the ISO standards development process as follows:

- The need for a standard is usually expressed by an industry sector, which communicates this need to a national member body. The latter proposes the new work item to ISO as a whole. Once the need for an International Standard has been recognized and formally agreed, the first phase involves definition of the technical scope of the future standard. This phase is usually carried out in working groups which comprise technical experts from countries interested in the subject matter.

- Once agreement has been reached on which technical aspects are to be covered in the standard, a second phase is entered during which countries negotiate the detailed specifications within the standard. This is the consensus-building phase.

- The final phase comprises the formal approval of the resulting draft International Standard (the acceptance criteria stipulate approval by two-thirds of the ISO members that have participated actively in the standards development process, and approval by 75% of all members that vote), following which the agreed text is published as an ISO International Standard.

It is also possible to publish interim documents at different stages in the Standardisation process (ISO, Nd(t)).

Most standards require periodic revision. Several factors combine to render a standard out of date: technological evolution, new methods and materials, new quality and safety requirements. To take account of these factors, ISO has established the general rule that all ISO standards should be reviewed at intervals of not more than five years. On occasion, it is necessary to revise a standard earlier.

To date, ISO's work has resulted in over 16 000 International Standards, representing more than 620 000 pages in English and French (terminology is often provided in other languages as well).

ISO maintains a list of all standards in the ISO Catalogue which can be purchased from National Standards Organisations or from the ISO web-store (ISO, Nd(u)).

3.14 STAGES OF DEVELOPMENT OF INTERNATIONAL STANDARDS

An International Standard is the result of an agreement between the member bodies of ISO. It may be used as such, or may be implemented through incorporation in national standards of different countries.

International Standards are developed by ISO technical committees (TC) and subcommittees (SC) by a six-step process:

Stage 1: Proposal stage;
Stage 2: Preparatory stage;
Stage 3: Committee stage;
Stage 4: Enquiry stage;
Stage 5: Approval stage; and
Stage 6: Publication stage.

If a document with a certain degree of maturity is available at the start of a Standardisation project, for example a standard developed by another organisation, it is possible to omit certain stages. In the so-called "Fast-track procedure", a document is submitted directly for approval as a Draft International Standard (DIS) to the ISO member bodies (stage 4) or, if the document has been developed by an international standardizing body recognized by the ISO Council, as a Final Draft International Standard (FDIS, stage 5), without passing through the previous stages.
The following is a summary of each of the six stages:

Stage 1: Proposal stage

The first step in the development of an International Standard is to confirm that a particular International Standard is needed. A ‘new work item proposal’ (NP) is

submitted for vote by the members of the relevant TC or SC to determine the inclusion of the work item in the programme of work.

The proposal is accepted if a majority of the P-members of the TC/SC votes in favour and if at least five P-members declare their commitment to participate actively in the project. At this stage a project leader responsible for the work item is normally appointed.

Stage 2: Preparatory stage

Usually, a working group of experts, the chairman (convener) of which is the project leader, is set up by the TC/SC for the preparation of a working draft. Successive working drafts may be considered until the working group is satisfied that it has developed the best technical solution to the problem being addressed. At this stage, the draft is forwarded to the working group's parent committee for the consensus-building phase.

Stage 3: Committee stage

As soon as a first committee draft is available, it is registered by the ISO Central Secretariat. It is distributed for comment and, if required, voting, by the P-members of the TC/SC. Successive committee drafts may be considered until consensus is reached on the technical content. Once consensus has been attained, the text is finalized for submission as a draft International Standard (DIS).

Stage 4: Enquiry stage

The Draft International Standard (DIS) is circulated to all ISO member bodies by the ISO Central Secretariat for voting and comment within a period of five months. It is approved for submission as a final draft International Standard (FDIS) if a two-thirds majority of the P-members of the TC/SC are in favour and not more than one-quarter of the total number of votes cast are negative. If the approval criteria are not met, the text is returned to the originating TC/SC for further study and a revised document will again be circulated for voting and comment as a draft International Standard.

Stage 5: Approval stage

The final draft International Standard (FDIS) is circulated to all ISO member bodies by the ISO Central Secretariat for a final Yes/No vote within a period of two months. If technical comments are received during this period, they are no longer considered at this stage, but registered for consideration during a future revision of the International Standard. The text is approved as an International Standard if a two-thirds majority of the P-members of the TC/SC is in favour and not more than one-quarter of the total number of votes cast are negative. If these approval criteria are not met, the standard is referred back to the originating TC/SC for reconsideration in light of the technical reasons submitted in support of the negative votes received.

Stage 6: Publication stage

Once a final draft International Standard has been approved, only minor editorial changes, if and where necessary, are introduced into the final text. The final text is sent to the ISO Central Secretariat which publishes the International Standard (ISO, Nd(v)).

3.15 REVIEW OF INTERNATIONAL STANDARDS (CONFIRMATION, REVISION, WITHDRAWAL)

All International Standards are reviewed at the least three years after publication and every five years after the first review by all the ISO member bodies. A majority of the P-members of the TC/SC decides whether an International Standard should be confirmed, revised or withdrawn.

3.16 STAKEHOLDERS IN INTERNATIONAL STANDARDISATION

Stakeholders in international Standardisation comprise all those groups who have an interest in international Standardisation because they are affected by it and wish therefore to contribute to the process of the development of International Standards. Stakeholders participate in the technical work of ISO through national delegations appointed by the member bodies of ISO or, if they are organized in international or broadly-based organisations, through liaison organisations. National delegations are normally composed of a mix of the stakeholder groups listed below and represent national positions which have been consolidated at the national level prior to the participation of delegations at ISO meetings (ISO, Nd(w).)

The following main groups of stakeholders can be discerned:

Industry and industry/trade associations: This stakeholder group comprises manufacturers from all industry sectors, trading companies, retailers, importers and exporters and any associations through which these stakeholders may be represented. This group also includes industry associations representing small and medium enterprises.

Science and academia: This group comprises researchers from universities and other types of research institutions, laboratory staff, etc.

Consumers and consumer associations: Consumers are normally organized within consumer associations at national, regional or international level.

Governments and regulators: National governments and regulators at national or regional level are another important stakeholder group providing the link between legal and technical aspects which influence the development of standards.

Societal and other interests: There are additional interests addressing societal, environmental and other issues which are often represented by non-governmental Organisations (NGOs).

3.17 ISO DELIVERABLES

ISO has developed a schematic representation of the different types of available deliverables. These are:

- ISO Standard;
- ISO/PAS: Publicly Available Specification ;
- ISO/TS: Technical Specification;
- ISO/TR: Technical Report;
- IWA: International Workshop Agreement; and
- ISO Guide.

While due process remains a fundamental concept to all of ISO's activities, it is believed that the balance of procedures and deliverables demonstrates ISO's willingness to be flexible and responsive to international requirements for technical standards.

3.18 ISO GUIDES

Guides provide guidance to technical committees for the preparation of standards, often on broad fields or topics. Guides used in this research were ISO Guides 72 and 73. Guide 72 gives guidance as to how standard should be developed and Guide 73 gives information about the vocabulary for risk management.

3.18.1 The Process

Guides are prepared by Policy Development Committees (PDCs, such as CASCO or COPOLCO), or by committees or groups established by the ISO Technical Management Board (TMB) and operating under the TMB (e.g. REMCO). A number of Guides are jointly developed between ISO and IEC and then published as ISO/IEC Guides.

After consensus has been obtained in the group preparing the Guide, the draft is disseminated to all ISO member bodies for a four-month enquiry vote as a DIS. A draft Guide is approved if not more than 1/4 of the votes cast by the ISO member bodies are negative. In the case of ISO/IEC Guides, the acceptance criterion has to be met in both organisations independently.

If the acceptance criteria are met, the Guide is published without being subject to an additional approval vote as an FDIS (ISO, Nd(x).)

In this research, the most applicable guides were Guides 72 and 73.

ISO Guide 72: 2001: Guidelines for the justification and development of management system standards

The justification and evaluation of new management system standards can be complex, especially when it comes to assessing market relevance. Guidelines on the methodology of developing and maintaining management system standards are

given in Guide 72. Important advice is also given to help ensure new management system standards are compatible and aligned with existing ISO or ISO/IEC management system standards (e.g. ISO 9000, ISO 14000, ISO 22000, ISO/IEC 27000 and ISO 28000 series). This guide is used by those who are involved with the development and interpretation of management standards.

ISO Guide 73: 2009: Risk management: Vocabulary

This guide provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk as referenced in ISO 31000: 2009.

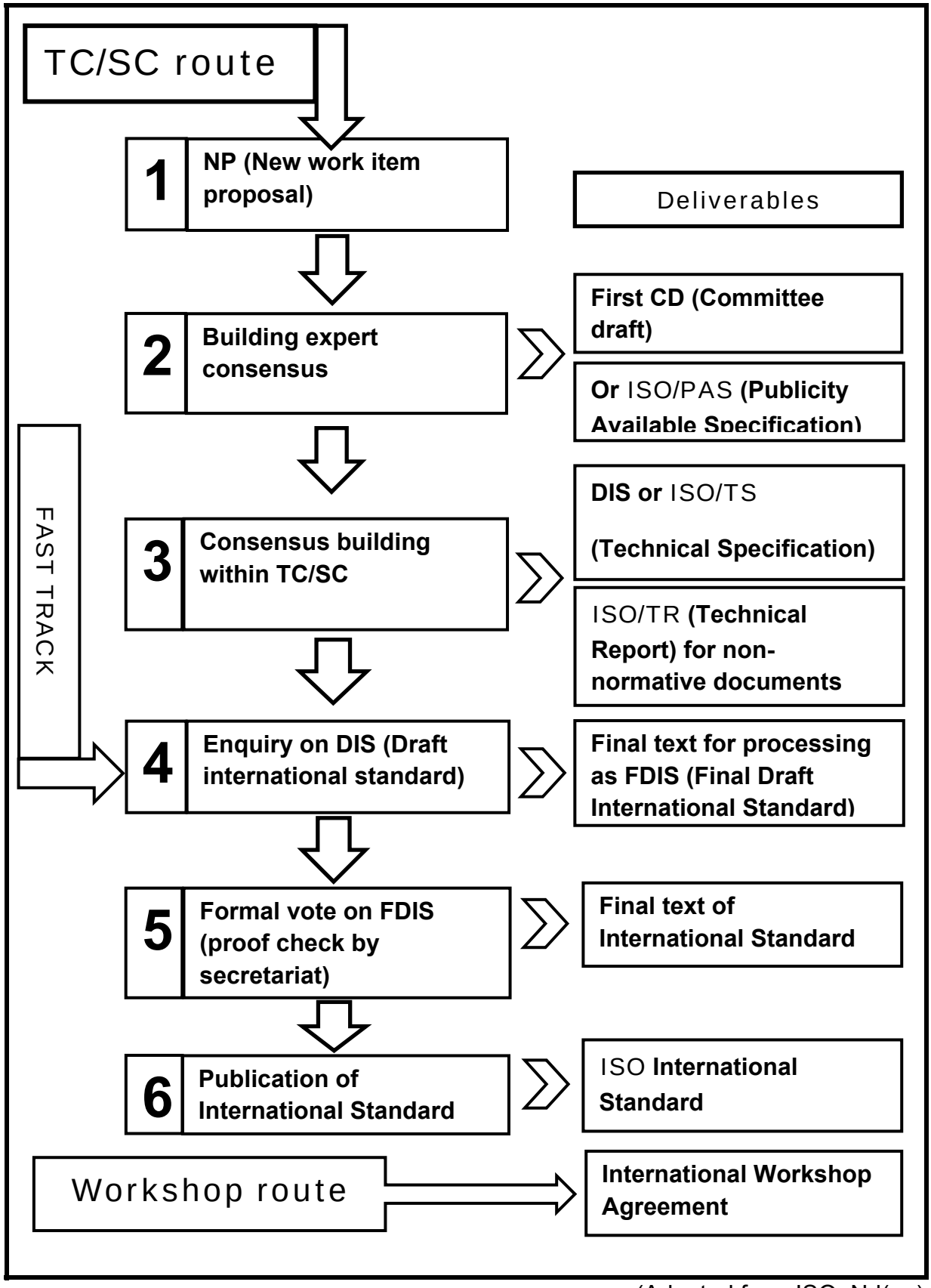
It is intended that this guide is used by people who are:

- engaged in managing risks;
- involved in activities of ISO and IEC; and
- developers of national or sector-specific standards, guides, procedures and codes of practice relating to the management of risk (ISO, Nd(y)).

(For an outline of the International Harmonized Stage Codes see Annexure D and for the Standards Development Stages and Processes see Annexure E) (ISO, Nd(z)).

The following is a schematic representation of the process for the development of a standard and the deliverables at each point:

Figure 1: Schematic representation of ISO deliverables



(Adapted from ISO, Nd(aa).

3.19 MANAGEMENT SYSTEMS STANDARDS

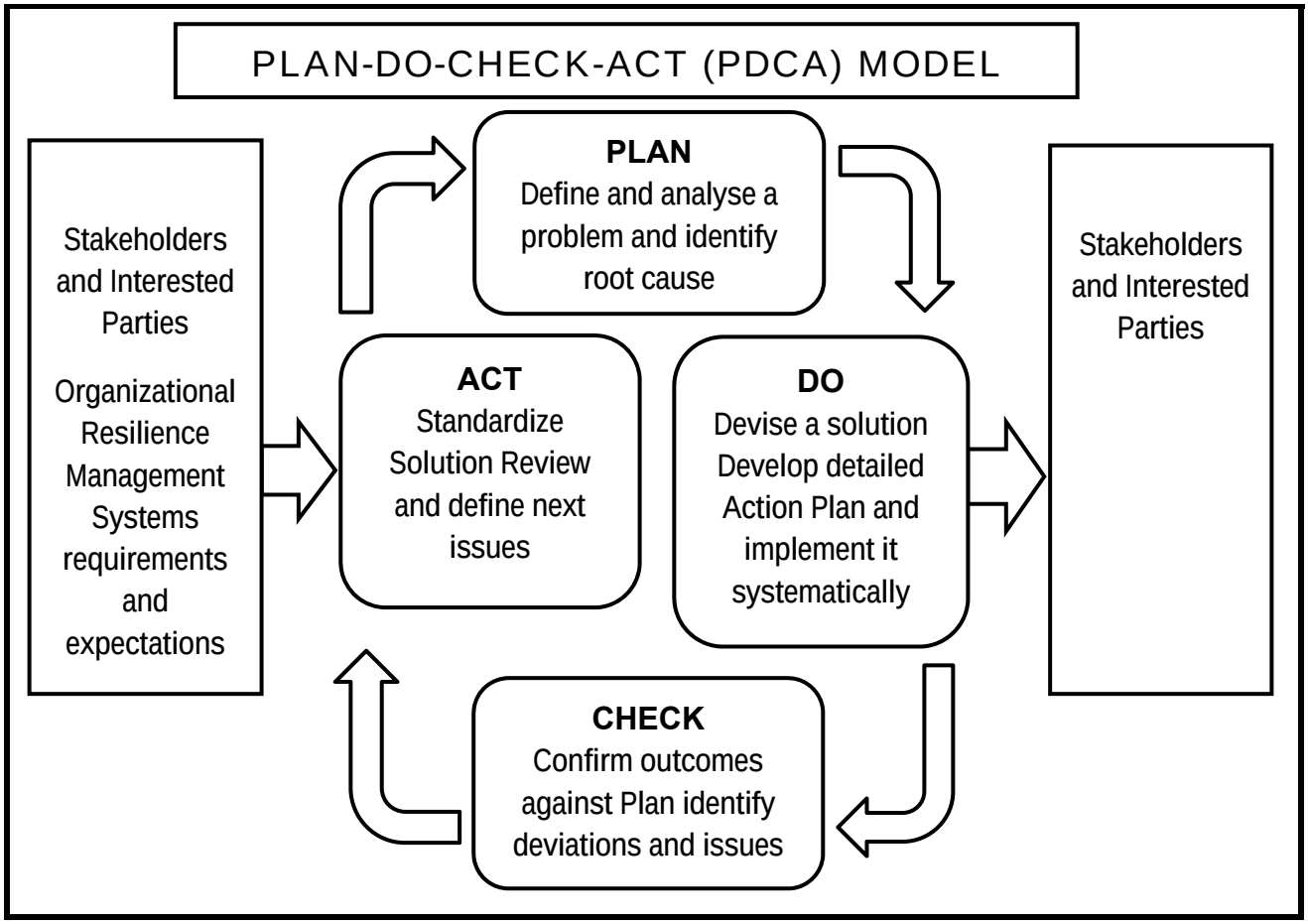
Management systems are found in all organisations. All the standards that apply to the security risk environment fall within the ambit of a management systems standard.

Management systems standards generally adopt a *process approach* for the establishment, implementation, operation, monitoring, reviewing, maintaining, and improving of an organisation's Organisational Resilience (OR) management system. An organisation needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process (ISO, Nd(u).)

The application of a system of processes within an organisation, together with the identification and interactions of these processes and their management, can be referred to as a “process approach”.

All of the more recently developed management systems standards are based on the "Plan-Do-Check-Act" (PDCA) model. The PDCA model is applied to give structure to the management systems system and its various processes. The PDCA model is sometimes referred to as the APCI (Assess-Protect-Confirm-Improve) Model. Figure 2 illustrates how a management system takes as input the management requirements and expectations of the interested parties and through the necessary actions and processes produces risk management outcomes that meet those requirements and expectations. Although this specific model was obtained from the ANSI ASIS SPC.1 Organisational Resilience Standard, 2009, it is the same in all the other management standards (ANSI/ASIS, 2009: ix).

Figure: 2: Plan-Do-Check-Act Model. ISO Management Systems



(ANSI/ASIS, 2009: ix).

Plan (Establish the management system)

Establish management system policy, objectives, processes, and procedures relevant to managing risk and improving security, incident preparedness, response, continuity, and recovery and to deliver results in accordance with an organisation's overall policies and objectives.

Do (Implement and operate the management system)

Implement and operate the management system policy, controls, processes, and procedures.

Check (Monitor and review the management system)

Assess and measure process performance against management system policy, objectives, and practical experience and report the results to management for review.

Act (Maintain and improve the management system)
Take corrective and preventive actions, based on the results of the internal management system audit and management review, to achieve continual improvement of the management system.

Compliance with this *Standard* can be verified by an auditing process that is compatible and consistent with the methodology of ISO 9001: 2008, ISO 14001: 2004, and/or ISO/IEC 27001: 2005, and the PDCA Model (ANSI/ASIS, 2009: ix).

3.20 DIFFERENCES BETWEEN ISO 9001 AND ISO 14001

The majority of ISO standards are very specific to a particular product, material, or process. However, ISO 9001 (quality) and ISO 14001 (environment) are "generic management system standards". "Generic" means that the same standard can be applied to any organisation, large or small, whatever its product or service, in any sector of activity, and whether it is a business enterprise, a public administration, or a government department. ISO 9001 contains a generic set of requirements for implementing a *quality management* system and ISO 14001 for an *environmental management* system. A comparative table of a number of other standards as well as ISO 9001 and ISO 14001 is attached to this research document (Annexure: F)

Many products require testing for conformity with specifications or compliance with safety, or other regulations before they can be put onto the market. "Conformity assessment" means checking that products, materials, services, systems, processes or people measure up to the specifications of a relevant standard or specification. ISO guides and standards for conformity assessment represent an international consensus on best practice. Their use contributes to the consistency of conformity assessment worldwide and so facilitates trade.

When the large majority of products or services in a particular business or industry sector conform to International Standards, a state of industry-wide Standardisation exists. The economic stakeholders concerned agree on specifications and criteria to be applied consistently in the classification of materials, in the manufacture and supply of products, in testing and analysis, in terminology and in the provision of services. In this way, International Standards provide a reference framework, or a

common technological language, between suppliers and their customers. This facilitates trade and the transfer of technology (ISO, Nd(ab)).

3.21 ISO CERTIFICATION

Within the world of ISO standards, you can opt for certification in order to demonstrate that you have met all of the standard's requirements. This is done so by using a Certification Body, an independent third-party that has proven qualified expertise to verify your claims. Such organisations are the British Accreditation Bureau (BAB), American National Standards Institute (ANSI) and the South African Bureau of Standards (SABS) as examples.

For many people *'certification'* and *'accreditation'* have the same meaning and sometimes people will interchange the words. However, when it comes to ISO standards, certification and accreditation actually mean two different things.

3.21.1 Accreditation

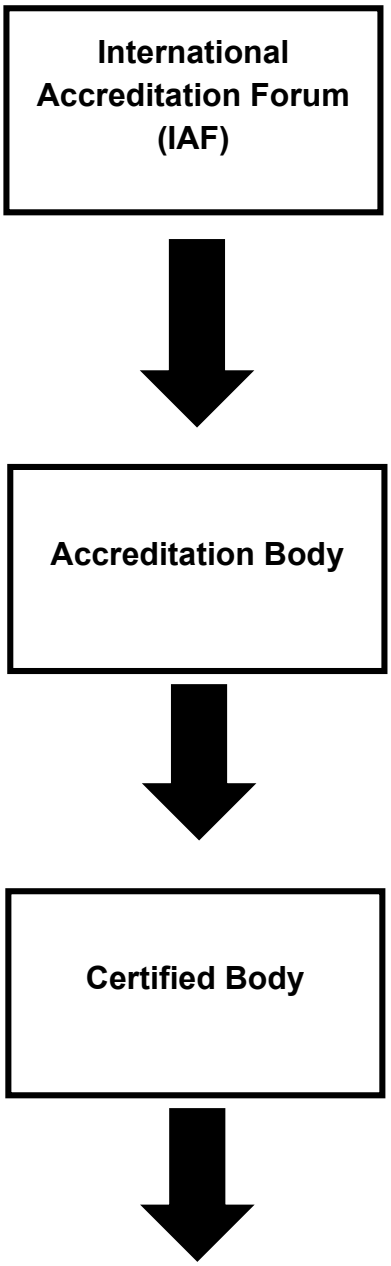
An organisation can become, for example, ISO 9001 ‘certified’, though technically it cannot become ISO 9001 'accredited'. This is because accreditation is intended for Certification Bodies. Certification Bodies become accredited so they too can demonstrate they meet a standard, ensuring they are fit to carry out their certification roles. Effectively, it is the certification of certification (British Accreditation Bureau, 2012: 1).

3.21.2 Accredited certification bodies

There is no international regulator for the certification body industry. However, accredited Certification Bodies meet standards that demonstrate their competence and impartiality, ensuring an organisation gets the most out of the certification process. Because of the benefits of accredited certification, many buyers insist on it (British Accreditation Bureau, 2012: 1).

3.21.3 Accreditation schematic

The tiers of accreditation and certification can, at first glance, appear confusing. Below is a schematic aimed at simplifying the structure, based on ISO's own model:



The International Accreditation Forum (IAF) is an association of Accreditation Bodies and other interested parties from around the world who work together to promote confidence and consistency in the accreditation and certification processes. A question mark tends to be raised over any Accreditation Body which is not a member of the IAF.

The accreditation process provides additional confidence that the certification nobody is competent and has the necessary integrity to issue a certificate. Accreditation is usually carried out by a National or Regional Accreditation Body, and their accreditation mark will be visible on their certificate.

A common way for a supplier to demonstrate conformity to an ISO standard is via third-party certification. A Certification Body (sometimes called a 'Registrar'), conducts and audit of the organisation to ensure they meet the requirements of the standard. If they have, a certificate of conformity is issued. Ongoing surveillance audits are required to ensure the organisation is still meeting the standard's requirements.

The organisation that holds accredited certification to an ISO standard will benefit from the audit process, thanks to the auditors having proven they are experts in their field. Accredited certification demonstrates to clients of the organisation that their credentials have been verified, providing confidence in the services or products supplied.

(British Assessment Bureau, 2012: 2).

3.22 CONCLUSION

The international standards system is complex and requires specialised knowledge of the environment to be able to effectively participate in the development of new standards and implementation guidelines.

The environment is also one where consensus plays a major role. Without consensus, many elements which are required in the development of a standard could result in lengthy delays in actually getting the standard accepted and published. To coordinate the various work groups (WG) during the various stages of development requires patience and diplomatic skills from all the participants to achieve the required end result.

When using standards as a risk management tool, a number of elements have to be considered. The same outcomes that the implementation of standards may have on a business, the same could be said for the risk management approach to improve security risk management. The combined and similar requirement elements in standards and risk management have to be considered during the whole process, on both sides of the scale.

Hopkin (2010: 5) states that not only does risk management require strategic decision making, but also that consideration should be given to the effective delivery of projects and programmes while also ensuring the security of routine operations of the organisation. The implementation of a resilience programme has to have measureable results and the way in which the organisation will benefit from such an implementation.

The implementation of standards to support any resilience program should thus have a clear set of desired outcomes/benefits. Each stage of the process must be properly evaluated. Attention should be given to the design, implementation and monitoring of the framework that supports the implementation (Hopkin 2010: 5).

CHAPTER 4
BACKGROUND TO ORGANISATIONAL RESILIENCE

4.1 INTRODUCTION

The first use of the term resilience is contested but can be attributed to either, ecology, physics or psychology. In ecology, it was introduced through Holling's (1973) seminal work *Resilience and Stability of Ecological Systems*. Holling described resilience as, '…a measure of persistence of systems and their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables' (Holling, 1973: 14). Stephenson, et al (2010: 35-36) write: "Resilience is a theoretical concept, metaphor. …a result of interactions between people and the environment, a property of a dynamic system, a measureable social and cultural construct ….and a paradigm."

The term resilience is used in a broad range of contexts including – individual, community, ecological and organisational resilience. As such, definitions of resilience have evolved in parallel with many different interpretations and understanding. In respect of organisational resilience, emerging ideas involve ways of assisting organisations to effectively manage adverse/disruptive situations and capture or realise any presenting opportunities. Resilience is not only having a sound risk management programme in place, but rather an organisational culture that is developed to ensure asset and resource protection, performance excellence and strategic leadership, organisational development, and a responsive and adaptive culture within an organisation to manage a magnitude of risks. Resilience is not a once-off program or management system that can be developed and then reviewed annually or as required. It is an approach that takes time to develop and is not a "one size fits all".

The Australian Government have prioritised their organisational resilience strategy, and see it as an issue of such importance, that they created a Resilience Expert Advisory Group (REAG) under the chairmanship of the Attorney General, The Hon. Robert McClelland, MP (Resilience Expert Advisory Group (REAG), 2011: 1).

All organisations face unique and specific risk landscapes. Resilience is seen as an outcome and forms a fundamental part of corporate governance. Sustainability focuses on the long term performance of an entity while the resilience is focused on and organisations ability to achieve intermediate objectives in uncertain and non-routine times (REAG, 2011: 5-6).

Organisational Resilience specialist researcher, Yossi Sheffi, (2007: 68) states that many corporations can recover quickly from disruptions of any magnitude if they knew what to expect and had developed some form of preparedness. He further states that the impact of two low probability disruptions should be taken into account. The first being the potential cascading effects from governmental agencies and other organisational institution's responses to the incident. The second would be the competitive advantage that the company has within the market where its competitiveness and ability to bounce back to business will be severely tested as will its ability to act in a resilient manner.

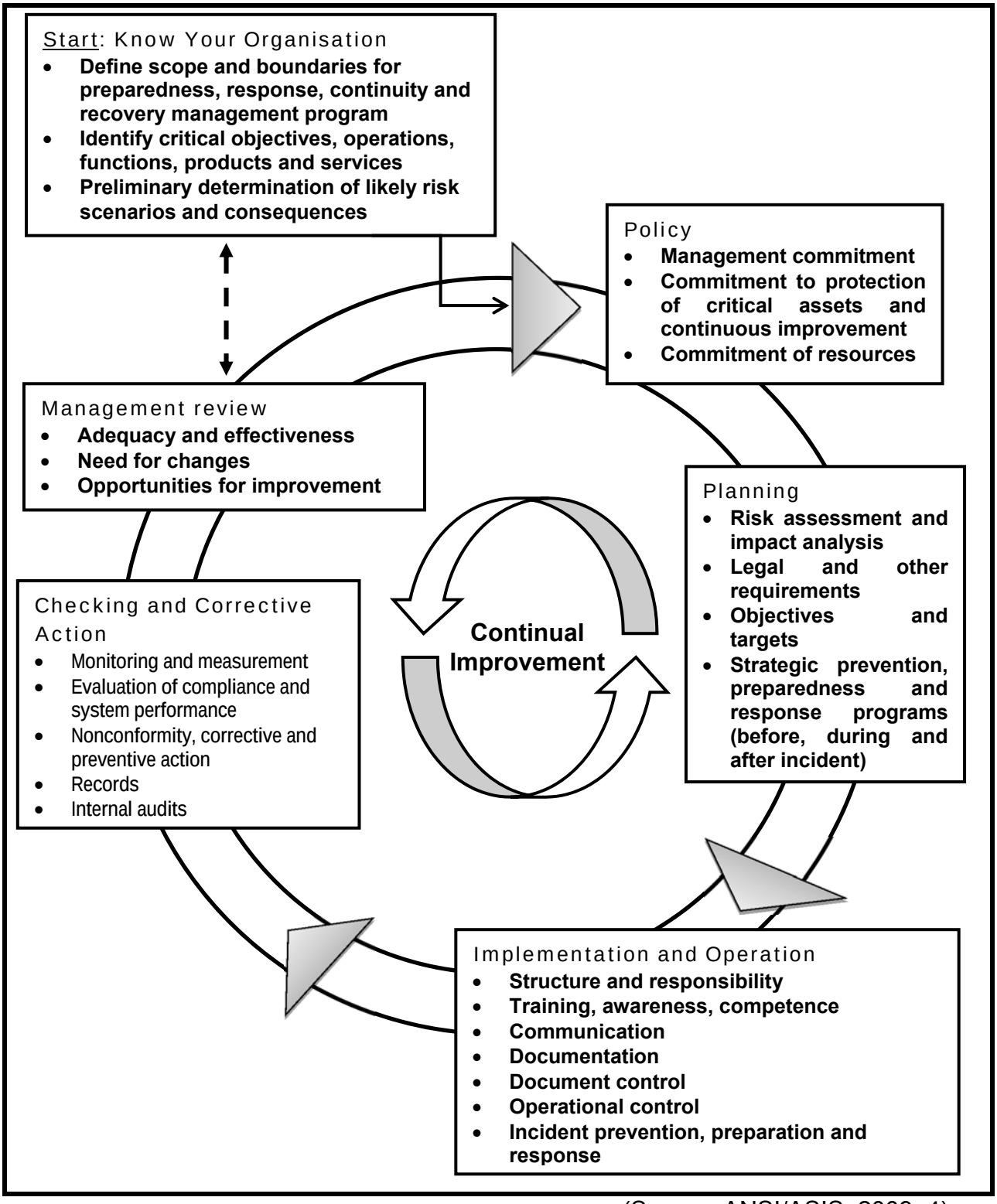
> The world is becoming more turbulent faster than organisations are becoming resilient. In a turbulent age, the only dependable advantage is a superior capacity for reinventing your business model before circumstances force you to (Hamel & Valikangas, 2003: 1)

The ANSI/ASIS SPC.1 Organisational Resilience Standard: 2009, defines **"Organisational Resilience Management"** as: "Systematic and coordinated activities and practices through which an organisation manages its operational risks, and the associated potential threats and impacts therein*"* (ANSI/ASIS, 2009: Annex D: D.38 & 47).

It further defines an **"Organisational Resilience Management Program"** as:

> Ongoing management and governance process supported by top management: resourced to ensure that the necessary steps are taken to identify the impact of potential losses; maintain viable recovery strategies and plans; and ensure continuity of functions/products/services through exercising, rehearsal, testing, maintenance and assurance" ((ANSI/ASIS, 2009: Annex D: D.39, 47).

Figure 3: Organisational Resilience Management System Flow Diagram



(Source: ANSI/ASIS, 2009: 4).

During a workshop arranged in 2007 by the Council on Competitiveness, Australia, Robert Oldfield presented a paper on Organisational Resilience. He specifically mentioned the aspects of managing turbulent environments in isolation. He commented on how risk managers maintain Risk Registers, security managers conduct threat and vulnerability assessments while business continuity managers established the impact on the business through a Business Impact Analysis (BIA) He stated that a resilient organisation recognises the synergies between these functions. Such an organisation also recognised that a risk is a risk no matter who identifies it.

Oldfield had stated at the workshop that “resilience is not a plan or a checklist” and then proceeded to summarise the main elements of a resilient organisation into the following headers:

Adaptive capacity: Recovery to an original state may not be the best option, and organisations need to be able to adapt to maintain competitive advantage.

Communications: Lack of communications has been a contributor to global disasters when those who had the information did not pass it on, or when those in authority did not act on it.

Interdependencies: Independent thinking is not suited to independent reality. Independent people who do not have the maturity to think and act independently may be good producers, but they will not be good leaders or team players.

Situational awareness: Awareness includes understanding risks and vulnerabilities, enabling quick detection of change and rapid response.

Leadership: The key elements include principle-centred leadership, non-hierarchal communications and empowerment to act.

Culture and values: Culture is about how principles are learned and translated in day-to-day behaviour. Values contribute to the culture and may include integrity, customer focus and results.

Enterprise-wide: All business units and functions contribute to organisational resilience.

Ownership: Resilience is not a word to describe only one of the tactical elements of security, risk or business continuity. It is the balanced integration of all of these (Oldfield, 2007: 1).

4.2 BENEFITS OF A RESILIENCE APPROACH

Many organisations do however rely solely on silo type structure to develop protection plans for their organisations. They also want to use these same silos in isolation to get their business back into operation once a disruptive incident has taken place. The main elements are:

4.2.1 Risk management;
4.2.2 Emergency planning;
4.2.3 Disaster management;
4.2.4 Business continuity;
4.2.5 Security risk management; and
4.2.6 Occupational health and safety.

Organisations with adaptive cultures, innovative thinkers and who have the inner strength are organisations that survive (Hamel & Valikangas, 2003: 5). Organisational resilience programmes do have an initial financial impact but if properly managed, can also be implemented through the re-channelling of existing resources into a more focussed programme.

Once a culture of resilience is implemented in an organisation's daily business operations, the benefits are quickly visible. Benefits include:

Leadership:

- More successful outcomes from strategic and operational planning
- Enhanced leadership capacity

Organisational performance:

- Reduced disruption costs, including insurance premiums due to reduced exposure to uninsured losses
- Faster return to pre-disruption profits after disruption
- Reduced need for regulation to meet community expectations
- Enhanced reputation with stakeholders (e.g. staff, community, regulators and clients)
- Increased staff morale, commitment and productivity
- Improved ability to attract quality staff
- Generation of reputational and sustainable advantage
- Increased market share

Change ready:

- Increased foresight of emerging external threats
- Enhanced ability to create innovative thinking
- Improved ability to use adversity for change and improvement (REAG, 2011: 9-10).

In this same research report by the REAG, the authors mention that “in practical terms, the focus of resilience is generally on protection, performance and adaptation”. They further state that the resilience maturity objectives of an organisation is to create value propositions for Boards and other governance bodies. A clear message must be sent to the organisation’s shareholders and stakeholders on how they plan to approach adverse events (Latour, 2001).

An organisation’s resilience objectives will normally reflect business direction, corporate culture, risk appetite and stakeholder expectations. Some of these events impacting on the various stages are summarised in the following table:

Table 1: Examples of events impacting on an organisation's resilience objectives

Decline	An organisation accepts that adversity may cause it to cease operating.	**Ericson and the Philips Albuquerque Fire** When Philips had a fire at its New Mexico electronics production plant, their customer, Ericsson, did not spring into action the moment the employees detected the disruption. Ericsson's employees lacked the urgency, mindfulness and passion to react quickly. Ericsson suffered production disruption and lost more than US$400 million. Ericsson's competitors grew their market share.
Survive	An organisation's resilience objective is to exist in a reduced form after adversity.	**1997 Fire at Bankstown City Council Offices** Bankstown City Council offices burnt down in July 1997. With good leadership and motivated staff, services were restored to the community quickly.
Bounce Back	An organisation's resilience objective is to regain pre-adversity position quickly and effectively.	**2008 Hurricane Katrina and Mississippi Power's Response** Following Hurricane Katrina, Mississippi Power grew from 1,200 staff to 10,000 in just a few days. A prior investment in developing mutual aid agreements with other energy infrastructure providers, extensive planning and training, strong supplier and regulatory relationships, exceptional leadership and empowered staff meant electricity supplies were restored to all customers in just 12 days. Mississippi Power received positive community recognition for its outstanding effort
Bounce Forward	An organisation's resilience objective is to improve aspects example of the	**Nokia and the Philips Albuquerque Fire** By comparison with Ericsson, when Philips had the fire in it New Mexico electronics production plant, their customer, Nokia, quickly escalated the

	organisation's functioning e.g. reputation, asset condition, future risk management,	issue, conducting situational risk assessments. Through extraordinary efforts and intensive collaboration with its suppliers. Nokia effectively managed the event and significantly increased its share of the mobile phone market **Wal-Mart and Hurricane Katrina** Wal-Mart was monitoring the formation of Hurricane Katrina prior to any public announcements by the US Weather Service. Staff were alerted and supply chains rearranged well before Hurricane Katrina reached the Mississippi Coast. Wal-Mart's response to restoration of customer services and support of impacted communities received national recognition. As a result of the success of the operation, Wal-Mart's brand reputation was significantly enhanced

(REAG, 2011: 11-12).

Johnson-Lenz and Johnson-Lenz (2009: 1-2) theorise that most companies live fast and die young. They quote from a study in 1983 by Royal Dutch/Shell that found only 40 corporations that were over 100 years old. In contrast, they found that one-third of the Fortune 500 companies from 1970 were, at that time, already gone. They then looked at what differentiates success and failure, resilience and collapse? The Royal Dutch/Shell study emphasised shared purpose and values, tolerance of new ideas, financial reserves, and situational awareness.

More recently, Ceridian Corporation collected best thinking and strategies to publish an executive briefing on Organisational Resilience. They highlighted the paradox that successful, resilient organisations are those that are able to respond to two conflicting imperatives:

- **managing for performance and growth**, which requires consistency, efficiency, eliminating waste, and maximizing short-term results

- **managing for adaptation**, which requires foresight, innovation, experimentation, and improvisation, with an eye on long-term benefits (Johnson-Lenz and Johnson-Lenz, 2009: 1-2).

Most organisations pay great attention to the first imperative but little to the second. Start-ups often excel at improvisation and innovation but flounder on the borders of consistent performance and efficiency. About half of all new companies fail during their first five years (Johnson-Lenz, 2009: 1-2).

Each mode requires a different skill set and organisational design. Moving quickly between them is a tricky dynamic balancing act. Disruptions can come from anywhere – from within, from competitors, infrastructure or supply chain crises, or from human or natural disasters. The financial crisis has riveted current attention, but it's just one of many disruptions organisations must cope with daily. Planning for disruption means shifting from "just-in-time" production and efficiency to "just-in-case" resilience (Johnson-Lenz and Johnson-Lenz, 2009: 1).

Johnson-Lenz and Johnson-Lenz (2009: 3) took from these two studies, and others, to develop what they called the '***six habits of highly resilient organisations'***. These six habits are listed below and then discussed individually thereafter:

1. Resilient organisations actively attend to their environments;
2. Resilient organisations prepare themselves and their employees for disruptions;
3. Resilient organisations build in flexibility;
4. Resilient organisations strengthen and extend their communications networks – internally and externally;
5. Resilient organisations encourage innovation and experimentation; and
6. Resilient organisations cultivate a culture with clearly shared purpose and values (Johnson-Lenz & Johnson-Lenz, 2009, 2-3).

1. Resilient organisations actively attend to their environments

Monitoring internal and external indicators of change is a means of identifying disruptions in advance. Resilient organisations seek out potentially disturbing information and test it against current assumptions and mental models. They work to

detect the unexpected so they can respond quickly enough to exploit opportunity or prevent irreversible damage. In short, they anticipate to being prepared.

2. Resilient organisations prepare themselves and their employees for disruptions.

Attentive preparations build a team that imagines possibilities and displays inventiveness in solving problems. Managers know how and when to allow employees to manage themselves for focused productivity as well as adaptive innovation. Resilient organisations cross-train employees in multiple skills and functions. They know that when people are under pressure, they tend to revert to their most habitual ways of responding.

After the 1993 World Trade Centre bombing, Morgan Stanley, the largest employer at the WTC, realised it was operating in a highly symbolic building and began emergency preparedness with detailed plans and drills. On 11 September 2001 it had three recovery sites at the ready where employees could congregate and continue business. They began evacuating about 2 700 employees one minute after the first plane hit, and their offices across 22 floors were almost empty when the second plane hit 15 minutes later. They lost only six people. According to their 2001 Annual Report, investments in redundant computing and communication technology made after the 1993 WTC bombing also played a significant role in this successful recovery (Morgan Stanley, 2001: 1).

3. Resilient organisations build in flexibility

Even while executing for lean and mean performance, resilient organisations build in cushions against disruptions. The most obvious approach is the development of redundant systems – backup capacity, larger inventories, higher staffing levels, financial reserves, and the like. But those are costly and not always efficient. Flexibility is a better approach.

Engaging suppliers and their networks in devising makeshift solutions to temporary disruptions is a flexibility strategy. So are policies that encourage flexibility in when and where work is done. Employees who are used to telework and virtual workspaces adapt more quickly and are more productive following a

crisis. In addition, research shows that flexible work practices contribute to greater employee resilience, productivity, and commitment, and to lower levels of stress.

In 1997, a fire at an Aisin factory (which manufactured the P-valve used in rear brakes to prevent skidding) in Japan destroyed most of the precision machine tools being used. Toyota Motor Corporation received 99% of its P-valves from Aisin. As a just-in-time manufacturer, Toyota had only a few days' valves in stock at its plants. While the fire was still burning, Toyota and Aisin immediately collaborated to make emergency requests of their networks of suppliers. Aisin helped other suppliers improvise different production techniques, providing them with detailed plans and technical support. Two days after the fire, the first valves came off the production line at other factory sites, and a week later, Toyota's vehicle production line was back to normal. Two months later, Aisin resumed production at pre-fire levels.

In more recent times, Toyota lost 30 percent of its stock value in the first month after the Japan Tsunami (6 April 2011) because they had not considered the 'sole supplier' status they had on many different and separate items they needed for production in their plants. The rival motor manufacturer, Nissan, did, and was able to restart their production by merely shifting their supply chain (Lowe, 2011: 15).

4. Resilient organisations strengthen and extend their communications networks: internally and externally.

A robust and redundant communications infrastructure holds up in a crisis. Social networks among employees at resilient organisations are rich, varied, and visible. People who have trust relationships and personal support systems at work and with friends and family are much more able to cope with stress and change.

Good connections and communications also apply to external relationships with suppliers and customers. A key is to recognize what is important to meet organisational goals and to listen to those with needed expertise and ideas wherever they are in the value web.

Resilient organisations use networked communications to distribute decision-making. As much as possible, they push decisions down to where they can be made most effectively and thus quickly. This in turn requires good access to information at all levels of the organisation.

After Hurricane Andrew devastated Florida in 1992, the state reassessed its preparedness and greatly expanded its planning to include stakeholders from every level of government, as well as organisations in the private sector, non-profits, and faith-based groups. These organisations came together to cooperate and collaborate, addressing the complex problems that none of them could solve by themselves. This Florida “mega-community” was prepared for Hurricane Katrina, unlike localities on the Gulf Coast. In fact, within hours of Katrina’s landfall, more than 3 700 of Florida’s first responders were deployed to affected areas.

5. Resilient organisations encourage innovation and experimentation.

In times of great uncertainty and unpredictability, the success and failure of small-scale experiments can help map a path to the future. Resilient organisations engage in market research, product development, and ongoing operations and service improvements. They invest in small experiments and product trials that carry low costs of failure.

United Parcel Services (UPS) tells its drivers to do whatever it takes to deliver packages on time. They encourage improvisation to solve all the small things that can go wrong every day. At the same time, they have clear rules and regulations, such as always putting their keys in the same place, closing truck doors the same way, making only right turns 90% of the time to save time and fuel, and so on. Those routines, combined with creative improvisation, allowed UPS to deliver packages the day after Hurricane Andrew struck, even to people temporarily living in their cars.

Resilient organisations foster a culture of continuous innovation and ingenuity to solve problems and adapt to challenges. A side benefit is that employees who believe they can influence events that affect their work and lives are more likely to be engaged, committed, and act in positive ways associated with resilience. Some organisations also have internal idea markets to surface new ideas and innovations.

6. Resilient organisations cultivate a culture with clearly shared purpose and values

When an organisation's sense of purpose is shared by its employees, suppliers and customers, those networks can provide flexibility to help it through a disruption. Engaged employees will seek out opportunities to try new approaches, find creative solutions, and achieve great results.

A University of Michigan study of major airlines in the aftermath of September 11 found that those whose market value rebounded shared two characteristics:

1. They maintained their commitments to employees; and
2. They had adequate financial reserves.

Others went bankrupt or out of business. Instead of layoffs or cancelling severance packages and employee benefits, the resilient ones did everything they could to preserve employee relationships and loyalty. Financial reserves and a strong sense of purpose and organisational values made that possible.

4.3 BUSINESS CONTINUITY OR RESILIENCE?

Simpson (Blog Business Continuity Professionals:, July 2011) raises the question asking if *organisational resilience* is just *business continuity* dressed up for the twenty-first century? It might look that way, but resilience goes further than simply making sure that critical business functions are available after a disruption or disaster.

One of the companies identified in the Royal Dutch/Shell study was Stora Enso, the world's oldest company. Founded as a copper mining company in 1288, the Swedish entity changed lines of business several times, but it has remained committed to its people, purpose and values. It survived the Black Plague, mine collapses and much more. Now it operates as the world's second largest forest products company (Johnson-Lenz and Johnson-Lenz, 2009: 4).

Simpson (2011), also raises the next question as to "why is a seven-hundred-year old company not well-known and celebrated as an exemplar of ***corporate***

resilience?" The recent events of corporate espionage and intrigue at *News of the World*, a newspaper owned by the Murdoch Group of companies, in the UK, prove that age (longevity in business) of an entity is not really an indicator of its current degree of resilience. In fact, this is further evidence to support the primary role that culture plays in establishing and sustaining organisational resilience. In the case of the *News of the World* it would appear that the widespread prevalence through their ranks of an unethical culture diminished their resilience, or perhaps just another case of arrogance and complacency from a market leader.

There appears to have been little value placed on the length of the period in business of the *News of the World* title by the News Limited Crisis Managers, the holding company. When the fallout hit the media headlines around the world, relentless pressure was placed on Rupert Murdoch, his family and his executive team at News of the World. The pressure was so intense that News Limited decided to scrap the acquisition of the BSkyB Television network. The pressure increased to such an extent that the 168 year-old newspaper simply became expendable and was summarily closed down by the holding company.

Habits and culture can work in both positive and negative ways. Simpson (2011) applied the 'Six Habits' to the situation that the *News of the World* had found them in, in the following manner:

Resilient organisations actively tend to their environment

- Success can make you overconfident, nobody can take you down.
- Simpson in his article actually suggests part of the problem as being "too little transparency. No moral compass."

Resilient organisations prepare themselves and their employees for disruptions

- Some organisations do not prepare their employees, but they do have plans
- Simpson, himself, has consulted to companies who have contingency plans to shut down a business unit in the event of a disaster, and found that these were not discussed internally with staff.

- The abandoning of the *News of the World* could possibly have been a pre-arranged contingency if things got too hot.

Resilient organisations build in flexibility

- Dumping the newspaper to protect the Sky TV acquisition shows that News Ltd can be flexible.
- The purpose is not the continuity of a single business unit or publication but the returns generated by the ultimate holding company.

Resilient organisations strengthen and extend their communications networks: Internally and externally

- Clearly they excelled in this category with contacts and links right into Scotland Yard (HQ of the London Metropolitan Police) and Number 10 Downing St (the UK Prime Minister's residence in London).

Resilient organisations encourage innovation and experimentation

- Get the story, the end justifies the means.
- Phone hacking is innovative – we need to be clear on the ethics of our innovations.

Resilient organisations cultivate a culture with clearly shares purpose and values

- It seems that this was shared, but it was the value of arrogance and the purpose was to get the 'scoop' at any cost (Simpson 2011).

Simpson (2011) concludes with his analysis of the reasons for the closure of the *News of the World* by stating that "culture is about the way we do things – it is driven by the attitude from the top… [and] [T]hat is why the culture of resilience has to start from the top level and filter down, it cannot be established from the middle or bottom". All of the above confirms that the question of leadership is most important in guiding any organisation and creating the functional channels to create a resilient organisation.

The number of examples that have been researched in this research indicate that even high level corporate executives have problems in understanding the concept of resilience and steps that need to be taken into consideration if an organisation is to develop and implement a successful organisational resilience programme. This very fact was observed during the period where the researcher and the team at Tsogo Sun Group had to get the message across to the executive management of the Group that implementing the Organisational Resilience Management Standard based on the Maturity Model would be a valuable programme. It's implementation would not only be valuable in the short-term but rather in the long term if they actually stood by the programme requirements, assisted in the roll-out and ongoing programme maintenance throughout the organisation.

4.4 RESILIENCE AND RISK

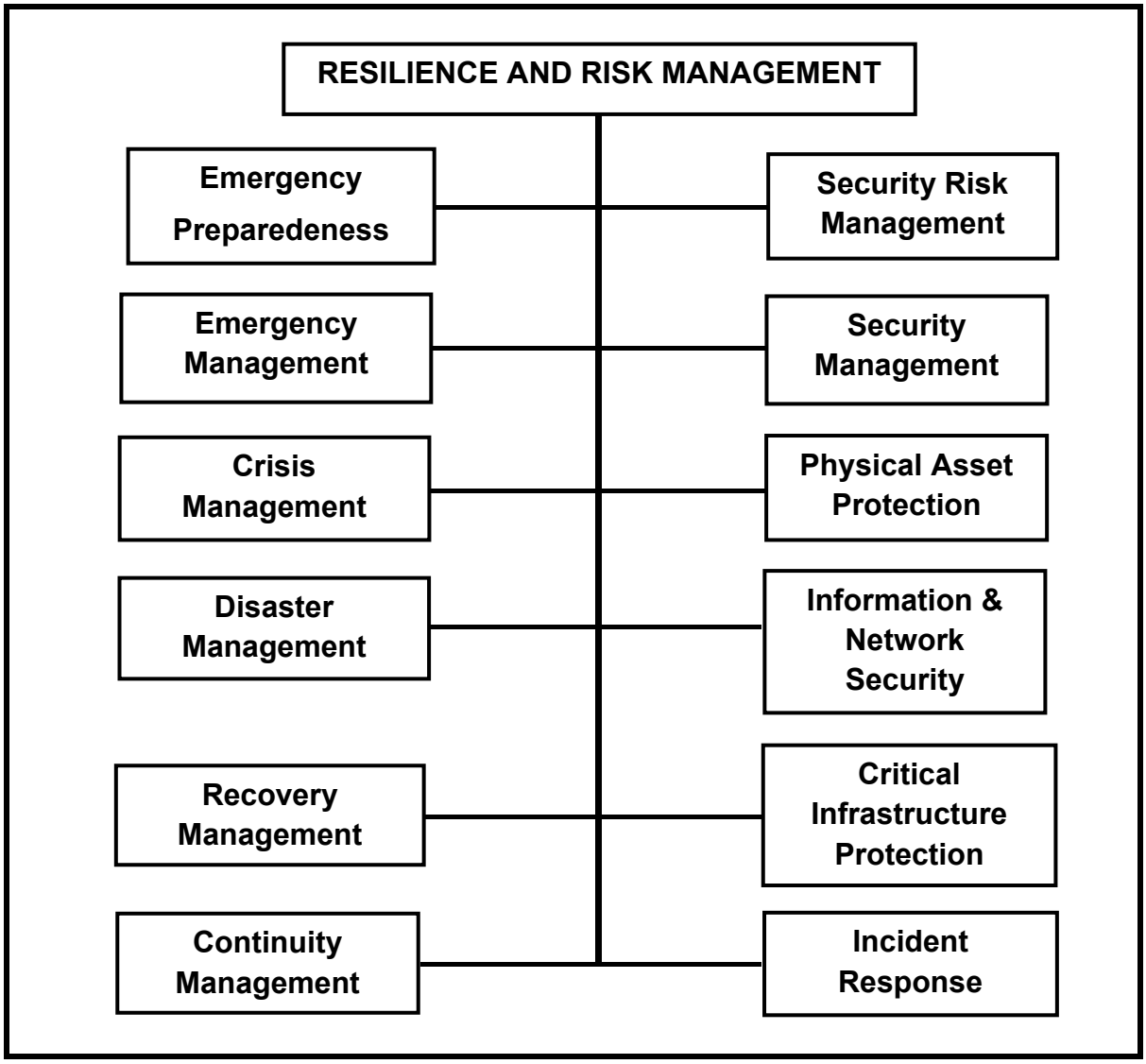
Resilience is very closely linked to the risk management process. These concepts drive major organisational policy and operational decisions. Neither of these two topics can thus be discussed in isolation although there is still a tendency to treat these two concepts individually.

Risks are elements in all spheres of life and business. In the business environment there are many risks and although these have been categorised in many forms over the years.

This research will only look at the risks as they would apply to the five main silos as previously mentioned in this chapter and the side elements that could form a sub-category of the main risk elements.

The following diagram forms the basis of the work done in this research regarding risk:

FIGURE 4: Elements of resilience and risk management



(Siegel & Siegel, 2009: Presentation).

Resilience is not a checklist of best practises. It seems that some of the best practices for risk management that are currently available, are still inadequate to deal with the challenges that organisations face. Efforts have been made over many risk management disciplines to aspire to a position where traumatic effects on businesses and people can be reduced to 'zero'. The objective of a resilient enterprise is to ensure that it is continuously re-inventing and forever adapting itself through compliance and situational changes so as to deal with emerging trends and opportunities. Risk management should be dynamic and not static. Dynamic businesses implementing proper risk management systems would be able to adapt

to changes very quickly since they are always in a ‘state of preparedness.’ Organisations and people would be able to deal with trauma more easily than an organisation that has no, or very little, planning in place. In a resilient business there is an air of excitement that stretches from the boardroom down to the people on the ground. The programme includes its suppliers, stakeholders as well as the local community.

Resilient businesses seek continuous change and have already conquered that sense of ‘denial’ and believe that it could never happen in their organisation. Resilience is not a formal ‘plan’. Executives are surprised when, due to an incident, the business has to deal with a traumatic event and there is no capacity to deal with it. Normally there is also no plan in place that could possibly have detected and ‘red flagged’ the early warnings timeously. When an incident does occur and they have to deal with the shock and dramatically changed circumstances (financial loss and business failure), they go into denial and start looking for scapegoats. This virtually guarantees that the work of renewal will be significantly delayed while they deal with the trauma of the shock resulting from an unexpected incident and try to understand why their “strategy” did not plan for such an occurrence (Sheffi, 2005: 26)

.

The researcher has observed that people battle to open their minds to new possibilities but rather go about comparing it to existing information or knowledge about a situation or based on such a major event as 9/11 (Terrorist attack on the World Trade Centre, New York, and other targets in the USA, 11 September, 2001). Having been in New York on 9/11 and having witnessed the fire and devastation, the researcher has subsequently read many accounts of people who were in the midst of the drama and how this impacted on them and the effected organisations. Some people have been able to deal with the impact that it has had on their lives but everyone will carry the scars of that day with them for the rest of their lives. The organised businesses that had done pre-planning were able to get back into business within days but a number of others were not resilient and had no proper plans and thus went out of business.

4.5 BENCHMARKING AND MEASURING ORGANISATIONAL RESILIENCE

Mitroff, Pauchant, Finney and Pearson (1989, 34) developed the following list of faulty assumptions and beliefs that were raised during their research by organisations to justify their lack of investment and action in creating a resilient organisation:

4.5.1 List of faulty organisational assumptions and beliefs

1. The fallacy ***of size***: our size will protect us.
2. The fallacy of ***protection/resource abundance***: another entity will come to our rescue or absorb our losses.
3. The fallacy of ***excellence***: excellent/well managed organisations do not have crises.
4. The fallacy of ***location/geography***: we don't have to worry about a crisis here.
5. The fallacy of ***immunity/limited vulnerability***: certain crises only happen to others.
6. The fallacy of ***misplaced social responsibility***: crisis management is someone else's responsibility.
7. The fallacy of ***unpredictability***: it's not possible to prepare for the crisis because they are unpredictable.
8. The fallacy of ***cost***: crisis management is not warranted because it costs too much.
9. The fallacy of ***negativism***: crises are solely negative in their impacts on an organisation.
10. The fallacy of ***"the end justifies the means"***: business ends justify the taking of high risk means or action.
11. The fallacy of ***discouraging bad news***: employees who bring bad news deserve to be punished.
12. The fallacy of ***luxury***: crisis management is a luxury.
13. The fallacy of ***quality***: quality is achieved through control not assurance.
14. The fallacy of ***fragmentation***: crises are isolated.
15. The fallacy of ***reactiveness***: it is enough to react to crises once they have happened.

16. The fallacy of ***experience and over-confidence***: the best prepared organisations are those that have experienced and survived a large number of crises or who have dealt with crises over their history.
17. The fallacy of ***financial/technical quick fixes***: it is enough to throw financial and technical quick fixes at crisis management (Mitroff, et al., 1989: 275)

Using the Mitroff, et al (1989: 269-283) study as cited in Stephenson, et al (2010: 19), they looked at ways to refine the benchmarking of resilience. After Stephenson sent out their initial questionnaires, adapted from the Mitroff, et al (1989: 269-283) model, they dropped twenty of the questions. They then updated the model and worked on the principle that organisational resilience comprised of two dimensions and thirteen indicators. The following table was developed from this refinement:

Table 2: A 'new' Organisational Resilience Model

Planning Dimension	**Adaptive Capacity Dimension**
Planning Strategies	Leadership
Participation in Exercises	Staff Involvement
External Resources	Situation Monitoring and Reporting
Recovery Priorities	Minimisation of Silos
Proactive Posture	Internal Resources
	Decision Making
	Innovation and Creativity
	Information and Knowledge

(Mitroff, et al, 1989: 276)

It is interesting to note how a number of these elements cross reference to Mitroff, et al earlier mentioned list of Faulty Organisational Assumptions and Beliefs (Mitroff, et al, 1989: 275).

4.6 GOVERNANCE AND COMPLIANCE

The *King Code of Governance for South Africa 2009* (Institute of Directors for Southern Africa *(IO*D) & King Committee on Governance, 2009) followed on from King I & II reports on corporate governance, and is a further refinement of corporate

governance in South Africa. Through the various King Reports, South Africa has attempted to ensure that South African businesses, especially those listed on the Johannesburg Stock Exchange, are given guidance regarding corporate governance based on international best practice. The content of King III Report is unique and although the initial thoughts were guided by the Sarbanes-Oxley Act of 2002 (also known as SOX (Pub.L. 107-204, 116 Stat. 745, enacted July 29, 2002), legislation in the United States, it has now developed its own character and is used as a reference guide by other countries seeking to do the same (Stimpson, 2012: 5-8). (See The *King Code of Governance for South Africa 2009* (IOD, 2009) and the new Companies Act, 2008 (Act 71 of 2008). At the launch of King III on the 1st of September, 2009, the chairman of the report, Judge Mervyn King, chaired a workshop that was held under the auspices of the Southern African Institute of Directors (SAIOD) dealt with the main elements of the Report and Code of Conduct. The programme included the following points of discussion:

- Governance
- Is Your Brand and Reputation Protected
- The importance of Sustainability Reporting
- Corporate Citizenship And Business Ethics
- Corruption Scandals
- Sustainability and Resilience: Moving beyond Reporting
- The Changing Role of the Audit Committee
- Risk Management
- The Relational Company

Resilience also featured as a point on the agenda which indicates that organisations are expected to prepare themselves for disruptive incidents. The structure of the corporate governance areas also indicate that directors of boards cannot say that they did not know as many checks and balances have been built into the process and audit committees play a very important role, not only in the way the business is run but also to the security and resilience of companies.

The Code does not only apply to listed companies but to any registered business in South Africa. It is now, more than ever before, a situation where company executives

are culpable, accountable and thus liable. Directors have to ensure an environment where the risks to the business are timeously and adequately identified and reduced to ensure a safe and secure environment for people to work in. Dr Gert Cruywagen, Director of Risk at TSG served on the Risk Management Committee of the King III Report and thus gave support and guidance as the ORMS was implemented at TSG.

Bigger organisations are now kept in line by the various compliance avenues. These include internal and external audit committees, risk committees, health and safety as well as security committees. These committees have to make sure that the business is in full compliance to applicable legislation and regulations. In the past few years we have seen how many of the bigger companies have been heavily fined by such agencies as the Competitions Board and the Department of Environmental Affairs (National Environment Management Act, 1998 (Act No. 21 of 1998). The Competition Commission is a statutory body constituted in terms of the Competition Act, 1998 (Act No. 89 of 1998) by the Government of South Africa, empowered to investigate, control and evaluate restrictive business practices, abuse of dominant positions and mergers in order to achieve equity and efficiency in the South African economy.

The result has been multi-million rand fines. The shareholders have not taken lightly to the dilution of their shares and have in some instances instituted direct civil action against board members for their lack of judgement and poor management decisions. The outcomes the increased compliance requirements for businesses will be seen in the next few years and if effectively implemented, will ensure a change in the way that business is done in South Africa, compared to the way it has been done previously.

Under the section, “Compliance with laws, rules, codes and Standards”, in the King III Report, companies must comply with all applicable laws. Laws should be understood not only in terms of the obligations that they create, but also for the rights and protection that they afford. Boards at companies are responsible for such companies’ compliance with applicable laws and with those non-binding rules, codes and standards with which the company has elected to comply. One of the most important responsibilities of a board is the monitoring of a company’s compliance

with all applicable laws, rules, codes and standards (PricewaterhouseCoopers (PwC), 2009: 43).

The result is that companies have started seeing the value and are spending money on developing an environment where the five silos of risk management, occupational health and safety, emergency planning, disaster management and security risk management can be better managed to create a more resilient organisation.

The past has shown that organisations manage many risk reduction programmes but that many of these are developed and implemented in isolation. A decision is taken at one level of a company and implemented without consultation with other parts of the business. This brings about confusion and an 'us versus them' scenario which serves no positive purpose in the company. The result is that not all the gaps are identified and resources are wasted, due to the building of supposedly specialised business units or divisions. In practice, Security Managers conduct physical security risk assessments and generate copious reports, Business Continuity managers conduct the Business Impact Analysis and the board develops a Group Risk Register that is maintained by the Risk Manager. Each of these units generally work in isolation and not as part of the same team.

According to Valsamakis, Vivian and Du Toit (2001: 10-17) the integration of the various risk management activities comprises the holistic risk management process. This is of a synergetic or systemic nature. This is where the sum of the parts is greater than the whole thereof. This is a fundamental principle of any form of modern risk management.

The result is that a portion of the information that should be shared in order to ensure a better understanding of the actual risks that the company may be facing, is hidden from members of the board by the operational heads of departments in some self-centred report that is often never disseminated beyond the actual persons involved in drawing up such report. Another common element that was found in the study by Stephenson, et al (2010: 30) was that organisations normally rely on a small group of people to "get the job done". The significance here is that organisations are supposed to have a functional compliance and responsive resilience programme but

they still do not fully grasp the value of having a resilient organisation. Many organisations rely on often ad hoc, poorly planned or under developed (in terms of detail, processes and procedures) arrangements that have been developed and designed to manage only expected small disruptions, to also manage larger scale problems and crises. They often believe that their arrangements can merely be ~~will~~ scaled up, i.e. merely increase numbers of required response or personnel involved. This 'upscaling' of an existing 'arrangement' or plan is then viewed as being applicable to any problem that might arise in the future. However, this is not necessarily true. Organisations should develop the skills sets to think about how their 'business-as-usual' approach would cope and work in an operational environment in the event of a large scale emergency, or during a crisis that lasted longer than expected. This slow attitude to adapt to the changing environment is a very dangerous situation to be in for any business or executive in today's times of compliance measurement and surveillance by internal and external audit committees. Corporate governance legislation and guidance brings a whole new dimension to the way businesses are managed today.

4.7 ESTABLISHING A RESILIENCE CULTURE

In a report titled: 'Managing risk in perilous times', authored by Alasdair Ross, edited by Rob Mitchell and published by *The Economist* Intelligence Unit, (Ross & Mitchell, 2009: 2-3), ten main points with reference to risk management were identified, namely:

1. Risk management must be given greater authority;
2. Senior managers must lead risk management from the top;
3. Businesses need to review the level of risk expertise in their organisation, particularly at the highest levels;
4. Institutions should pay more attention to the data that populates the risk models and must combine this output with human judgement;
5. Stress testing and scenario planning can arm executives with an appropriate response to events;
6. Incentive schemes must be constructed so that they reward long-term stability, not short-term profit;
7. Risk factors should be consolidated across all the business's operations;

8. Businesses should ensure that they do not rely too heavily on data from external providers;
9. A careful balance must be struck between the centralisation and decentralisation of risk; and
10. Risk management systems should be adaptive rather than static.

While all these identified factors were drawn from the financial sector in the UK, they are applicable to any environment and would therefore require the attention of executives in all different fields across an economy. The same can be said for Security Risk Management. The 10 points mentioned here can also be directly overlaid into the security filed. It has been an ongoing battle over many years to get commercial executives to understand the value of security in their organisations. Those executives who have fully incorporated there security function from something that was previously seen as an alien concept, have had more success with actually running their businesses. Today there are a number of security executives who serve on board of the companies they work for.

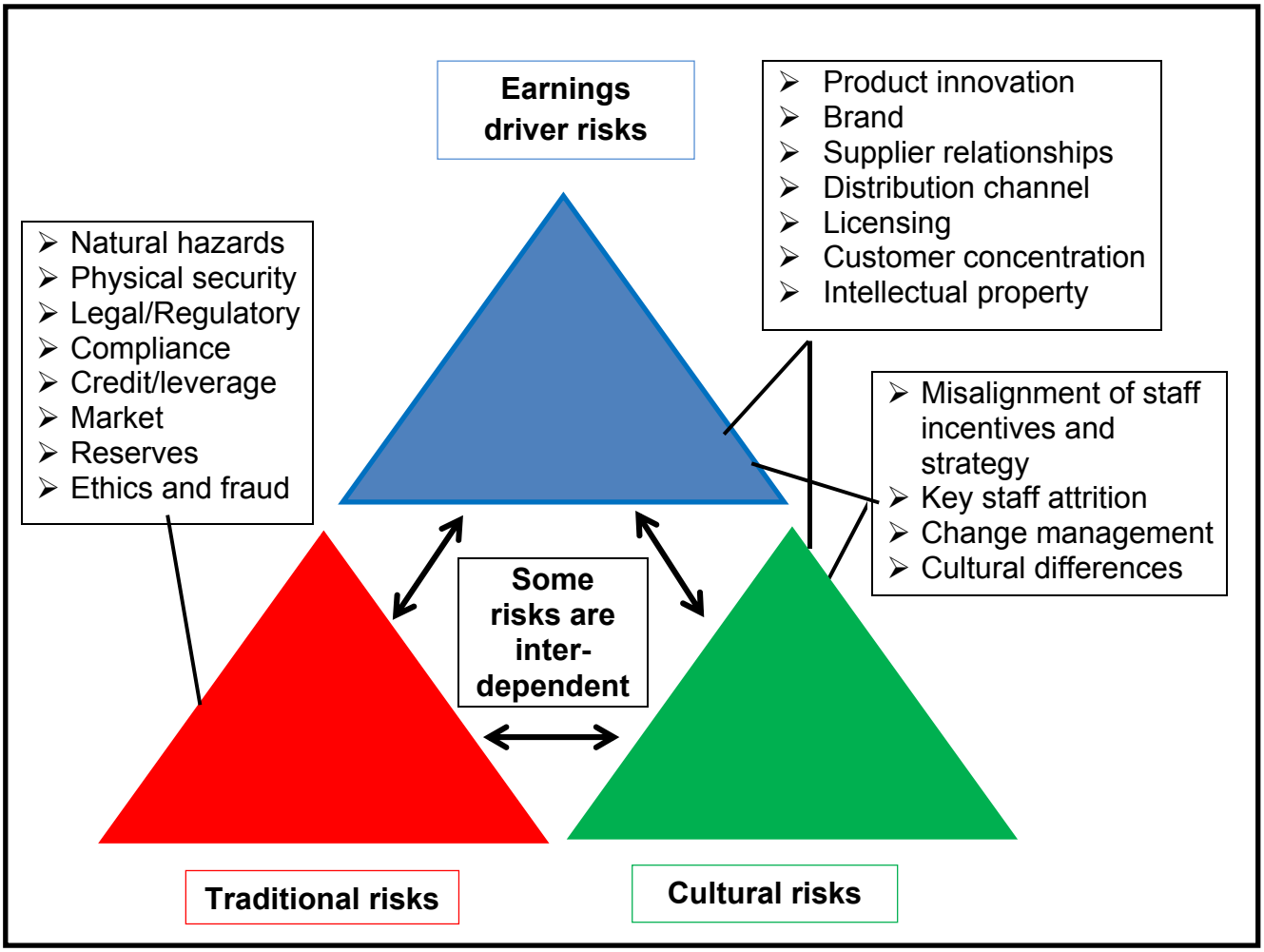
On the other hand, according to Kocourek, Pasternack, Kelly, Newfrock, Bienenstock, Gregory, Messineo and Powers (2004: 2), an effective enterprise-wide resilience approach should set the broad risk agenda and heightens awareness and transparency around material risks and efforts to manage them. This will enhance business discipline and internal controls while ensuring informed decision-making processes to strengthen strategic plans and overcome potential obstacles to meeting corporate performance objectives.

It would align risk management activity with board and management risk agendas and reconcile risk management priorities with strategic imperatives. This would bring about improvement of risk control management objectives while establishing a culture that embodies a common vision and taxonomy for managing and thinking about risk (Kocourek, et al, 2004: 2) It would further protect directors and officers against charges of lack of good faith and preserves for directors and officers the benefit of the business judgement rule and also improve corporate performance and shareholder value that builds stakeholder trust (e.g. investors, strategic partners, etc.) (Kocourek, et al, 2004: 2).

Based on the ten points of Ross and Mitchell and the list of Kocourek, et al, (2004: 2), there are a number of common points that are applicable to achieving the security risk management goals within a resilient organisation. The success of such a programme will be based on the way that leadership is provided by the board and executives of the company as well as the resources that are made available to ensure the implementation is successful and thus provides value to the organisation.

In order to graphically depict an important part of the changing the business risk landscape Kocourek, et al, (2004: 3) developed the following diagram on enterprise resilience. The diagram graphically summarises the risks that businesses face and the elements that are required for a resilient enterprise.

Figure 5: Enterprise resilience expands the view of risk



(Kocourek, et al, 2004).

With the advent of the King III Report in September 2009, directors and board members can no longer rely entirely on their top managers' management to determine what issues the board considers and what information is presented to the board for consideration and action. Directors have to ensure that systems are in place so as to flag issues that affect the whole company and its continued existence and/or survival in the future.

4.8 CONCLUSION

An organisational resilience approach, assists owners and operators of businesses and organisations to manage unforeseen or unexpected risks. These could be the risks that might never have been experienced by an organisation before or even categorised as foreseeable. Such unforeseen risks may also not form part of the formal risk management processes or business continuity exercises.

Attributes of organisational resilience need to be better understood and integrated into an organisation's philosophy and culture. This might ultimately help ensure survival of a company/organisation in times of adversity. The context in which organisations operate includes challenges such as rapidly changing operating environments, reliance on highly interdependent systems and globally dispersed third party providers.

While organisational resilience means different things to different people and different organisations/companies, this research sought to establish a set of core resilience principles and attributes that would establish a foundation for the tailoring of these attributes for organisations to consider and implement as appropriate.

CHAPTER 5
USING A MATURITY MODEL

5.1 INTRODUCTION

A Capability Maturity Model (CMM), including Capability Maturity Model Integration (CMMI), is a simplified representation of the word for use in some of the most complex projects. CMMs contain the essential elements of effective processes. These elements are based on the concepts developed by Crosby, Deming, Juran and Humphrey. In the 1930s, Walter Shewhart began work in process improvement with his principles of statistical quality control (Shewhart, 1931). These principles were refined by Edwards Deming (Deming, 1986), Phillip Crosby (Crosby, 1979) and Joseph Juran (Juran, 1988). Watts Humphrey, Ron Radice and others extended these principles even further and began applying them to software in their work at International Business Machines (IBM) and the Software Engineering Institute (SEI) (Humphrey, 1989). Humphrey's book, *Managing the software process*, provides a description of the basic principles and concepts on which many of the Capability Maturity Models (CMMs) are based (Software Engineering Institute (SEI), 2008).

Maturity Models are aimed at providing a simplified and easily communicable reproduction of reality. Maturity Models will generally distinguish no more than about five or six different levels of maturity. The principle behind the different levels is that an organisation develops new practices and processes, from which it learns and from which it can subsequently optimize these practices and processes to move on to the next level. Most Maturity Models are designed in such a way that an organisation cannot skip a level, although not all specialists agree on this statement (Mingay, 2002: 3). Simple models only describe the various maturity levels, while more extensive models also identify practices that can bring organisations from one level to the next (Smit, 2005, 27).

The Maturity Model that was used in this case study was developed by Dr Marc Siegel**,** Commissioner for Standards Development at ASIS International, and Maya Siegel, a graduate of Brandeis University in Waltham, Massachusetts, with input from the researcher as to some of the practical aspects that required attention. The

Model was developed during the latter part of December 2009 and January 2010 so that it could be used for the first ever implementation of the *ANSI/ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with guidance for use.* A copy of the Model developed by Siegel and Siegel is included as an addendum. The first time this Maturity Model was used, was here in South Africa prior to the FIFA World Cup. It was developed so that organisations can develop from one level to the next as the organisation improves its processes and establishes a resilient culture within the organisation, its stakeholders and the community it serves.

Subsequently, the *ANSI/ASIS.SPC.4-2012: Maturity Model for the Phased Implementation of the Organisational Resilience Management System,* (SPC.4), was published in April 2012. The standard development committees used the initial work done in South Africa to test the model from a practical perspective. The researcher served on the Technical Committee and Working Group of SPC.4 to develop this standard for ASIS International.

In this chapter the structure and workings of a few different Maturity Models are discussed. Specific reference is made to the Risk Management Maturity Model and the then unpublished ANSI/ASIS.SPC.4 model. The other models are discussed briefly to show that the development of the ANSI/ASIS.SPC.4 model used the same scientific base for its development as did the other previously used models in other sectors.

Most Maturity Models have five different levels of maturity. The exception here is that the ORMS Maturity Model is used together with the ANSI/ASIS SPC.1 - Organisational Resilience Standard where there are six levels. This should be noted while reading through the initial sections on the different types of Maturity Models as some of them have either one or two less, or one more, main elements that form the outline of the specific model. The ORMS Maturity Model is more fully explained later in this chapter.

5.2 A MATURITY MODEL

A maturity model can be viewed as a set of structured levels that describe how well the behaviours, practices and processes of an organisation can reliably and sustainably produce required outcomes. A Maturity Model may provide, for example:

- A place to start;
- The benefit of a community's prior experiences;
- A common language and a shared vision;
- A framework for prioritizing actions; and
- A way to define what improvement means for your organisation.

A maturity model can be used as a benchmark for comparison and as an aid to understanding a comparative assessment of different organisations, where there is something in common that can be used as a basis for comparison. In the case of the CMM, for example, the basis for comparison would be the organisations' software development processes.

Smit, (2005, 49-50) in her research on a maturity model for Business Continuity Management, documents the following stages which substantiate the general structure of previous and subsequent Maturity Models with a few minor adaptations for a specific environment:

- Initiated;
- Planned;
- Implemented;
- Embedded;
- Controlled; and
- Optimised.

5.2.1 Structure

The **Capability Maturity Model (CMM)** provides a theoretical scale along which process maturity can be developed incrementally from one level to the next. Skipping levels is not allowed or feasible. The CMM was originally intended as a tool to evaluate the ability of government contractors to perform a contracted software project in the United States of America.

The **Capability Maturity Model (CMM)** involves the following aspects:

Maturity levels: A five-level process maturity range – where the uppermost (5th) level is a hypothetical ideal state where processes would be systematically managed by a combination of process optimization and continuous process improvement.

Key process areas: A Key Process Area (KPA) identifies a cluster of related activities that, when performed together, achieve a set of goals considered important.

Goals: The goals of a key process area summarise the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organisation has established at that maturity level. The goals signify the scope, boundaries and intent of each key process area.

Common features: Common features include practices that implement and institutionalise a key process area. There are five types of common features:

- Commitment to Perform;
- Ability to Perform;
- Activities Performed;
- Measurement and Analysis; and
- Verifying Implementation.

Key practices: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the KPAs.

5.2.2 Levels

There are five levels defined along the range of the CMM. According to the SEI:

> Predictability, effectiveness and control of an organisation's software processes are believed to improve as the organisation moves up these five levels. While not rigorous, the empirical evidence to date supports this belief (SEI, 2008).

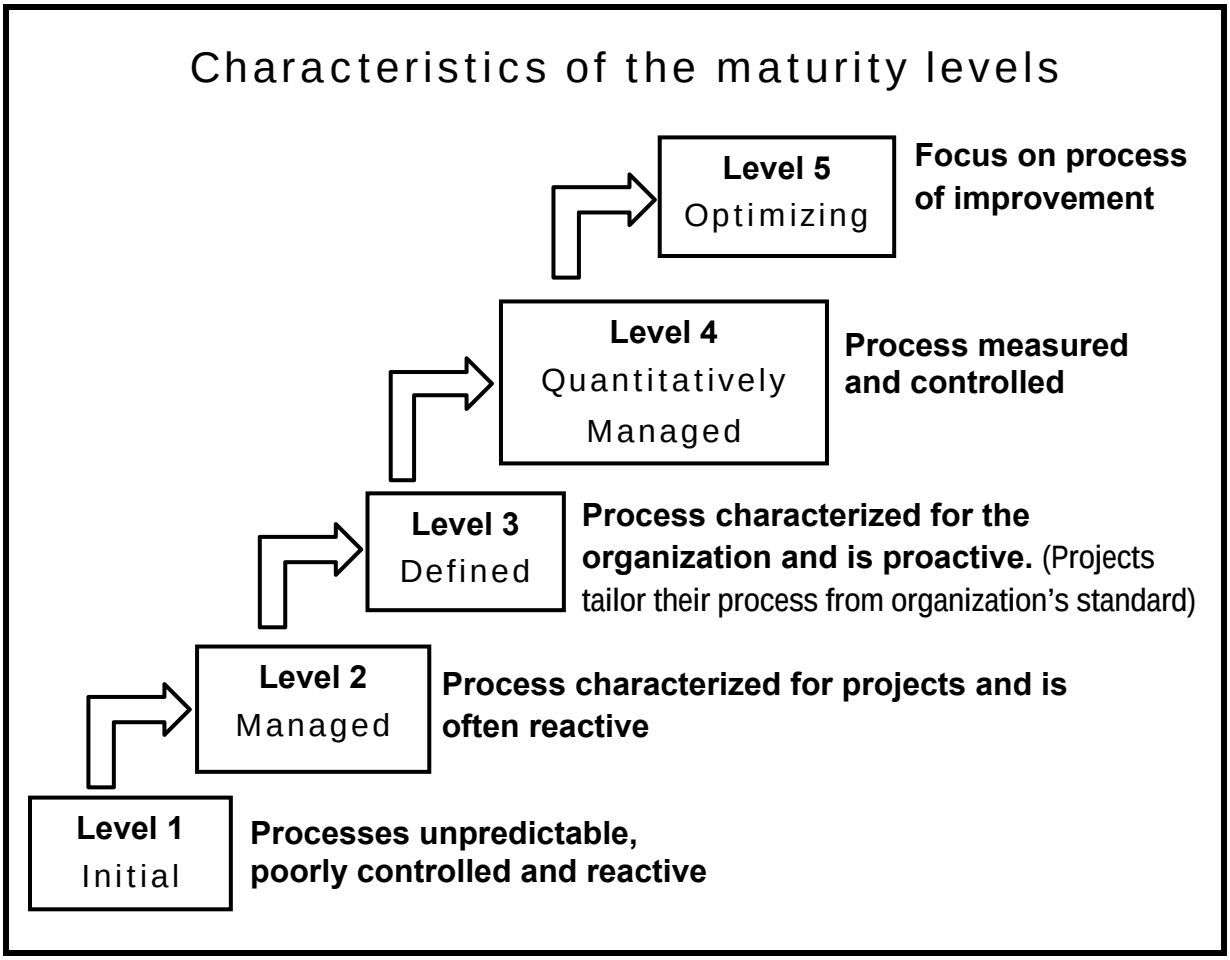
Initial (chaotic, ad hoc, individual heroics): This is the starting point for use of a new process.

Managed: The process is managed in accordance with agreed metrics.

Defined: The process is defined/confirmed as a standard business process and decomposed to levels zero, one and two (the latter being Work Instructions).

In her presentation, “What is CMMI?” at NASA, Sally Godfrey (2008) presented the following graphic model describing the different maturity levels:

Figure 6: Characteristics of the maturity levels



Sally Godfrey (2008).

5.2.3 Quantitatively managed

Optimising: Process management includes deliberate process optimisation/ improvement.

Within each of these maturity levels are Key Process Areas (KPAs) which characterise that level and for each KPA five definitions have been identified:

- Goals;
- Commitment;
- Ability;
- Measurement; and
- Verification.

The KPAs are not necessarily unique to CMM, representing, as they do, the stages that organisations must go through on the way to becoming mature.

A list of a few of the better known Maturity Models are listed here along with a short description that has been sourced from different sources where definitions are recorded.

5.3 CAPABILITY MATURITY MODEL (CMM)

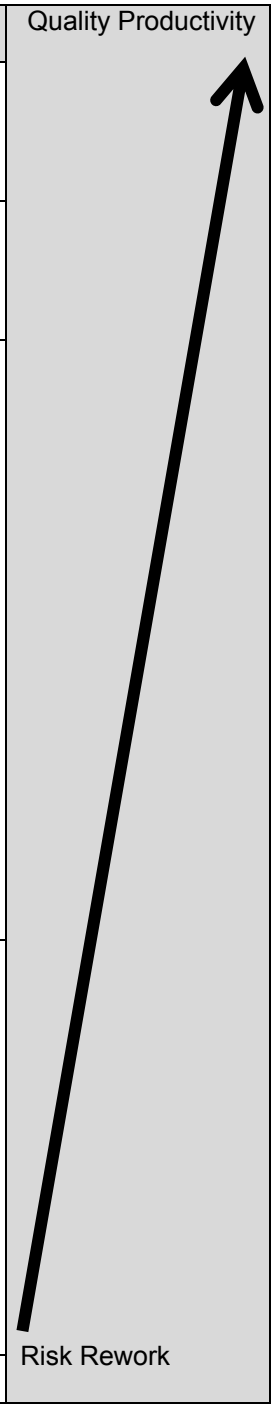
The Capability Maturity Model (CMM) is a service mark registered with the U.S. Patent and Trademark Office by Carnegie Mellon University (CMU) and refers to a development model that was created after studying data collected from organisations that contracted with the U.S. Department of Defence. The Department of Defence funded the research. This became the foundation from which CMU created the Software Engineering Institute (SEI, 2008). Like any model, it is an abstraction of an existing system (Paulk, Weber, Curtis & Chrissis, 1993: 177).

When it is applied to an existing organisation's software development processes, it allows an effective approach toward improving them. Eventually it became clear that the model could be applied to other processes. This gave rise to a more general concept that is applied to business processes and to developing people.

Standard CMMI Appraisal Method for Process Improvement (SCAMPISM) A, Version 1.2: Method Definition Document". CMU/SEI-2006-HB-002. Software Engineering Institute. 2006 (Software Engineering Institute (SEI), 2006).

Figure 7: Capability Maturity Model Integration (CMMI) process areas

Level	Focus	Process Areas
5. Optimizing	Continuous Process Improvement	Casual Analysis and Resolution Organisational Performance Management
4. Quantitatively Managed	Quantitative Management	Organisational Process Performance Quantitative Project Management
3. Defined	Process Standardization	Decision Analysis and Resolution Integrated Project Management Organisational Process Definition Organisational Process Focus Organisational Training Product Integration Requirements Development Risk Management Technical Solution Validation Verification
2. Managed	Basic Project Management	Configuration Management Measurement and Analysis Project Monitoring and Control Project Planning Process and Product Quality Assurance Requirements Management Supplier Agreement Management
1. Initial		



(Software Engineering Institute (SEI). 2006).

Following on from the previous two graphics and the general highlights of the different levels of the maturity models, the following pointers are summarised from the CMMI process (Software Engineering Institute (SEI). 2006).

Level 1: ***Initial (Chaotic)***

It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an *ad hoc*, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2: ***Repeatable***

It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3: ***Defined***

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the ASIS processes) and used to establish consistency of process performance across the organisation.

Level 4: ***Managed***

It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

Level 5: ***Optimising***

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

At maturity Level 5, processes are concerned with addressing statistical common causes of process variation and changing the process (for example, to shift the mean of the process performance) to improve process performance. This would be

done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives.

5.4 E-LEARNING MATURITY MODEL (EMM)

In the arena of e-Learning, the Modelling of Maturity Levels is a classification system defined by Kleppe, Warmer and Bast in their book: *MDA explained: The model driven architecture – practice and promise* (2003: 9). The levels characterise the role of modelling in a software project to be used in the e-Learning sector. The concept shows resemblance to the way software processes are rated with and compared to the Capability Maturity Model described here above. This is further substantiated in this environment by Mettler, Rohner and Winter in their book: *Towards a Classification of Maturity Models in Information Systems, Management of the Interconnected World* (2010: 333-340).

The levels are:

Level Zero (0): No Specification:
The specification of software is not written down. It is kept in the minds of the developers.

Level 1: Textual Specification:
The software is specified by a natural language text (be it English or Chinese or something else), written down in one or more documents.

Level 2: Text with Models:
A textual specification is enhanced with several models to show some of the main structures of the system.

Level 3: Models with Text:
The specification of software is written down in one or more models. In addition to these models, natural language text is used to explain details, the background and the motivation of the models, but the core of the specifications lies in the models.

Level 4: Precise Models:

The specification of the software is written down in one or more models. Natural language can still be used to explain the background and motivation of the models, but it takes on the same role as comments in source code.

Level 5: Models only:

The models are precise and detailed enough to allow complete code generation. The code generators at this level have become as trustworthy as compilers; therefore no developer needs to even look at the generated code.

5.5 THREADS IN MATURITY MODELS

All Maturity Models have certain threads that follow through to the model.

- Open Source Maturity Model;
- OPM3 (Organisational Project Management Maturity Model);
- People Capability Maturity Model;
- P3M3 (Portfolio, Programme and Project Management Maturity Model);
- Quality Management Maturity Grid; and
- Testing Maturity Model.

The same threads also form the foundation of the maturity model used for *ANSI/ASIS SPC.1-2009,* the Organisational Resilience Management System Standard. One of the main differences in the maturity model used in the case study implementation, based on ANSI/ASIS SPC.1, is that where all the other models have five levels, the latter has six levels. This is because it is based on the Organisational Resilience Management System Standard where there is a cycle of continuous improvement added. The system is thus based on the Plan-Do-Check-and-Act framework of a management system.

The last example of a maturity model before researching the maturity model's as applicable to the risk and security risk management environments, is a model that was developed by Moore (2008), for the Gartner "IAM Program Maturity Model". It shows basically the same levels and threads as the others that have been discussed

and also only has five levels of maturity as indicated from the header and footer section that is shown here:

Figure 8: Gartner IAM Program Maturity Model

IAM Program Maturity Level	1. Initial	2. Developing	3. Defined	4. Managed	5. Optimized

Legacy Program Maturity Level	Blissful Ignorance	Awareness	Corrective	Optional Excellence

This model is more fully populated across the various elements here below:

The Gartner IAM Program Maturity Model					
IAM Program Maturity Level	**1. Initial**	**2. Developing**	**3. Defined**	**4. Managed**	**5. Optimized**
Governance	**Ad hoc, informal**	**Subsumed within InfoSec (and InfoSec governance structures)**	**IAM governance structure defined and accepted**	**IAM governance structure fulfilled and refined**	**IAM governance optimization**
Organisation	**Informal, basic roles, responsibilities decentralized**	**Technical projects sponsored by Bus and CISO; informal inventory of IAM skills**	**IAM PMO Established IAM roles an training needs defined**	**IAM PMO active, RACI matrix defined; proactive skill development**	**Optimal integration with business; skills optimized**
Vision and Strategy	**Conceptual awareness**	**Certain business drivers identified; tactical priorities set**	**Business-aligned vision defined; strategic priorities set**	**IAM vision and strategy continually reviewed to track business strategy**	**Periodic optimization of vision and strategy**
Processes	**Ad hoc, informal**	**Semiformal BU-specific and target-**	**Formal processes defined,**	**Formal processes integrated**	**Process optimization**

		specific processes	**consistent across Bus and target systems**	**and refined; aligned with business processes**	
Architecture and Infrastructure Design	**Possible use of target-specific productivity tools**	**Disjoint technical projects; technology redundancy likely**	**Discrete IAM architecture defined; rationalization and consolidation in hand**	**IAM architecture refined and aligned with EA**	**IAM architecture embedded with EA; optimization**
Business Value	**None measurable**	**Tactical efficiency and (maybe) effectiveness improvements ; low direct value**	**Sustained, quantifiable improvements tied to GRC imperative; moderate direct value**	**Sustained, quantifiable contribution to all key business imperatives; high direct value**	**Business value optimization; transformational direct value**
Legacy Program Maturity Level	**Blissful Ignorance**	**Awareness**	**Corrective**	**Optional Excellence**	

(Anon (Gartner Group website), 2010)

5.6 MATURITY MODELS FOR MANAGING RISK

The Risk Management Society (RIMS) (Australia) Risk Maturity Model presents the Risk Maturity Model as 7 steps. However, on closer examination it was found that in comparison to the ANASI.ASIS. SPC.1 ORMS, the 6th step of the ORMS model and 7th step of the RIMS models are very similar (Anon (Griffith University), 2011). RIMS, the Risk and Insurance Management Society, Inc. (RIMS) is a global not-for-profit organisation representing more than 3,500 industrial, service, non-profit, charitable and government entities throughout the world. Founded in 1950, RIMS brings networking, professional development and education opportunities to its membership of more than 10,000 risk management professionals who operate in more than 120 countries (RIMS: 2012).

Step 1: Enterprise risk management-based approach

Implanting ERM into an existing organisation will require substantial investment both in financial and human resources. Therefore, the chances of success rely heavily on not only the C-suite commitment to the project, but even the support from the board of directors (clearly, that will depend on the value proposition involved in ERM).

Step 2: ERM process management

Successful ERM is achieved through a change in the corporate culture. If ERM is global – transcending the silos of risks – it must also be integrated into every manager's mission and all business processes. This accountability of all risk owners to manage their risks is a key to the successful implementation of ERM.

Step 3: Risk appetite

The global management of all risks – threats as well as opportunities – requires clearly defining a level of risks with which the Board is 'comfortable' and making sure that the decision-making process internalises the risk element to allow for the best possible management of the risk appetite.

Step 4: Root cause analysis

Capitalising on past experience, building a strong data bank to assist in decision-making and measuring the results of risk reduction efforts is crucial to demonstrating the value created by ERM. However, for rare and catastrophic events there may be no 'data bank'. Furthermore, for repetitive events, understanding the causes is essential to sound prevention. This is why conducting root cause analysis is necessary to link events and the causal chain that made them possible, so as to prevent or contain the undesirable ones or to enhance the occurrence or impacts of the desirable ones.

Step 5: Risk assessment

Rational decisions on risks can only be reached if decision-makers can rely on robust information to form a judgment. This is why a continuous risk assessment process must be in place, identifying, analysing and evaluating risks, threats and opportunities alike and consigning them on a risk register where risk owners are

clearly identified and the steps to improvement entered into a timetable.

Step 6: Management performance

If risk management is part of any manager's mission, then it must also be a factor in determining their bonus – i.e. the measure of their performance. Balanced scorecards must be developed to encompass not only short-term results but also long-term contribution to sustainability and growth.

Step 7: Resilience and sustainable development

The overall goal of any company is to retain its 'social licence to operate' and achieve sustained growth for the benefit of its stakeholders. Precisely the full development of ERM will be achieved when its contribution to long-term sustainability, financial, economic and social, and its enhancement of the organisation's resilience is clearly benchmarked and measured through its integration into operational planning.

5.7 LEVELS OF MATURITY IN REDUCING OPERATIONAL RISK

5.7.1 Keeping people safe

Asset-intensive industries that put their employees in harm's way have always taken responsibility for safety and security seriously. However, this too often became an exercise managing documentation, responding to adverse events. The objective is to make sure those documented policies and procedures are integrated in such a way that safety and security is managed proactively. This suggests that a closed loop monitoring system is developed and maintained to functionally deliver this goal (Parker, Feblowitz & Knickle, 2008: 15-17).

They further state that the integration of all organisational operational risk issues creates major problems for companies. The lack of a comprehensive view of standards and practices prevents compliance and hinders the ability to protect employees and assets. The problem lies largely at the detail level, including issues such as whether employees have the right training and medical baseline established, thorough follow-through on corrective measures, and tracking exposure levels. The details are known in isolation but must be made transparent in context to affect full control.

Getting the integration done requires several key capabilities. The effort must start with a view of employee safety that transcends organisational boundaries that exist between human resources, asset management, industrial health/safety personnel and external authorities. Once a culture of collaboration is established across the company, key processes can be improved and better managed.

Assuring the health and safety of employees is the foremost benefit, but several other advantages can be achieved. Streamlined, integrated processes save time and money. Better capture of legally required information, more complete documentation and more accurate application of the surveillance protocols are also then realised.
Prevention shouldn't get in the way of performance. An industry-standard process platform for asset management with the attendant visibility into activity at the machine, plant, and corporate-wide level, will allow companies to not only control operational risk but optimise operational effectiveness.

A comprehensive approach ensures that the benefits which are captured simultaneously requires an assessment of existing capabilities and an understanding of the necessary steps toward implementation.

5.8 LEVELS OF MATURITY IN REDUCING OPERATIONAL RISK

As seen from the different maturity approaches that have been discussed previously in this chapter, there is a path to improving performance. At each step of the way an organisation will need to focus on moving up the ladder in sync to arrive at the next level.

To ensure that they receive the full benefits of an operational risk management program, companies should make progress in order to mature approaches to stakeholder transparency underpinned by increasingly sophisticated capabilities to keeping people, assets and the environment safe. The operational risk maturity model should be used to assess current capabilities, bring the various dimensions into a common state and articulate the steps that need to be taken. This exercise will form the basis for organising an enterprise risk management program unit to manage the projects that will change behaviour, transform processes, and deliver results. The next figure displays the levels of maturity for reducing operational risk.

Table 3: Expected results of a Comprehensive Operational Risk Management Programme

Expected results of a Comprehensive Operational Risk Management Programme	
Focus	**Benefits**
Keeping stakeholders informed	Proactive risk management with visibility and early warning signals Stronger connection between company reputation and operational and environmental policies Global workflows to produce better, higher-quality information for customers, including improved material/safety data sheets
Keeping the environment safe	More forward planning to eliminate regulatory infractions and financial penalties Lower costs and more efficient use of resources such as water and energy to lower greenhouse gas emissions Better material handling including processes related to safety, dangerous goods tracking and security
Keeping the people safe	Reductions in serious incidents through prevention management, best practice sharing and improved visibility More productive, safer workforce with less downtime through accident avoidance Certified, company-wide processes for safety training and medical management
Keeping the assets safe	Audit transparency and best practice sharing across operations and facilities Cost-effective maintenance and reliability programmes Better ROA through integration of assets, operations and compliance

5.9 AN OPERATIONAL RISK MATURITY MODEL

Figure 9: An Operational Risk Maturity Model

(Parker et al, 2008: 18)

5.10 THE DEVELOPMENT OF THE MATURITY MODEL FOR ORGANISATIONAL RESILIENCE

As mentioned earlier in this chapter, the Maturity Model for *ANSI/ASIS SPC.1-2009* Organisational Resilience Management System Standard was developed by Dr Marc Siegel and his daughter Maya Siegel in the USA. The draft was published in January 2010 (ANSI/ASIS:2009 - Maturity Model for the ORMS, vii). This is the document that the Case Study in this research is based on. This section is based on their work and the implementation elements that were identified by the project team for implementation during the case study. The work has been slightly modified for the requirements of the Case Study where in particular a scoring mechanism was required.

The scoring mechanism was based on the following:

- ‘0’ - If nothing had been done and no proof of work on the specific point could be shown to the audit team;
- ‘1’ - Work in progress and proof of such work is made available during the audit/review but is not as required by the organisations; and

- ‘2’ - Completed with proof of completion. All documentation is tabled.

This model is not meant to be regarded as a certification tool, but rather a mechanism to help organisations become more focussed and aware of the benefits of resilience management and preparedness programme. The model assists the organisations phase in a globally recognised management system based on their own business needs and economic capacity.

(Siegel and Siegel, 2010: 2) states that:

> A maturity model for the phased implementation of the *ANSI/ASIS SPC.1-2009* helps develop the momentum in support of resilience management and preparedness needed to encourage persons to manage their risks by seeing clear benefits of their participation. By carefully setting objectives and targets to maximize chances of early success, it is possible to stimulate top management support and acquire needed resource to implement the management system. Publicizing and recognizing success breeds necessary level of enthusiasm and credibility throughout the organisation to move from phase to phase towards the goal of a fully integrated resilience management and preparedness system. Standards are designed to promote managed and repeatable performance. This will be achieved by moving up the phases of the model.

An effective resilience management and preparedness programme is reliant on the participation of everyone in the organisation. A significant paradigm shift in the

culture of the organisation is required. The management of risks is no longer just the responsibility of management but of every member of the organisation. To eventually fully integrate a management system, the participation of all stakeholders in the organisations is required. Creating excitement with the development and implementation of the programme is essential to make it successful at all levels in the organisation. Everyone needs to feel that their contribution is as important as that of anyone else in the organisation.

This Maturity Model is a series of steps designed to help organisations to:

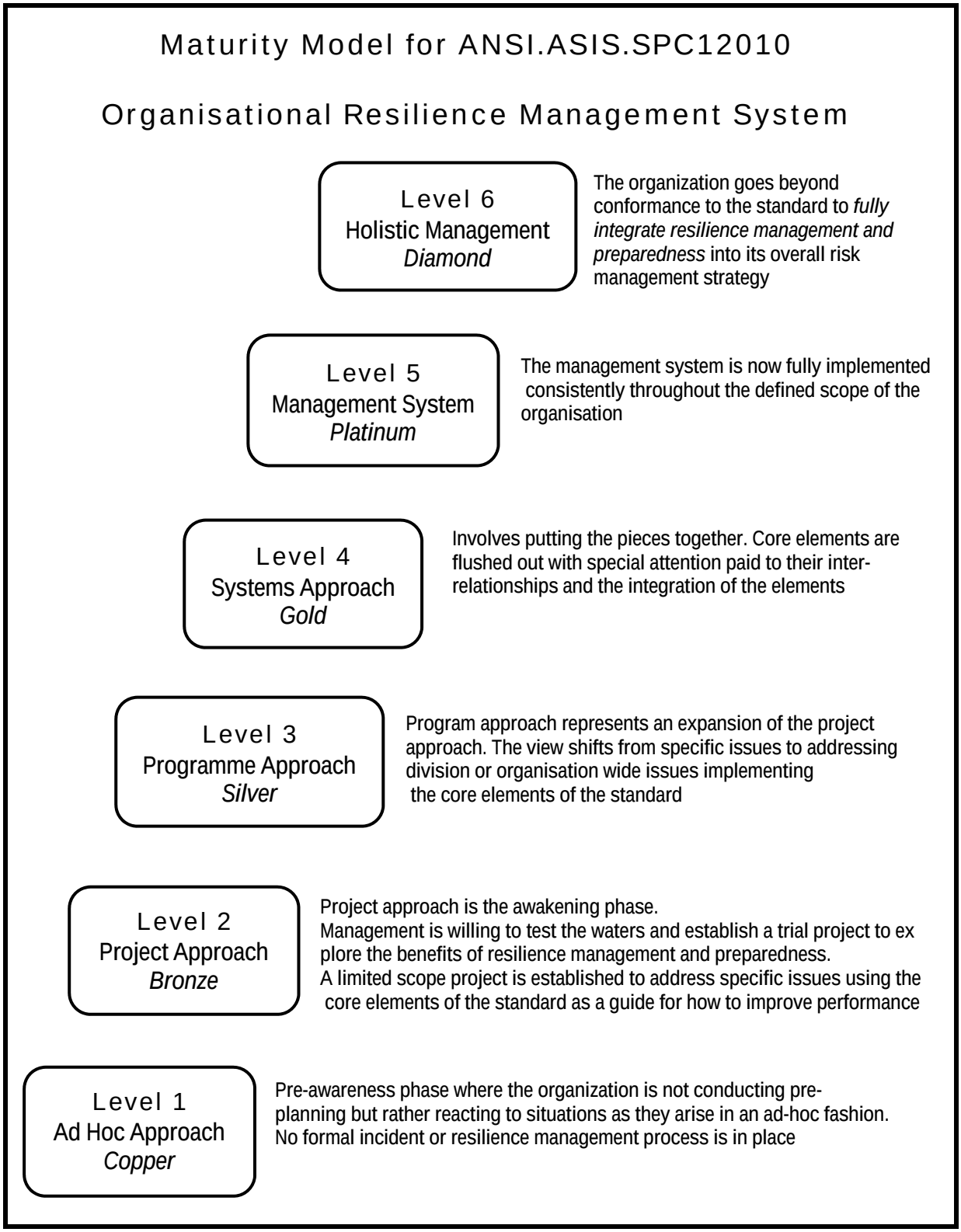
- Evaluate their present status in respect of resilience management and preparedness;
- Set goals for what they want to achieve;
- Establish a benchmark where they are relative to those goals; and
- Strategise a feasible business programme to achieve these goals.

The tables used for reference in this section are used with the permission of ASIS International who are the copyright holders.

5.11 LEVELS OF THE ORGANISATIONAL RESILIENCE MATURITY MODEL

The following are the different levels of the Maturity Model used in the case study and are depicted in graphic form:

Figure 10: Maturity Model for ORMS



(ANSI/ASIS, 2009: 47).

The initial document had six levels and naming protocols as mentioned above. This initial model has now been superseded by a full-blown standard which was published in April 2012. The standard has been published as the *ANSI/ASIS SPC.4 Maturity Model for the Phased Implementation of the Organizational Resilience Management System.* The researcher served on the international committee which developed this new standard.

[For a summary of all the elements of the levels of the Organisational Resilience Maturity Model as developed by Siegel and Siegel (2010) see the matrix in Annexure I: MATURITY MODEL FOR THE PHASED IMPLEMENTATION OF THE *ANSI/ASIS SPC.1-2009 ORGANIZATIONAL RESILIENCE: SECURITY, PREPAREDNESS AND CONTINUITY MANAGEMENT SYSTEMS – REQUIREMENTS WITH GUIDANCE FOR USE*.]

The six different Levels of the Organisational Resilience Maturity Model are as follows:

1. The standard's clause;
2. Core element;
3. Issues addressed by the core element;
4. The specific level's requirements;
5. Documentary or other proof requirements; and
6. Score.

[The tables in Annexure E are more fully descriptive of each of the different levels and how these are divided into the respective columns]

A description of each of the levels and the specific requirements for each is given here below. The numbering of the left-hand columns in the table are linked to the (ANSI/ASIS, 2009: 47).

5.11.1 Level 1: Ad Hoc approach - Copper

This is the ***pre-awareness*** phase.

- The organisation is not conducting pre-planning but is reactive to incidents and threats in an ad-hoc manner.
- No formal incident or resilience management process is in place.
- Lack of information and knowledge about resilience management and preparedness.
- Financial barriers are normally the barrier to effective preparedness planning.
- Management are scared that recognition of problems may be interpreted as an admission of weakness.
- Comfort is sought in the assumption that not identifying or recognizing problems makes the organisation not accountable for the problems.

The requirements of stepping up from Level 1 to Level 2 are:

- Recognize the need and value of resilience management and preparedness.
- A disruptive event may trigger a realization that pre- planning might have saved the organisation time and money.
- External factors, such as stakeholder concerns, contractual requirements, or government encouragement may cause the organisation to consider exploring a more proactive approach.

5.11.2 Level 2: Project approach - Bronze

This is the ***awakening*** phase.

- Management is willing to test the waters and establish a trial project to explore the benefits of resilience management and preparedness.
- A limited scope project is established to address specific issues using the core elements of the standard as a guide for how to improve performance.
- Management clearly defines the objectives and expectations of the project.
- Management designates a “Project Leader” with the authority and competence to conduct the project and serve as the resilience champion.
- To assure the best outcome of the project, issues addressed must be carefully selected to maximize the likelihood of quick success.

- The project focus is on demonstrating the need and value of resilience management and preparedness.
- The underlying assessment of the project is a gaps analysis examining what is needed for achieving the goals of the project in order to recognize and publicize a success to generate momentum for a broader resilience management and preparedness program.

To move to the next step, Level 3, the following is required and has to be understood:
As in any business project, the following is required:

- clear definitions of objectives;
- authorities;
- roles;
- responsibilities;
- budgets;
- timeframes;
- measurement methodology; and
- outcomes monitoring.

The Project Leader needs to have:

- management support;
- adequate resources to conduct the project;
- access to adequate training; and
- expertise is needed to support the Project Leader and members of the project team, especially if they have not had any experience in this field before.

Before moving to Level 3, issues need to be addressed using the core elements of the structure provided by the standard. The core elements need to be identified by the project group so that they can develop a programme which will improve the organisation's resilience, performance and preparedness. These are all steps that are taken to start establishing a culture of resilience ad preparedness in the organisation.

At this level, the operational issues should be addressed first as they are normally the easiest to identify, correct if required and structure for effective future management. Once this is done, and results become visible, getting buy-in at all levels will start to improve. “Success breeds success” (Siegel and Siegel, 2010: 4).

5.11.3 Level 3: Programme approach - Silver

This is the program approach. It is an expansion of the project approach.

- Move to address business unit and organisation wide issues implementing the core elements of the standard;
- Focus is on the activities outlined in the individual core elements rather than their interrelationships and integration of the elements;
- Risk management applications are selected for chances of demonstrating success and awareness;
- Top management recognises the importance of the elements and the need for pre-planning; and
- The application of the standard is still in a pilot testing mode with parts of the organisation applying the elements of the standard and testing action plans to make a business case for implementing the management system standard in full.

This phase provides the opportunity to increase awareness to a larger portion of the organisation. The ‘Program Manager’, appointed and endorsed by top management, is expanding the project to address broader issues related to the organisation’s reliability, sustainability and survivability in the event of a disruption.

Emphasis is on developing a series of action plans to deal with critical issues. The issues selected may be in reaction to an incident or near miss, or driven by external concerns. When developing the action plans the organisation develops proactive plans to better respond to the identified issues.

The organisation should consider measures to reduce the likelihood of disruptive incidents as well as the consequences. Typically, more weight is given to proactive planning to address the symptoms and consequences of a disruption.

5.11.4 Level 4: Systems approach - Gold

Phase Four involves putting the pieces together. Core elements are flushed out with special attention paid to their interrelationships and integration of the elements.
The core elements are viewed in terms of identifying and addressing root causes of disruptions as well as finding economically viable solutions addressing the root causes.

Resilience management and preparedness are viewed as part of an iterative continual improvement process using the ***Plan-Do-Check-Act*** model. Integration and feedback loops of the systems approach encourage learning from experience.

Top management recognises, understands and is committed to the strategic importance of resilience management and preparedness. Top management is actively engaged in the elements of the management system and standards. Critical business functions and activities have been identified, risk criteria set, and risks are prioritised.

The focus is on identifying opportunities for improvement in resilience and preparedness performance. Various parts of the organisation are testing the standard's core elements to refine the implementation of the standard. Audit findings are used to identify opportunities for improvement in order to reinforce the competitive and strategic advantage of the organisation. A culture of resilience and preparedness should now be visible in the organisation.

5.11.5 Level 5: Management system: Platinum

Fully implemented management system. Consistent functioning of system throughout the defined scope of the organisation.

It is from this level onward that it becomes more difficult for organisations to adhere to the recommended processes, as the elements become more focussed

on the requirements of the standard. Top management realises that there is value in the results, but may feel that the financial resources that are required for further development are not justified. This is also seen as the level that many organisations will set out to achieve. It is at this level that all basic systems that affect the resilience, performance and preparedness of the organisation should have been implemented and adequately tested.

- The organisation can now demonstrate conformance to the standard (either by first, second or third party validation).

- A multi-year perspective recognizing the utility of the management system standard has been visibly endorsed by top management and resilience and preparedness are fully integrated into the organisations functions and activities.

- A resilience management culture is promoted within the organisation encouraging persons throughout the organisation to take ownership of risk and think about their role in identifying, assessing and managing risk to promote resilience and preparedness.

The managing of risk uses balanced strategies to adaptively, proactively and reactively address the minimisation of both the likelihood and consequences of disruptive events. However, adaptive and proactive strategies are clearly seen as the preferred approaches to managing risks. Risk management, risk assessment and resilience management are considered key components of the overall decision- making process in the organisation. Resilience and preparedness training and awareness are a routine part of the human resource management of all persons providing services to the organisation.

All the core elements of the ORMS Standard have been applied and tested. Audits, evaluations and management review move beyond a focus on opportunities for improvement, to promoting competitive advantage and extending the management systems approach. This approach is applied to new applications,

divisions and parts of the enterprise. There is a continual drive to make the system processes more efficient and effective to support continued interest and excitement in the resilience management and preparedness processes.

5.11.6 Level 6: Holistic Management: Diamond

Fully integrated resilience management throughout the organisation:

- Ongoing maintenance and improvement.

- The organisation goes beyond conformance to the Standard to:
  - Fully integrate resilience management and preparedness into its overall risk management strategy.

- The organisation emphasises enterprise- wide and supply chain relationships, as well as:
  - Community responsibilities, in all aspects of it resilience management system.
  - Resilience management culture is well developed and considered an inseparable part of decision making.
  - Resilience management and systems principles are expanded to all areas of business and activities.

The organisation mentors other stakeholders (in its supply chain and community) recognising that Organisational Resilience is an integral part of community resilience.

5.12 CONCLUSION

Maturity Models are 'living' entities and thus adapt to changing circumstances and operational environments. The ORMS model, as used in the case study, was used for the first time in 2010 as mentioned before. It had not been tested anywhere else and as there had to be a starting point from where the first steps could be taken in its development, it had to be adjusted and tested against available, practical, working environments.

The ORMS Maturity Model worked exceptionally well for this Case Study. As the base was quite solid, it was quickly implemented throughout the Tsogo Sun Group, with some minor adjustments to the deliverables that were required from an organisational perspective.

A number of organisations, such as the Marriott Hotel and Leisure Group have also started implementing the Maturity Model across their network. There are many interested organisations from around the world that have started working on the implementation of this tool for the standardisation of a process to measure the maturity of an organisation's resiliency capacity.

CHAPTER 6
ISO 19011: 2002 GUIDELINES FOR QUALITY AND/OR ENVIRONMENTAL MANAGEMENT SYSTEMS AUDITING

6.1 INTRODUCTION

The existing guideline for auditing quality and/or environmental management systems is the *ISO 19011:2002: Guidelines for quality and/or environmental management systems auditing*. It replaced the previous 10012 guides in 2002. This guideline was updated towards the end of 2011 as it was then still awaiting final approval as a Final Draft International Standard (FDIS). This chapter is based specifically on ISO 19011: 2002, since it was used as the baseline audit criteria for the Case Study in this research report.

A summary of the sections have been made to ease the referencing and understanding of the process. As there is very little research material available regarding the audit process used by this standard, the material used for reference is based on the content and layout of the standard itself along with experiences that the researcher encountered during the Case Study.

The framework of the standard has been used as it is published in ISO 19011:2002 to outline the requirements and guidelines.

6.2 APPLICATION

The application of the Standard to other types of audits is possible in principle, provided that special consideration is given to identifying the skills competencies needed by the audit team members and the environment that is being audited.

The most significant change brought about with ISO 9001: 2000 and ISO 19011: 2002 is the concept of auditing for process and system effectiveness. The previous two editions of the standard and their audit guidelines focused primarily on compliance to the clauses/sections in the standards and not on the impact evaluation of the implemented measures.

An organisation must still comply with the standard's requirements or there would be very little point to having a standard. However, the primary focus of the audit is:

- meeting customer requirements through controlled and effective processes;
- meeting the objectives for the process; and
- continual improvement of the processes.

This follows the principle of a management system which is based on the Plan-Do-Check-Act (PDCA) principles.

Management system audits are used to detect any weaknesses or potential weaknesses in the organisation that could affect customers.

Environmental management system audits are conducted as a pollution prevention activity.

ISO 19011: 2002 is subdivided into the following headings:

Section 1: Scope reference and definitions;
Section 2: Principles of auditing;
Section 3. Managing an audit programme;
Section 4: Audit programme implementation;
Section 5: Audit activities;
Section 6: Preparing for onsite activities;
Section 7: Conducting onsite activities;
Section 8: What the auditor is looking for;
Section 9: Audit reporting;
Section 10: Audit techniques;
Section 11: Audit path;
Section 12: Effective communications;
Section 13: Sampling;
Section 14: Audit completion and follow-up; and
Section 15: Competence and evaluation of auditors.

ISO 19011: 2002

Section 1: Scope, reference and definitions

The ISO 19011: 2002 provides guidance on the principles of auditing, managing audit programmes, conducting quality management system (QMS) audits and Environmental Management System (EMS) audits, as well as guidance on the competence of quality and environmental management system auditors.

It is applicable to all organisations needing to conduct internal or external audits of quality and/or environmental management systems or to manage an audit programme.

References

The following documents contain provisions which, through references in this text, constitute provisions of this Standard.

ISO 9001, Quality Management Systems Fundamentals and Vocabulary

ISO 14050: 2002, Environmental Management Vocabulary

Terms and definitions:

For the purpose of ISO 19011: 2002 the terms and definitions given in ISO 9000 and ISO 14050 apply, unless superseded by the terms and definitions given below and copied directly from the standard so as not to lose any context in the interpretation.

Audit: Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

NOTE 1: Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organisation itself for management review and other internal purposes, and may form the basis for an organisation's self-declaration of conformity. In many cases, particularly in smaller organisations, independence can be demonstrated by freedom from responsibility for the activity being audited.

NOTE 2: External audits include those generally termed second and third party audits. Second party audits are conducted by parties having an interest in the

organisation, such as customers, or by other persons on their behalf. Third party audits are conducted by external, independent auditing organisations, such as those providing registration or certification of conformity to the requirements of ISO 9001 or ISO 14001.

NOTE 3: When a quality management system and an environmental management system are audited together, this is termed a combined audit.

NOTE 4: When two or more auditing organisations cooperate to audit a single auditee, this is termed a joint audit (ISO 19011:2002: 3.1).

Audit Criteria: A set of policies, procedures or requirements.

NOTE: Audit criteria are used as a reference against which **audit evidence** (3.7) is compared (ISO 19011:2002: 3.2).

Audit evidence: Records, statements of fact or other information, which are relevant to the **audit criteria** (3.3) and verifiable.

NOTE: Audit evidence may be qualitative or quantitative (ISO 19011:2002: 3.3).

Audit findings: Results of the evaluation of the collected **audit evidence** (3.3) against **audit criteria** (3.2).

NOTE: Audit findings can indicate either conformity or non-conformity with audit criteria or opportunities for improvement (ISO 19011:2002: 3.4).

Audit conclusion: Outcome of an **audit** (3.1), provided by **audit team** (3.9) after consideration of the audit objectives and all **audit findings** (3.4) (ISO 19011:2002: 3.5)

Audit client: Organisation or person requesting an **audit** (3.1).
NOTE: An audit client may be the **auditee** (3.7) or any other organisation which has the regulatory or contractual right to request an audit (ISO 19011:2002: 3.6).

Auditee: Organisation being audited (ISO 19011:2002: 3.7).

Auditor: A person with the **competence** (3.14) to conduct an **audit** (3.1) (ISO 19011:2002: 3.8)

Audit team: One or more **auditors** (3.8) conducting an **audit** (3.1), supported if needed by **technical experts** (3.10).

NOTE 1: One auditor of the audit team is appointed the audit team leader.

NOTE 2: The audit team may include auditors-in-training (ISO 19011:2002: 3.9)

Technical expert: A person who provides specific knowledge or expertise to the **audit team** (3.9).

NOTE 1: Specific knowledge or expertise is that which relates to the Organisation, the process or activity to be audited, or language or culture.

NOTE 2: A technical expert does not act as an **auditor** (3.8) in the audit team (ISO 19011:2002: 3.10).

Audit programme: A set of one or more **audits** (3.1) planned for a specific time frame and directed towards a specific purpose.

NOTE: An audit programme includes all activities necessary for planning, organizing and conducting the audits (ISO 19011:2002: 3.11).

Audit plan: A description of the activities and arrangements for an **audit** (3.1) (ISO 19011:2002: 3.12)

Audit scope: The extent and boundaries of an **audit** (3.1).

NOTE: The audit scope generally includes a description of the physical locations, organisational units, activities and processes, as well as the time period covered (ISO 19011:2002: 3.13).

Competence: Demonstrated personal attributes and demonstrated ability to apply knowledge and skills (ISO 19011:2002: 3.14).

The definitions form a very important part of the audit process and should be used a point of departure before each audit commences (ISO 19011:2002: 1-3).

ISO 19011: 2002

Section 2: Principles of auditing

ISO 19011: 2002 principles of auditing apply to the ISO 9001 quality management system and ISO 14001 environmental management system standards.

Auditing is characterised by reliance on a number of principles. These make an audit an effective and reliable tool in support of management policies and controls, providing information on which an organisation can act to improve its performance. Adherence to these principles is a prerequisite for providing audit conclusions that are relevant and sufficient and for enabling auditors working independently from one another to reach similar conclusions in similar circumstances.

The following principles relate to auditors:

Ethical conduct: the foundation of professionalism, trust, integrity, confidentiality and discretion are essential to auditing.

Fair presentation: the obligation to truthfully and accurately report audit findings, audit conclusions. Significant obstacles encountered during the audit and unresolved diverging opinions between the audit team and the auditee are reported.

Due professional care: the application of diligence and judgment in auditing. Auditors exercise care in accordance with the importance of the task they perform and the confidence placed in them by audit clients and other interested parties.

Having the necessary competence is an important factor. Further principles relate to audit, which is by definition independent and systematic.

Independence: the basis for the impartiality of the audit and objectivity of the audit conclusions. Auditors are independent of the activity being audited and are free from bias and conflict of interest. Auditors maintain an objective state-of-mind throughout the auditing process to ensure that the audit findings and conclusions will be based only on the audit evidence.

Evidence-based approach: the rational method for reaching reliable and reproducible audit conclusions in a systematic audit approach. Audit evidence is verifiable. It is based on samples of the information available, since an audit is conducted during a finite period of time and with finite resources. The appropriate use of sampling is closely related to the confidence that can be placed in the audit conclusions. The guidance given in the remaining clause of ISO 19011: 2002 is based on the principles set out above.

The above principles also play a role in helping to determine an auditor's competence to perform audits (ISO 19011:2002: 3-4).

ISO 19011: 2002

Section 3: General information on managing audit programmes

An audit programme may include one or more audits, depending upon the size, nature and complexity of the organisation to be audited. These audits may have a variety of objectives and may also include joint or combined audits.

When a quality management system and an environmental management system are audited together, this is termed a combined audit.

When two or more auditing organisations cooperate to audit a single auditee, this is termed a joint audit.

An audit programme also includes all activities necessary for planning and organising the types and number of audits, and for providing resources to conduct them effectively and efficiently within the specified time frames.

An organisation may establish more than one audit programme. The organisation's top management should grant the authority for managing the audit programme. Those assigned the authority for managing the audit programme should:

- establish, implement, monitor, review and improve the audit programme, and
- identify the necessary resources and ensure they are provided.

If an organisation to be audited operates both quality management and environmental management systems, combined audits may be included in the audit programme. In such a case, special attention should be paid to the competence of the audit team.

Auditing an environmental management system requires specific knowledge of environmental aspects and impacts. Although a quality system auditor may have the required auditor skills, they should receive specific training and evaluation for environmental issues. The same can be said for environmental auditors moving into the quality auditing realm.

Two or more auditing organisations may cooperate, as part of their audit programmes, to conduct a joint audit. In such a case, special attention should be paid to the division of responsibilities, the provision of any additional resources, the competence of the audit team and the appropriate procedures. Agreement on these should be reached before the audit commences. A best practice is to have a lead auditor controlling the audit process (ISO 19011:2002: 3-4).

ISO 19011: 2002

Section 4: Document the Audit Programme

Audit programme implementation needs to be carefully planned and then documented. The standards require certain aspects in the audit programme be documented. When an organisation prepares for its certification, the certification body auditors will need to review a number of relevant issues. The following is a list of some of the aspects that need to be considered:

- Communicating the audit programme to relevant parties;
- Coordinating and scheduling audits and other activities relevant to the audit programme;
- Establishing and maintaining a process for the evaluation of the auditors and their continual professional development;
- Ensuring the selection of audit teams;
- Providing necessary resources to the audit teams (ISO 19011:2002: 4).

ISO 19011: 2002 contains a more extensive list of descriptions and should always be reviewed before implementing the audit programme. It's better to plan for all contingencies than have to fix an issue and the audit team has to back-track.

Audit programme records

Records need to be kept of the programme implementation for the third party auditors and the organisation’s management team to review. These include all items such as:

- audit plans,
- audit reports,
- non-conformity reports,
- corrective action reports; and
- audit follow-up reports.

The audit programme also needs to be audited. This audit should be performed by an auditor that has NOT performed other audits in the programme that could possibly bias the results. Records of the audit programme review are also to be kept.

Further records that have to be kept are:

- records related to auditor competence and performance,
- audit team selection; and
- maintenance and improvement of competence.

These records should be retained and safeguarded from damage for at least three years (ISO 19011:2002: 6-9).

Audit programme monitoring and reviewing

The implementation of the audit programme needs to be monitored and reviewed to assess whether its objectives have been met and to identify opportunities for improvement. The results must be reported to top management.

Some of the performance indicators that an organisation can use include:

- the ability of the auditors to implement the individual audit plans they are assigned
- overall conformity with the audit programme and schedule; and
- feedback from audit clients, auditees and auditors.

The audit programme review should consider, for example:

- Results and trends from monitoring
- Conformity with procedures
- Evolving needs and expectations of interested parties
- Audit programme records
- Alternative or new auditing practices; and
- Consistency in performance between audit teams in similar situations.

The reviews of the audit programme can lead to corrective or preventive action and improvement of the audit programme. It is always better that the organisation finds any weaknesses in their audit programme in lieu of their 3rd party auditor finding the weaknesses, as this could result in the audit being cancelled with the resultant costs (ISO 19011:2002: 7-9)

ISO 19011: 2002

Section 5: Audit Activities Stages 1 and 2

Stages one and two of seven:

This is step 5 of 11 in the requirements set out in ISO 19011: 2002.

Step 5 covers the methods needed to conduct the physical audit from start to finish. It's important to understand the proper sequence of events for developing and implementing an internal audit process. It is also important to have a clear understanding of the definitions of the terms used. One of the most common problems found by certification auditors is an incomplete or inadequately designed and implemented internal audit programme.

When the internal audit programme is lacking proper structure and implementation, the audits usually lack meaningful results. When an organisation has a good internal audit programme and competent auditors, there should not be any unknown outcomes from the certification or surveillance audits.

Certification auditors may not always agree as to whether an issue or condition is acceptable or not. However, the issue or condition itself must never be a surprise. If the certification auditors find something that comes as a complete surprise, the internal audit programme needs to be improved (ISO 19011:2002: 11).

The following is a breakdown of Step 5:

The audit activities usually consist of seven stages:

1. Initiating the audit;
2. Conducting the document review;
3. Preparing for the on-site audit;
4. Conducting the on-site audit;
5. Preparing, approving and distributing the audit report;
6. Completing the audit; and
7. Conducting audit follow-up (ISO 19011:2002: 13-16).

Stage 1: Initiating the audit consists of the following activities:

a. Appointing the audit leader;
b. Defining audit scope, objectives and criteria;
c. Determining the feasibility of the audit;
d. Selecting the audit team members; and
e. Contacting the auditee.

Stage 2: Conducting the document review:

The majority of an auditor's time is used to review the documentation that applies to the process or processes to be audited. The auditor must have a thorough understanding of what the process's inputs, actions, outputs and measurements are.

An effective and competent auditor will not start the audit until the process documentation and records have been reviewed and any discrepancies explained or corrected. The document review should provide evidence that the process(es) has been effectively planned and methods of controlling and maintaining them are place.

The process documents/records should also show what monitoring and measuring methods are used to determine if the process(es) are effective at reaching their objectives/goals (ISO 19011:2002: 13-14)

ISO 19011: 2002

Section 6: Stage 3: Preparing for the on-site audit activities:

The audit team leader should prepare an audit plan agreement among audit client, audit team and the auditee. The plan should cover the scheduling and coordination of the audit activities. The detail provided in the audit plan should reflect the audit scope and complexity of the audit.

The details may differ, for example, between the initial and subsequent audits and also between internal and external audits. The audit plan should be sufficiently flexible to permit changes in the audit scope, which can happen as the on-site activities progress.

The plan should be reviewed and accepted by the audit client, and presented to the auditee, before the on-site audit activities begin. Any objections by the auditee should be resolved between the audit team leader, the auditee and the audit client.

Any revised audit plan should be agreed on before continuing the audit.

Process approach to auditing:

Management systems have to be audited using the process approach to auditing. Processes do not normally recognise departmental or functional boundaries. Each identified process to be audited has inputs, outputs, interactions and objectives with both qualitative and quantitative measures of its outputs. The audits have to be conducted in terms of inputs, outputs and the ability to achieve objectives. The understanding of the interaction of the processes of an organisation is a key to a successful process audit (ISO 19011:2002: 13-15).

Audit team leader

The audit team leader, in consultation with the audit team, should assign to each team member the responsibility for auditing specific processes, functions, sites, areas or activities.

The audit team members should review the information relevant to their audit assignments and prepare auditing work documents as necessary for reference and for recording audit proceedings. Such working documents may include:

- checklists and audit samplings plans; and
- forms for recording information, such as supporting evidence, audit findings and records of meetings (ISO 19011:2002: 16).

ISO 19011: 2002

Section 7: Stage 4: Conducting the on-site activities:

An opening meeting should be held with the auditee's management and process owners for the functions or processes to be audited. The purpose of an opening meeting is:

a. To confirm the audit plan;
b. To provide a short summary of how the audit activities will be undertaken;
c. To confirm communication channels; and
d. To provide an opportunity for the auditee to ask questions.

An attendance record for the opening meeting should be kept, as well as a record of topics covered and questions asked and answered.

It is during this time that the auditee gets a proper clarification of any aspect of the audit process. For example, if the audit programme classifies non-conformances as either minor or major and the auditee isn't clear on the difference, then this is the time to discuss it. It is not accepted practice to wait until the non-conformances have been written and classified and then attempt to argue the auditor out of his/her decision.

Contrary to what some auditees believe, auditors are human and can become aggravated and an angry auditor may be bad for the required end-result. It is better to clear the air amicably and ensure that a proper position is achieved with objective evidence for issues the auditor may be mistaken about or does not understand. Evidence should be gathered and presented in a professional manner. It would be ~~a~~ better if the auditor presented the situation to the auditee before the non-conformance has been written and any misunderstandings are avoided.

Opening meetings are not a mandatory internal audit activity and many organisations don't hold them. As long as everyone involved in the internal audit is clear on the methods and process to be used, an opening meeting may not be necessary, but is still a good way to get the process going.

Communication~~s~~ during the audit

Depending upon the scope and complexity of the audit, it may be necessary to make formal arrangements for communication within the audit team and with the auditee during the audit. The audit team should get together occasionally to exchange information, assess audit progress, and to re-assign work between the audit team members as needed.

During the audit, the audit team leader should periodically communicate the progress of the audit and any concerns to the auditee and audit client, as needed. Objective evidence collected during the audit that shows an immediate and significant risk (e.g. safety, environmental or quality) should be reported without delay. Any concern about an issue outside the audit scope should be noted and reported to the audit team leader, for possible communication to the audit client and auditee.

Where the available audit evidence indicates that the audit objectives are unattainable, the audit team leader should report the reasons to the audit client and the auditee to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit (ISO 19011:2002: 17-18).

Guides, escorts and observers

Guides, escorts and observers may accompany the audit team but are not a part of it. They should not influence or interfere with the conduct of the audit. However, they must protect their organisation's interests and information.

When guides are appointed by the auditee, they should assist the audit team and act on the request of the audit team leader. Their responsibilities may include the following:

a. Establishing contacts and timing for interviews;
b. Arranging visits to specific parts of the site or organisation;
c. Ensuring that rules concerning site safety and security procedures are known and respected by the audit team members;
d. Witnessing the audit on behalf of the auditee; and
e. Providing clarification or assisting in collecting information (ISO 19011:2002: 18).

Collecting and verifying information

Information and data relevant to the audit including information relating to interfaces between functions, activities and processes should be collected by appropriate

sampling and interviewing techniques and must be verified before being recorded. Only information that is verifiable may be objective evidence. All audit objective evidence should be recorded.

The audit evidence is based on samples of the available information. Therefore, there is always an element of uncertainty in auditing, and all those involved should be aware of this uncertainty (ISO 19011:2002: 18).

Generating audit findings

Objective evidence should be evaluated against the audit criteria to generate the audit findings. Audit findings can indicate conformity or non-conformity with audit criteria. In other words, findings are just relevant audit information. Findings must be determined as acceptable or not. It isn't unusual to hear an auditor that has been auditing for years to refer to a non-conformity as a finding. Non-conformities were commonly called findings when the first edition (1987) of the ISO 9000 standards came into existence (Warwick, 2011).

When specified by the audit objectives, audit findings can identify an 'Opportunity for Improvement' (OFI). An example of an OFI might be when an operation is currently functioning at a minimally acceptable level but shows signs of deterioration. The audit team should meet as needed to review audit findings at appropriate stages during the audit. If more than one auditor finds the same type of OFI in different operations the OFI may need to be elevated to a non-conformity (ISO 19011:2002: 18-19).

Preparing audit conclusions

The audit team needs to get together prior to the closing meeting to:

a. Review the audit findings against the audit objectives;
b. Agree on audit conclusions, always taking into account the uncertainty inherent in the audit process;
c. Prepare recommendations, if specified by the audit objectives; and
d. Discuss an audit follow-up, if included in the audit plan (ISO 19011:2002: 19).

Conducting the closing meeting

Many organisations do not conduct opening meetings in their internal audits. However, a closing meeting should be held. The agenda should include a list of attendees and topics presented.

A closing meeting, chaired by the audit team leader, should be held to present the audit findings and conclusions in such a manner that they are understood and acknowledged by the auditee, and to agree, if appropriate, on the time frame for the auditee to present a corrective action plan.

The people attending the closing meeting should include the auditee, and may also include the audit client and other parties. If necessary, the audit team leader should advise the auditee of problems from the audit that may affect the reliability of the audit conclusions. For example, if there were minimal audit evidence to reach a comfortable level of confidence to reach a conclusion. The evidence that was available may have appeared satisfactory, but its volume was too small.

In a small organisation, the closing meeting may consist of just communicating the audit findings and conclusions before generating and delivering the final report (ISO 19011:2002: 19).

ISO 19011: 2002

Section 8: What the auditor is looking for

The most critical factor for an auditor to record in the audit findings and report are that all conclusions must be supported by objective evidence. Objective evidence is provable and retrievable. The auditor must not present or record subjective evidence or conclusions. If it can't be verified, it can't be presented. The auditor is looking for:

- Objective evidence of compliance to procedures and work instructions; and
- Objective evidence of compliance to the ISO 9001 or other standards' requirements.

The objective evidence can consist of:

- Records;
- Documentation (work instructions, procedures, standards);
- Knowledge/training of employees from interviews; and
- Compliant product handling.

The types of non-conformances

A non-conformance, sometimes called a discrepancy or finding, is when objective evidence of non-compliance is found in relation to:

Procedures, work instructions or workmanship standards

The auditor finds objective evidence that the procedure, work instruction, workmanship standard, checklist, or specification is not being followed, (i.e. the procedure calls for keeping a record of an inspection on the traveller/router, or for signing-off on a sales order as evidence of contract review, while auditing the records the auditor finds that this not being done.)

The requirements of the standard being audited

The auditor finds objective evidence that a requirement of the standard is not met in the procedure or in the implementation of the procedure, (i.e. the procedure calls for an inspection to be made, but does not require a record of the inspection to be made, nor for the inspection/verification status on the inspected product be maintained. This is non-conformity to clauses 8.2.4 and 7.5.2 of ISO 9001. Or the orders are being shipped late without agreement from the customer, clause 7.2.2 of ISO 9001.

Customer requirements not fulfilled

This is one of the most often found non-conformances. Sometimes it is caused by product requirements not being met. However, ignoring the customers' shipping date or packaging and labelling requirements are more apt to be the reason for non-conformity.

Levels of non-conformities

Minor non-conformity: Objective evidence of deviations from the procedure's or the standard's requirements.

1. The deviation is NOT systemic (throughout the management system).
2. The deviation does NOT imply that non-conforming products are systematically shipped to the customer.
3. The deviation does NOT imply that non-conforming products are KNOWINGLY shipped to the customer.

Major non-conformity: Objective evidence of deviations from the procedure's or the standard's requirements.

1. The deviation IS systemic (throughout the management system). For example, a requirement is not addressed anywhere in the management system.
2. The deviation implies that non-conforming products ARE systematically shipped to customers.
3. The deviation implies that a non-conforming product IS knowingly shipped to customers.

ISO 19011: 2002

Section 9: Audit Activities Stage 5: Preparing, approving and distributing the audit report

The audit report is generally the final stage in the audit activities. It is prepared after the closing meeting where the audit conclusions were presented and agreed to. All items from the closing meeting should be in the audit report. This reinforces the need to keep minutes of the opening and closing meetings.

Technically, if an audit conclusion is not shown in the audit report, it didn't happen. If the organisation's procedures call for the auditor or audit team to oversee any corrective actions required due to audit non-conformances, the audit report should include a statement to that effect (ISO 19011:2002: 20).

Preparing the audit report

The audit team leader should be responsible for the preparation and contents of the audit report. The audit report should provide a complete, accurate, concise and clear record of the audit, and should include or refer to the following:

a. The audit objectives;
b. The audit scope, particularly identification of the organisational and functional units or processes audited and the time period covered;
c. Identification of the audit client;
d. Identification of the audit team leader and members;
e. The dates and places the on-site audit activities were conducted;
f. The audit criteria;
g. The audit findings; and
h. The audit conclusions.

The audit report may also include or refer to the following, where appropriate:

a. The audit plan;
b. A list of the auditee representatives;
c. A summary of the audit process, including the uncertainty and/or obstacles encountered that could decrease the reliability of the audit conclusions;
d. Confirmation that the audit objectives have been accomplished within the audit scope in accordance with the audit plan;
e. Any areas not covered, although they are within the audit scope;
f. Any unresolved diverging audit opinions between the audit team and the auditee;
g. Recommendations for improvement, if specified in the audit objectives;
h. Agreed follow-up action plans, if any;
i. A statement of the confidential nature of the audit contents; and
j. The audit report distribution list (ISO 19011:2002: 20).

Approving and distributing the audit report

The audit report should be issued within the agreed time period. If this is not possible, the reasons for the delay should be communicated to the audit client and the new issue date should be agreed upon.

The audit report should be dated, reviewed and approved in accordance with the audit programme procedures.

The approved audit report should then be distributed to recipients designated by the audit client, and maintain the confidentiality of the report (ISO 19011:2002: 20-21).

ISO 19011: 2002

Section 10: Auditing techniques include:

- Observation of evidence and operations,
- Interviewing auditee personnel,
- Verifying the audit finding; and
- Recording the findings and non-conformances.
- Tell me/show me:

This technique is one of the most effective in conducting audits. The auditor simply requests the auditee to explain or walk him/her through the activity or operation being audited. Questions need to be open-ended and precise. Open-ended questions are seen as less adversarial than closed-ended questions such as: “Why do you do the job this way?” or worse “Is this the way you are supposed to do this job?”

In the course of the research a series of more focused questions were formulated by the researcher that are recommended to be posed to respondees when doing such an audit in an organisation/company:

Reformulated audit questions:

- Tell me how you conducted this operation?
- Tell me how you make sure that this operation is effective?

- Tell me what the inputs to the process are?
- Tell me what the process outputs are?
- Tell me how the outputs link to other operations/processes?
- Tell me what the objectives of the operation are?

In addition to closed-ended questions being somewhat adversarial but also limiting in what information can be provided, they do not include the opportunity for the interviewee to answer more than ‘yes’ or ‘no’. Therefore, they don't inherently contain the opportunity for the auditor to learn anything about the operation except ‘yes’ or ‘no’. It is also common for organisations to sometimes have instructed their staff to "answer the auditor's question and then keep quiet". So, when a closed-ended question is asked, it should not come as a surprise if a ‘closed-ended’ answer (i.e. short and cryptic information) is given.

The next step is to compare the information gathered with:

- Procedures;
- Instructions;
- Standards;
- Forms;
- Checklists;
- Computer system entries; and/or
- Actual operation.

Examples of auditing questions for this phase of the audit are:

- Show me the workmanship standard or procedure you use for this job.
- Show me how you monitor/measure the operation.
- Show me how your objectives/requirements are defined.

The next step is to verify how the processes are operated consistently by looking at objective evidence of compliance such as:

- Records;
- Employee knowledge; and
- Compliant product handling (ISO 19011:2002: 21-25).

ISO 19011: 2002

Section 11: Audit Path

The audit path is the sequence of activities or personnel to be audited. A keen selection of the audit path is critical to a successful audit and should be conducted using a description of the interaction between the processes of the QMS (Quality Management System).

The important factors for this selection are:

Audit scope: The activities in the audit path have to be within the audit scope and need to ensure full coverage of all areas and operations to be audited.

Availability of the auditee: The auditee needs to be available and auditable at the scheduled time.

Activity/process flow: The sequence of activities to be audited should be based on a description of the interaction between the processes and the QMS. This will ensure effective auditing of various processes, enable a better comprehension by the auditor and facilitate the communications between auditor and auditee.

For audits requiring more than one auditor, the audit schedule will need to reflect multiple audit paths. Each auditor will have his/her own set of activities and processes to audit a specific path. The different paths can overlap in the areas where the activity requires more than one auditor to achieve a proper sampling within the given time frame.

The paths should also be selected according to auditor's expertise. For example, an auditor with a strong engineering background should focus on the engineering processes such as process and product design, floor plan layout and workflow.

At a predetermined time during the audit, the auditors need to meet and exchange information and notes based on observations made in their specific audit path. This is necessary to evaluate the level of non-conformities, if any.

If all the auditors found the same type of non-conformity in their audit paths, it will indicate that the non-conformity is systemic and is therefore major. They also need to co-ordinate audit activities for interacting processes, by exchanging information on the outputs of processes that may be inputs for other processes (ISO 19011:2002: 19).

ISO 19011: 2002

Section 12: Effective Communications

Effective communication depends on the psychology of the auditee and psychology is an extremely important factor in the success of the audit. Failure to communicate effectively by taking into account the psychology of the auditee can actually yield to degradation rather than improvement of an activity or process. This is primarily because of resentful or disgruntled auditees.

Example of some proper actions from section 12 of ISO 19011: 2002:

- Evaluate the auditee's attitude to see how receptive he/she is to the audit;
- Evaluate the situation to see whether the auditee is not in an uncomfortable position during the audit (i.e. be watched and scrutinised by his/her boss while being audited);
- Evaluate how the auditee perceives you in view of previous audits or professional relationships;
- Make the auditee comfortable by adopting an attitude, taking ~~an~~ action or making positive statements that will help diffuse any possible tension detected from the issues listed above;
- Ask open-ended questions and listen;
- Control the interview and make sure the auditee does not lead the interview;
- Manage your time in order to achieve the goal of the audit within the allotted time period, but be prepared to let the auditee talk as much as he/she wants as long as they stay on the topic; and
- Make sure the auditee understands this is not a personal audit, but an audit to determine how good the processes and system address requirements are (ISO 19011:2002: 18).

The following are some of the do's and don'ts of auditing:

Do’s:

- Show interest;
- Remove or reduce distractions;
- Be empathic but, not sympathetic (appear biased);
- Be patient;
- Ask concise and exact questions; and
- Focus on the customers’ organisation and the standards requirements.

Don'ts:

- Judge or be negative;
- Lose focus;
- Lose track of original question;
- Interfere with auditees’ thoughts/answers; and
- Hear what you want to hear (ISO 19011:2002: 22)

ISO 19011: 2002

Section 13: Sampling

The ISO definition of sampling is:

> The act, process or technique of selecting a suitable sample; specifically: the act, process or technique of selecting a representative part of a population for the purpose of determining parameters or characteristics of the whole population. For audits it is a technique used in order to collect sufficient objective evidence to determine whether a process or system is in compliance or has nonconformities to the standard (ISO 19011:2002: 16).

Examples of a sampling population for an audit could include members of an auditee’s organisation, or records for review.

Looking at all the records or interviewing every employee is very often not possible because of time and resource constraints on the audit team. Therefore,

representative samples of employees are interviewed and representative samples of records are reviewed.

The sample size selection is very subjective. The following guidelines are recommended:

- Take an initial random sample of 15: 25% of the records that needs to be reviewed. Lower sample sizes are used when the number of records is larger.

- If the records are generated primarily through an automated computer process, a smaller sample size is acceptable. Chances are, if the sample being reviewed is conforming, the remainder of the population generated by the system, this would also be acceptable. The same holds true if the sample is non-conforming.

- If the records show objective evidence of compliance, the observation can be made that there is objective evidence of compliance. A description of the reviewed sample document should be noted. If possible, the records should be initialled in an inconspicuous place.
- If the initial sample shows objective evidence of non-compliance, an additional 10-15% random sample should be taken to determine the severity of the non-conformity.

For the number of employees to interview/audit, the same percentage sampling guidelines are normally applied (ISO 19011:2002: 16-19).

ISO 19011: 2002

Section 14: Audit completion and follow-up

Audit completion

The audit is completed when all activities described in the audit plan have been carried out and the approved audit report has been distributed.

Documents pertaining to the audit should be retained by agreement between the participating parties and in accordance with audit programme procedures and applicable statutory, regulatory and contractual requirements.

If the organisation is registered/certified to one or more of the international standards, such information must be retained with the audit records. Audit records must be available for third-party auditors to review for compliance to the standard's requirements and effectiveness of the audit process. Audit results are also required to be reviewed at the management review meetings as they are a valuable input for continual improvement.

Unless required by law, the audit team and those responsible for managing the audit programme should not disclose the contents of documents, or any other information obtained during the audit or the audit report to any other party without the explicit approval of the auditee. If disclosure of the contents of an audit document is required, the audit client and auditee should be informed as soon as possible (ISO 19011:2002: 6.5.4: 18-19).

Conducting audit follow-up

The conclusions of the audit may indicate the need for corrective, preventive or improvement actions. These actions are usually decided and undertaken by the auditee within an agreed time frame and are not considered to be part of the audit. The auditee should keep the audit client informed of the status of these actions.

The completion and effectiveness of corrective action must be verified. This verification may be part of a subsequent audit. The audit programme may specify follow-up by members of the audit team, which adds value by using their expertise. In such cases, care should be taken to maintain independence in subsequent audit activities.

The auditor or audit team members should not be involved in developing or implementing any corrective actions for non-conformances arising from an audit they conducted. Involving oneself in corrective actions gives the impression of ownership. Ownership involves bias (ISO 19011:2002: 6.5.4: 19-21).

ISO 19011: 2002

Section 15: Auditor competence and evaluation

General

Auditor competence is important in order to have confidence and reliance in the audit process. This competence is based on the demonstration of:

- The auditor's personal attributes; and
- The ability to apply the knowledge and skills gained through the education, work experience, auditor training and auditing experience.

Auditors develop, maintain and improve their competence through continual professional development and regular participation in audits. A process for evaluation of auditors and audit team leaders should be implemented (ISO 19011:2002: 6.5.4: 21-22).

Personal attributes

Auditors should possess personal attributes to enable them to act in accordance with the principles of auditing described in Section 2 of the discussion of ISO 19011: 2002.

An auditor should be:

1. **Ethical,** (i.e. fair, truthful, sincere, honest and discreet);
2. **Open-minded,** (i.e. willing to consider alternative ideas or points of view);
3. **Diplomatic** (i.e. tactful in dealing with people);
4. **Observant** (i.e. actively aware of physical surroundings and activities);
5. **Perceptive** (i.e. instinctively aware of and able to understand situations);
6. **Versatile** (i.e. adjusts readily to different situations);
7. **Tenacious** (i.e. persistent, focused on achieving objects);
8. **Decisive** (i.e. reaches timely conclusions based on logical reasoning and analysis); and
9. **Self-reliant** (i.e. acts and functions independently while interacting effectively with others) (ISO 19011:2002: 6.5.4: 22).

Knowledge and skills

Auditors should have generic knowledge of quality management systems and environmental management systems. Auditors should have knowledge and skills in the following areas:

Audit principles, procedures and techniques to enable the auditor to apply those appropriate to different audits and ensure that audits are conducted in a consistent and systematic manner. An auditor should be able to:

- apply audit principles, procedures and techniques;
- plan and organise the work effectively;
- conduct the audit within the agreed time schedule;
- prioritise and focus on matters of significance;
- collect information through effective interviewing, listening, observing and reviewing documents, records and data;
- understand the appropriateness and consequences of using sampling techniques for auditing;
- verify the accuracy of collected information;
- confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;
- use working documents to record audit activities;
- prepare audit reports;
- maintain the confidentiality and security of information; and
- communicate effectively, either through personal linguistic skills or through an interpreter (ISO 19011:2002: 6.5.4: 22-24).

Management system and reference documents

Management system and reference documents to enable the auditor to comprehend the scope of the audit and apply audit criteria are required. The knowledge and skills in this area should cover the following:

- the application of management systems to different organisations;
- interaction between the components of the management system;
- quality or environmental management system standards, applicable procedures or other management system documents used as audit criteria;

- recognising differences between and priority of reference documents;
- application of the reference documents to different audit situations; and
- information systems and technology for authorisation, security, distribution and control of documents, data and records (ISO 19011:2002: 6.5.4: 23).

Organisational situations

Organisational situations to enable the auditor to comprehend the organisation's operational context. Knowledge and skills in this area should cover:

- organisational size, structure, functions and relationships;
- general business processes and related terminology; and
- cultural and social customs of the auditee (ISO 19011:2002: 6.5.4: 23).

Applicable laws, regulations and other requirements relevant to the discipline to enable the auditor to work within, and be aware of, the requirements that apply to the organisation being audited. Knowledge and skills in this area should cover:

- local, regional and national codes;
- laws and regulations;
- contracts and agreements;
- other requirements to which the organisation subscribes (ISO 19011:2002: 6.5.4: 23).

Generic knowledge and skills of audit team leaders

Audit team leaders should have additional knowledge and skills in audit leadership to facilitate the efficient and effective conduct of the audit. An audit team leader should be able to:

- To plan the audit and make effective use of resources during the audit;
- Represent the audit team in communications with the audit client and auditee;
- Organise and direct audit team members;
- Provide direction and guidance to auditors-in-training;
- Lead the audit team to reach the audit conclusions;
- Prevent and resolve conflicts; and
- Prepare and complete the audit report (ISO 19011:2002: 6.5.4: 24).

Specific knowledge and skills of QMS auditors

QMS auditors should have knowledge and skills in the following areas:

a. Quality-related methods and techniques to enable the auditor to examine quality management systems and to generate appropriate audit findings and conclusions. Knowledge and skills in this area should cover:

- quality terminology;
- quality management principles and their application; and
- quality management tools and their application (for example statistical process control, failure mode and effects analysis, etc.).

b. Processes and products, including services to enable the auditor to comprehend the technological context in which the audit is being conducted. Knowledge and skills in this area should cover:

- sector-specific terminology;
- technical characteristics of processes and products, including services; and
- sector-specific processes and practices (ISO 19011:2002: 24).

Specific knowledge and skills of EMS auditors:

Environmental Management System (EMS) auditors should have knowledge and skills in the following areas:

a. Environmental management methods and techniques to enable the auditor to examine environmental management systems and to generate appropriate audit findings and conclusions. Knowledge and skills in this area should cover:
   - environmental terminology;
   - environmental management principles and their application; and
   - environmental management tools (such as environmental aspect/impact evaluation, life cycle assessment, environmental performance evaluation, etc.).

b. Environmental science and technology to enable the auditor to comprehend the fundamental relationships between human activities and the environment. Knowledge and skills in this area should cover:

- the impact of human activities on the environment;
- interaction of ecosystems;
- environmental media (e.g. air, water, land);
- management of natural resources (e.g. fossil fuels, water, flora and fauna); and
- general methods of environmental protection.

c. Technical and environmental aspects of operations to enable the auditor to comprehend the interaction of the auditee's activities, products, services and operations with the environment. Knowledge and skills in this area should cover:

- sector-specific terminology;
- environmental aspects and impacts;
- methods for evaluating the significance of environmental aspects;
- critical characteristics of operational processes, products and services;
- monitoring and measurement techniques; and
- technologies for the prevention of pollution (ISO 19011:2002: 26-27).

6.3 APPLICATION OF AUDIT QUESTIONS TO THE CASE STUDY

The updated standard, ISO 19011:2011 has been published. The new standard gives fuller descriptions of audit processes for more specific audit environments than just a generic process. This will ensure that the quality of audits is enhanced for first, second and third party audits. At the time of the research, ISO 19011:2011 was only available in FDIS format.

The methodology of the ISO 19011:2002 process as described in this chapter, forms the basis of any audit that is undertaken of any ISO Management System. The same principles applied to the Case Study where many, but not all the questions and processes were carried over into the Maturity Model. Furthermore, the researcher is a RABQSA (Registrar Accreditation Board Quality Society of Australasia) qualified Business Improvement Auditor, Lead Auditor and Skills Examiner on the ISO 28000 Series of standards and has had to write international exams on the ISO 19011:2002

guidelines to qualify for these certifications. He has also concluded the Lead Auditor Training on the *ANSI/ASIS SPC.1-2009*: Organisational Resilience Management Standard which uses the same audit guidelines for that standard.

CHAPTER 7
CASE STUDY: IMPLEMENTATION OF AN ORGANISATIONAL RESILIENCE MANAGEMENT SYSTEM USING A MATURITY MODEL

7.1 INTRODUCTION

This Case Study, dealing with the implementation of an organisational resilience management system using a Maturity Model, is based on the guidelines (as outlined in previous chapters) of the standards setting document: *ANSI/ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with guidance for use.* The Case Study also formed the basis of an ongoing risk management project implemented by the South African based Tsogo Sun Group (TSG). The project was started at their South African business operations in preparation for the FIFA Soccer World Cup held in South Africa in June-July 2010. Subsequent to the completion of the tournament it was rolled out at their other properties in Africa, the United Arab Emirates (UAE) and the Seychelles. Tsogo Sun Group is presently the biggest hotel group in Africa. TSG owns ninety hotels in seven countries, 14 casinos, a convention centre and a theme park. Tsogo Sun Group granted the researcher permission to use the name of their organisation in this document, as well as to report on the findings of the implementation of the Case Study at their South African sites.

Tsogo Sun Group made a decision in October 2009 to embark on this project. TSG wanted to evaluate and strengthen, where necessary, their existing preparedness efforts and increase their resilience in preparation for the FIFA Soccer World Cup and the expected large number of supporters from overseas. TSG wanted to implement the ORMS programme in all the main centres, as well as those parts of the country that normally draw large numbers of tourists, where it has a presence. The initial stage would only be for the South African properties. With the world watching such a high-profile event, TSG wanted to ensure they were prepared for the many risk issues that might present challenges to their hotels and resorts. The ORMS project became an even greater opportunity for them as TSG had been selected as the accommodation provider for the “FIFA Family” (all the VIPs and senior officials). It thus became critical for them to ensure that a well-structured Organisational

Resilience plan was in place in the event of any emergencies or disasters occurring during the FIFA event.

The hotel group also considered using ISO 28000, the International Organisation for Standardisation's Security in the Supply Chain Standard and BS 25999, the British Standard for Business Continuity Management (BCM). In October 2009 TSG were introduced by the researcher to the *ANSI/ASIS SPC.1-2009: Organisational Resilience: Security, Preparedness and Continuity Management Systems Standard,* which had been developed using the ISO management systems foundation for standards (ANSI/ASIS, 2009: vii).

In the months leading up to the decision to rather go the Organisational Resilience route, TSG had completed a full review to check the implementation and functioning of their Business Continuity Plans (BCPs). They had decided that it did not make sense to implement two different standards. There was neither the time nor an immediate budget available to do a full roll-out of the ORMS throughout the group and it was decided to identify some of the more critical venues and develop the programme around these units.

Top management of TSG, valuing the balance of business decision-making options and the inclusion of the various risk-centred preparedness requirements in the standard, accordingly opted for the full implementation of *ANSI/ASIS SPC.1-2009*. The decision to implement it allowed TSG to cover many more risk elements than just one aspect of a single standard such as either ISO 28000 or BS 25999. The decision to use *ANSI/ASIS SPC.1-2009* instead provided a more comprehensive risk management approach to security, emergency response, crisis preparedness, disaster management, continuity management, as well as occupational health and safety requirements. To get the process going the decision to use the *ANSI/ASIS SPC.1-2009 (*ORMS standard) was taken in late October 2009 with a final implementation date of 31 May 2010 being set. Accordingly the schedule was very tight for completion before the start of the FIFA Tournament in June 2010.

This was the first global effort where the standard was implemented in practice. This meant that close attention was given to the processes that were used, as well as the

identification of methodologies to refine existing business processes and systems, including having to develop plans to change a number of fixed mind-sets within the organisation. Some individuals have difficulty with accepting change and they had to be convinced that a change would probably be beneficial to the manner in which they do business and protect the assets that they are accountable for. Being a management system, the *ANSI/ASIS SPC.1-2009* ORMS is based on the Plan-Do-Check-and-Act (PDCA) model as initially discussed in Chapter 3. A number of organisations, including the United Nations, have subsequently started implementing and developing audits based on this Standard while using the Maturity Model as the foundation or starting point (Sobon, 2011).

The researcher, a Senior Partner of Temi Group, was engaged as the Lead Consultant to initiate the project plan and to develop the evaluation and implementation process. Selling a totally unknown and untested system to a major corporation had its challenges. However, top management had the vision to see that the system would allow for the coverage of a cross-section of risk elements under the control of a single management standard.

In this chapter an outline is given of this specific implementation and some of its processes. The confidentiality agreement that was entered into with TSG to protect their intellectual property must be respected and thus will not allow for going into specific detail in respect of some of the operational documents (intellectual property).

7.2 BACKGROUND

In the initial discussions with Dr Gert Cruywagen, Group Director of Risk at TSG and two senior managers, Colin Ackroyd, Risk Manager for the TSG Hotel Group and Naresh Ramdhaney, Risk Manager for the TSG Gaming Operations, it had been arranged that they were to develop the initial implementation plan for discussion with the TSG Executive Board. It was evident that before the next steps could be taken, there were a few practical decisions that had to be taken.

The first of these was the TSG decision not to pursue third-party certification due to the time and cost involved. This decision was also based on the fact that TSG did not have a business case for doing costly external third-party certification. Instead, the

hospitality group resolved to do its own rigorous internal assessment of the implementation of the standard. To that end, TSG selected four people to form a team[2] with two consultants from the Temi Group to undergo Lead Auditor training in both the ISO 28000: 2007 standard based on the Security Management System as certified by the USA/Australian certification body, RABQSA,[3] as well as the *ANSI/ASIS SPC.1-2009* Standard. In early December 2009 Dr Marc Siegel, Commissioner, Global Standards Initiative at ASIS International, USA provided the team with ten days of training on the standard.

The main objective of the training being to provide the team with a thorough understanding of the standards and assist them in developing the internal auditing protocol to ensure that the operational objectives were met by the target date of 31 May 2010. The courses were completed by 15 December 2009. The decision to conduct an internal evaluation of the project was significant. According to Marc Siegel, "the company is setting up an internal mechanism that will have the same credibility and the same weight as if someone did it externally" (Berrong, S., 2010: 52).

7.3 DEVELOPMENT OF THE ORMS MATURITY MODEL

On completion of the ISO 28000 and ORMS Lead Auditor Course while trying to identify the audit methodology that would be used in the ORMS implementation at TSG, it became clear that the available audit protocols would not allow for a group wide achievement of a system that would be fully functional while not as complex and costly as normal third party auditing. To achieve the ORMS implementation objectives as required by TSG under the normal implementation and audit system would take years to cover all the business units in the group. The expense would not be worth the effort due to changes that will occur under normal business operational conditions

[2] The team consisted of Colin Ackroyd (TSG-Hotels), Giel Burger (TSG-Hotels), David Croft (TSG-Hotels, Inter-Continental Sandton), Naresh Ramdhaney (TSG-Gaming), Raymond van Staden (Temi Group-SA) (now deceased) and the researcher as the Lead Consultant.

[3] RABQSA is an Australian personnel and training certification body. RABQSA was created in 2004 from the acquisition of the personnel certification activities of United States of America-based Registrar Accreditation Board (RAB) by Australia-based Quality Society of Australasia (QSA). RABQSA's activities are to design, develop, and deliver personnel and training certification services for various industries (RABQSA:2012).

and that the process would have to be restarted time-and-again to keep up with the changes that would have to be updated and then re-audited.

As a result of discussions that took place between the researcher, Dr Siegel, Colin Ackroyd and later Dr Cruywagen it was decided that a Maturity Model would be the best option to achieve the required goals as set by TSG within the allocated time. A Maturity Model would also be easier to keep the staff involved as it is a participative programme at all levels and would have a much better chance of success. The problem was that no such Maturity Model existed for ORMS. Dr Siegel was tasked to develop the Maturity Model based on his experience in the development and required outcomes from standards writing and implementation. He undertook to develop the Maturity model within a six week period so that it would be available for use towards the end of January 2010.

The advantage of the Maturity Model was that it would be a phased approach and business units could work at their own pace. It could also be implemented at and to specific levels at the different brands within TSG. TSG agreed with this approach and financed the development of the Maturity Model for ORMS.

Dr Siegel spent the next four weeks developing the ORMS Maturity Model and, as promised, submitted a draft in the middle of January 2010. The draft Maturity Model was reviewed by the researcher, Colin Ackroyd and Giel Burger. The purpose was to see what documentation and processes would be necessary to achieve tangible results that could be measured in financial terms. The ORMS Maturity Model presented six levels of implementation.

One of the challenges in the formulation was converting a generic standard and customising it for use by the hospitality industry. An important lesson learnt was the need to engage people in the process, since buy-in from all levels was the key to achieving the required results. The phased approach taken by TSG provided a manageable path for implementation.

During further discussions with Dr Cruywagen and his team and teaching them the levels and requirements of the ORMS Maturity Model, it was decided that as there

was already an acceptable base level in TSG to work from, all TSG facilities would start at Level 3. It was also decided that if the five–star units were ready, that they could be audited up to Level 4, but would have to first achieve Level 3.

This process would allow an evaluation process for TSG to achieve and implement the following actions and obtain the requisite results, namely:

- Evidence the risk management work already in place.
- Refine existing Risk Management processes.
- Align existing standards and internal standard operating procedures to more easily measurable levels.
- Reinforce the confidence of all stakeholders in the organisation's ability to provide the necessary resources to deal with and recover from disruptive incidents. Stakeholders include shareholders, staff, customers, suppliers and the community.
- Provide the organisation with an objective and consistent tool to measure risk compliance; an initial snapshot and in the long term.
- Prove that the organisation meets or exceeds international best practice.
- Provide a standard that all role players will understand and know what the expectations are.
- Allow management to decide what level of compliance they wished to achieve and maintain.

7.4 DEVELOPMENT OF THE PROJECT PLAN

The first step for the team was to develop an ORMS Implementation Action Plan so that there were guidelines to follow. The Action Plan would also give TSG executives an implementation framework to which the Project Team would deliver. The plan was not all-encompassing but was adequate for the successful delivery of the project. The budget was drawn up in a separate document. The following ORMS Implementation Action Plan table is an example of the initial project plan for this implementation. The plan was accepted by TSG and gave guidance for the deliverables.

Table 4: ORMS IMPLEMENTATION ACTION PLAN

ORGANISATIONAL RESILIENCE IMPLEMENTATION ACTION PLAN					
PROJECT OWNER: TSOGO SUN GROUP: RISK MANAGEMENT DEPARTMENT CONSULTANCY AND IMPLEMENTATION ASSISTANCE: TEMI GROUP					
ITEM NO	**ELEMENT**	**ACTIVITY**	**NOTES**	**ACCOUNTABLE PERSON(S)**	**RETURN DATE**
1	**Communication**				
1.1	Internal	Internal memo to be developed and distributed company wide.			
1.2	Communication: Unit specific	Explanation of Organisational Resilience and intention			
1.3	Public Announcement	Media Release.			
1.4	Policy statement	From CEO			
1.5	Management Statement of Intent	From unit GM to their staff			
2	**Develop organogram of responsible people who will initially support the project**	Unit GM assisted by HO - Hotels by position - Casinos by name			
3	**Develop Project Plan**	Tsogo HO and Temi Group			
4	**Analysis of current systems and processes (GAP Analysis)**	Establish existing baseline			
4.1	Establishment of documentation	Identify documents and prepare index, including but not limited to identification and prioritising to assets and related risks.			
4.2	Review, design and development	Identify non-relevant and industry specific elements - Remove non-relevant sections of the Standard - Add missing items specific to industry (Hotel/Gaming)			
5	**Identify primary sites**	Sites identified. See Addendum “A”			
6	**Training the people involved**	Continuation training on OR			
7	**Risk Assessment and Impact Analysis**	Conduct Risk Assessments at pilot sites and then review 1 Hotel and 1 Casino before full roll-out			
8	**Formalise initial Standard document**	Refinement of Maturity Model			
9	**Implementation of the System at primary sites and Initiate audits at primary sites**	Sites identified and awaiting ratification. See Addendum “A”			
10	**Ratings and corrective actions**	Remedial actions as required or highlighted from 9 above			

	(PDCA)				
11	**Final audit if required**	Audit visits			
12	**Issue Certification (Level dependent)**	1. Develop Certificates to be presented to the units 2. Assess results and issue certificates.			
13	**Operation of the System**	Ongoing (PDCA)			
14	**Improvement of system and documentation**	Ongoing (PDCA)			
15	**Maintenance of the system**	Ongoing (PDCA)			

ADDENDUM "A"					
INITIAL FACILITIES TO BE AUDITED					
HOTELS	**PROPOSED AUDIT DATES**	**RESPONSIBLE PEOPLE**	**GAMING**	**PROPOSED AUDIT DATES**	**RESPONSIBLE PEOPLE**

The column named "Items" is the list that was used as a framework. The column named "Reference Point" was used to give an indication what documentation or activity was required. The others are self-explanatory. The first page has got some columns filled in under the 'Activity' header to serve as an example.

Table 5: Organisational Resilience: Planning phases

Organisational Resilience: Planning Phases						
Project Outline						
Item	**Reference Point**	**Action**	**Respon. Person**	**Est. Time**	**Est. Start**	**Est. End**
1.Initiation						
ID of Teams		Y	CDE			
Appointment of Team Leader		Y	CDE			
Appointment of Team		Y	CDE			
Appointment of Technical Consultants		WIP				
Set up communications protocols		Y				
Schedule for Team meetings		WIP				
Set up document control system		WIP				
Sign NDA: All Team members		Y				
Schedule of activities	Document. Revised as required	Y	ABC	1 Week	21/09/11	27/09/11
2.Policy Document						
Produce actual document for Executive (Group & Business Units)	HQ driven					
Print and have it signed	HQ driven					
Distribute to Top Management, Ops Directors and Business Unit GMs	HQ driven					
3.Scope (Generic)						
Objectives						
Define Context						
Internal						
External						
Risk Criteria						
Legal Obligations						
Identification of critical paths						
ID business mission						
Assets						
Functions						
Services						
Products						

Item	Reference Point	Action	Respon. Person	Est. Time	Est. Start	Est. End
4.Planning: Define Risk Assessment Methodology						
Scope of Risk Assessment						
ID of Role Players						
Documentation procedure						
Establish risk criteria						
Support documents for risk ID						
Risk Analysis: What process and format is going to be used?						
Risk Assessment Logistics						
5.Conduct Risk Assessment						
Risk Assessments						
Conduct the procedures for risk identification						
Conduct the procedures for risk analysis						
Conduct risk evaluation: GAP Analysis						
Prioritising the risk to determine the risk treatments						
Cost benefit analysis						
Prioritise the above						
Define risk treatments objectives						
Define targets and time frames						
Programmes						
Resources						
Manpower						
Champion for specific elements						
Administration						
Technologies						
Function						
Procedures						
Training						
Procedures						
Systems upgrade						
Redesign						

Item	Reference Point	Action	Respon. Person	Est. Time	Est. Start	Est. End
6.Implementation Phase						
Measure against risk assessment						
Select an “easy win”						
Empowerment of staff						
Develop missing procedures						
Document additional procedures as required						
Define roles and responsibilities						
Define competencies						
Develop training to achieve competencies						
Develop additional procedures to deal with emergencies						
Communications procedures						
Documentation control						
ID additional resources						
7.Performance evaluation						
How is performance going to be evaluated?						
Define measurement success						
Simulation exercises						
8.Audit						
Audit of the system and performance						
Risk management system performance						
Corrective actions						
Preventative actions						
Re-measurement						
Third Party Certification (If required) - Phase 1						

Item	Reference Point	Action	Respon. Person	Est. Time	Est. Start	Est. End
9.Checking and Corrective Action						
Measurement of success						
Define measurement of improvement and list						
Review performance						
Evaluate performance						
Evaluate audit results						
Conduct new risk assessment if required						
Identify corrective and preventative actions						
Identify opportunities for improvement						
Determine next round of priorities						
10.Certification						
Issue certificates for appropriate level achieved						
Actions: Y = Completed; N = Not completed; WIP = Work-in-progress						

7.5 SELF-ASSESSMENT SCORECARD/CHECKLIST

The initial Self-Assessment Scorecard/Checklist as developed by ASIS International, (Appendix 'G': ASIS Self-Assessment Scorecard/Checklist) was found to be inadequate for this project. The Self-Assessment Checklist formed part of the initial programme of resilience assessment and organisational capacity during the training, before it was decided to develop the Maturity Model. It was seen as a tool for the organisation to continually refer to and check if all its procedures and systems were adequate when measured against the ORMS Standard.

The Self-Assessment Checklist covered all the requirements as measured against the ORMS standard but was still lacking as an adequate tool although it did give management an overall view of where their organisation was on the grid to becoming resilient.

The Maturity Model, however, gave the assessment process a much better structure so that the organisation could start at an acceptable level and then grow into a more resilient organisation.

The Self-Assessment Checklist consists of a number of sections which in turn are based on the ORMS Standard.

The headers that are mapped out in the Self-Assessment Checklist are indicated here below. One can see that the numbering is aligned to the Project Plan that was developed for the TSG project.

4.1.1 Define Scope of ORMS;
4.2.1 Policy;
4.2.2 Management Commitment;
4.3.1 Risk Assessment and Impact Analysis;
4.3.2 Legal and Other Requirements;
4.3.3 Objectives, Targets and Programmes;
4.4.1 Resources, Roles, Responsibility and Authority;
4.4.2 Competence, Training and Awareness;
4.4.3 Communication and Warning;
4.4.4 Documentation;

4.4.5 Control of Documentation;

4.4.6 Operational Control;

4.4.7 Incident Prevention, Preparedness and Response;

4.5 Checking;

4.5.1 Monitoring and Measurement;

4.5.2.1 Evaluation of Compliance;

4.5.2.2 Exercises and Testing;

4.5.3 Nonconformity, Corrective Action and Preventive Action;

4.5.4 Control of Records;

4.5.5 Internal Audits;

4.6 Management Review;

4.6.4 Maintenance; and

4.6.5 Continual Improvement,

The headers flow through from the initial development of the policy through to the implementation cycle and auditing process. Lastly it comes to the point in the PDCA (Plan-Do-Check-Act) cycle where it addresses maintenance and continual improvement.

The document is self-explanatory as to each of the sections and what is required to ensure a satisfactory audit while implementing to the requirements of the Maturity Model.

The ASIS developed Self-Assessment Scorecard (Appendix 'G') has merit in doing a self-evaluation as it covers all the areas that are required to assess if an organisation has, or has not met the criteria as required in the standard. It also shows where the organisation stands at the time of measurement and what work still has to be done to get the programme to an acceptable level. The ASIS Self-Assessment Scorecard was not used in the TSG project. TSG only used the Maturity Model for ORMS.

7.6 USING THE MATURITY MODEL

The Maturity Model used and implemented by TSG provided a more efficient base to work from for the following reasons:

7.6.1 Value Maturity Model

7.6.1.1 A place to start;

7.6,1.2 Benefit from prior experiences and lessons learned;

7.6.1.3 A common language and a shared vision;

7.6.1.4 A framework for prioritizing actions;

7.6.1.5 Links between cost and value added;

7.6.1.6 A way to establish achievable and maintainable goals within resource constraints; and

7.6.1.7 A means to define what continual improvement means for the Organisation.

7.6.2 Structured design steps

7.6.2.3 Evaluate the current situation with regard to preparedness and resilience management;

7.6.2.4 Set goals to be achieved;

7.6.2.5 Benchmark present situation relative to the goals;

7.6.2.6 Plot a sensible business path to get there; and

7.6.2.7 Achieve a balance between business needs, time and financial constraints.

7.6.3 Commitment to achieving the goals

7.6.3.3 Determine the approach that fits the business model;

7.6.3.4 Focus on what is cost-effective and objective effective;

7.6.3.5 Consider a phased approach to build momentum; and

7.6.3.6 Build on success to promote cultural change.

7.6.4 Promoting cultural change

7.6.4.1 Helps develop the momentum needed to encourage persons to manage their risks by seeing clear benefits of their participation;

7.6.4.2 By carefully setting objectives and targets to maximize chances of early success, it is possible to stimulate top management support and acquire the needed resources; and

7.6.4.3 Publicizing and recognizing success breeds the necessary levels of enthusiasm and credibility throughout the Organisation to move from phase to phase.

7.6.5 Building the Recognition Programme

7.6.5.1 Each stage represents a benchmark of performance and achievement;

7.6.5.2 The Organisation can incentivize its stakeholders to continually improve resilience and preparedness performance; and

7.6.5.3 Stages can be translated into the following achievement levels:

- **Phase One** - Copper
- **Phase Two** - Bronze
- **Phase Three** - Silver
- **Phase Four** - Gold
- **Phase Five** - Platinum
- **Phase Six** - Diamond

As previously mentioned, TSG decided to start implementing at Level 3 as they already had a substantial investment in a Risk Management program that had been functional for many years. The objective was to improve on this and to establish a system that would ensure further resilience to TSG. As the programme had already developed quite substantially, it was also decided to audit some of the TSG five-star hotels and one of the large gaming establishments to Level 4. Levels three and four had the following basic criteria. This was a perfect example of performing an analysis of the existing framework and determining that the established work product justifies starting at a higher level within the Maturity Model structure.

LEVEL 3: Programme approach

- This phase provides the opportunity to increase awareness to a larger portion of the organisation.
- Typically, more weight is given to proactive planning to address the symptoms and consequences of a disruption.

LEVEL 4: Systems approach

- The focus is to identify opportunities for improvement in resilience and preparedness performance.
- The focus is to identify opportunities for improvement in resilience and preparedness performance.
- Various parts of the Organisation are to test the standard's core elements to refine the implementation of the standard.
- Audit findings are used to identify opportunities for improvement in order to reinforce the competitive and strategic advantage of the Organisation.
- A culture of resilience and preparedness starts taking hold in the Organisation.

It should be noted that once levels three and four have been completed, the actions required for levels five and six, become much more complex. TSG so far, has only one 5 Star hotel that has completed Level 5. It takes exceptional effort to get to these higher levels but has great potential for the organisation and all its stakeholders.

7.7 IMPLEMENTING THE PLAN

Once an understanding of the requirements of the Project Plan had been reached and the very tight timelines reviewed, the team gathered and set about evaluating what resources were required to implement the ORMS. A project plan was presented to the Group Director of Risk for approval. The advantage was that the Group Director of Risk was open to new ideas for time worn risk issues facing a modern organisation.

The support team was very small, but was still expected to respond to the challenges of protecting the organisation against a myriad of threats. With such a 'flat' organisational structure, it was realised that the project was destined to be difficult to complete in such a short timeframe.

After approval of the Project Plan and the budget were received, the team set about combining all of the hotel group's existing plans [see below list of different types of plans consulted and examined in this project]. All relevant documentation was consolidated into a single assessment effort. The existing plans included:

- Emergency Planning;
- Crisis Management;
- Business Continuity Planning;
  - Business Impact Analysis;
- Security Risk Management;
  - Risk Assessments;
  - GAP Analysis;
  - Action Plans;
- Risk Management;
  - Risk Assessments: High Level;
- Occupational Health and Safety; and
- Disaster Management.

These elements were all previously dealt with separately at different levels within the Organisation and in some instances were not drawn into the overall risk management plan. A combined plan was developed which allowed for easier management of the total process. Although the elements still have to be managed and measured separately at times, the overall plan allowed for a much 'sleeker and streamlined' management reporting system, which was easier to understand, implement and audit.

7.8 INITIAL FIELD ASSESSMENTS

Very strict timelines were set. The training of the project team in the ISO 28000 and the *ANSI/ASIS SPC.1-2009* standards and all the initial processes were driven very hard. Meetings normally started at 06: 00 in the morning and ended between 19: 00 and 21: 00 for at least four days a week over a three-month period. Once the training was completed and the project started in all seriousness, documents and processes had to be reviewed and refined to see what was still required in terms of the ORMS. A full GAP analysis was conducted.

To this end, it was decided to use five different facilities throughout the country to check and then decide what could be used and how this will fit into the resilience programme. The facilities that were chosen was a five-star hotel in Sandton (Gauteng), a four-star hotel in Durban (Kwa-Zulu Natal), a–three-star hotel and a

Casino in eMalahleni (Mphumalanga) and later another three-star hotel in Sandton. The files at each facility were reviewed and the continuing value of each document assessed.

7.9 THE IMPORTANCE OF PEOPLE

The project team knew the importance of involving the staff of the Organisation. Preparations were then made to begin the process of changing the attitudes of the workers and thereby begin the long process of changing the culture within the organisation. Generating excitement and communicating the importance of the work was a crucial element required for a successful project. The importance of this involvement was quite clear and it was stated continuously that staff members needed to understand that their work actually means something – with this understanding, the project picked up momentum.

The project team developed different presentations according to the audience and their job level within the Organisation. At an executive level the presentations spelt out what the process involved from a strategic perspective down to an implementation level. The other presentation was for the general staff from supervisor level down. This presentation showed how it would involve them, impact on their work environment and the positive spin-offs that it would have for them as well as the organisation. The employee's involvement in the project resulted in a direct relationship to the employee's performance review and potential bonuses.

7.10 PILOT PROJECTS

TSG was paying a number of different auditing organisations to conduct audits and assessments for each of the core elements as described in the ORMS, These included the following:

- Risk Management;
- Security Risk Management;
- Business Continuity Planning;
- Emergency Planning;
- Disaster Management; and
- Occupational Health and Safety.

As part of the explanation and gaining support from the highest level of management, the Director of Risk for the Group, gave a presentation to the Group Executive Management on the anticipated advantages of implementing and maintaining the Maturity Model, which incorporated all of the above areas for assessment plans.

The Executive Board approved the concept immediately and approved its implementation over a three-year period, the time that the project team had estimated that it would take to do a complete rollout of the Maturity Model. At that time the programme would be fully assessed as to its impact and how effective it had been.

The executive, however, wanted to see demonstrable evidence that the project had value. The team established a pilot project to demonstrate the practical application and value of the larger project. Two five-star hotels, a three-star hotel and a casino resort were selected for the pilot projects. Presentations (briefings) were conducted for each of these units' senior managers and heads of departments explaining the project, the goals and the value of the *ANSI/ASIS SPC.1-2009*. While some of the concepts were foreign to the managers and required explanation to show that the team was not reinventing the wheel, each General Manager quickly understood the value of the project.

The managers soon came to see that the project team was taking all the existing processes and forming a more synergistic approach with a single measurable process. Initially managers considered worst case scenarios when they heard about a "new" project, but perseverance and a clear strategy resulted in a positive understanding.

Once the initial GAP analysis was completed, a workshop was held and the team studied the results. The shortcomings were discussed and decisions taken as to what documentation and processes were required to keep the business units in-line with the overall plan. A plan was established on the way forward. This included the use of the revised Intervention Schedule which would serve as the base for management to keep abreast of legislative requirements and other business interventions. The

Project Plan is depicted in Table 4, earlier in this chapter and a sample of a section of the Intervention Schedule is shown in Table 6.

It was also decided that the documentation that was going to be retained should be kept in files and placed in a specific order. As this was a new approach, it was decided that the files would be specifically branded for the Organisational Resilience project. This was done and initially two volumes were found to be adequate for the general hotels but that the five-star units and the casinos all required four volumes due to the size and complexity of their individual organisational structures.

One of the goals was to have only documents with operational value retained in the files and it was decided that documents older than six months, which were not necessary to be retained as part of the policy, were to be archived. This would keep the files operational and manageable and also require a more regular assessment of all their activities and the status of any element within the files.

7.11 GROUP IMPLEMENTATION

As a result of all the above planning, presentations and pilot implementation the Tsogo Sun Group Risk Department received a mandate from their executive to implement the ORMS project throughout the organisation.

A Group Policy was signed by the Group CEO and issued directly to each of the Divisional CEOs. Each Divisional Manager and each Unit Manager also issued a Policy document and all are held accountable for its delivery. The measurement thereof forms part of their Key Performance Areas (KPAs) and thus has an influence on their bonuses.

The measurement process is managed by an Intervention Schedule that was initially developed by Colin Ackroyd for TSG and was refined during the roll-out of the project. It is now possible that a Unit Manager can actually keep control of the whole process from a few sheets paper (control and self-assessment checklists). The managers where this system was initially implemented were very excited about the way in which the document was structured and how it allowed them to manage an otherwise extensive programme.

An example of the headers that were used for the Intervention Schedule and two line items are shown:

Table 6: Sample of the Intervention Schedule

ITEM	MANAGED BY	FREQUENCY	STANDARD	OBJECTIVE	SLA	DATE LAST REVIEWED		
Controlled Self-Assessment Self-assessment Inspections	GM	Monthly	Checklist based on items listed below	To ensure emergency equipment is regularly checked	YES			
Fire Detection Service	Contractor	6-Months	SABS 0139/Manufacturer Specs	To ensure detection is maintained to its optimum.	NO			
Training	Management	3-Months	SABS 0139/SOP-18	Ensuring that staff are familiar with the operation of equipment	N/A			

This schedule is normally set in a spread sheet format in Excel and is not as condensed as it is depicted here.

The number of items covers all the legal and other compliance items that an organisation has to adhere to and can thus cover a number of pages.

One of the items that was found lacking with the initial schedule and why it was included, is that of Service Level Agreements (SLAs). Organisations enter into SLAs and expect that the service will be delivered as per the agreement. In many instances in this project, as well as others that the researcher has been involved with over the years, it has been found that the SLA is not worth the paper that it is written on or that the service agent does not comply or adhere to its own SLA. This can create a false sense of security within the organisation until an incident takes place and lives are lost or infrastructure is extensively damaged. To then try and place the blame at the culprit's door becomes a legal nightmare.

The roll-out of the Maturity Model on the ORMS standard in TSG has been very successful and the fruits of the are there for all to see as the multi-elements of the programme are now more easily managed and as people get a better understanding and also see the results, they have become more committed to making sure it works for them and thus for the organisation.

7.12 AUDIT PROCESS

The audit process was based on the information outlined in Chapter 5 regarding the ORMS standard (SPC.1) and followed the audit protocols and guidelines as discussed in Chapter 6 relating to the requirements of ISO 19011:2002.

The different documents are not going to be discussed here again as they were fully discussed in Chapter 5. What has been added here, are the documents required by the organisation to add their respective requirements of what document is required where, in order to satisfy the respective standard element.

As the project team completed their work on review and implementation, each business unit was given a pre-audit as part of the GAP analysis. They were then given two weeks to rectify any identified problems before a full audit was conducted.

The audits, conducted using the Maturity Model, used a scoring system for each item noted on the specific level of the Maturity Model. The scoring mechanism consists of an achievable score of two points per item. If nothing was done, then the score is zero and if there was an indication of “work-in-progress” then the score would be one. Each unit had to score at least 80% to receive a passing grade and a certificate of Compliance.

A column was also included in the Maturity Model evaluation sheet for samples of documents that were reviewed against the requirements of the Maturity Model. The auditee had to achieve at least 100% otherwise they were penalized by subtracting at least two points from their achieved score. The average score was 87% with over 36 audited units within TSG. Only one business unit failed resulting in a management change which indicated that the group was very serious about the whole implementation process of the Maturity Model.

The TSG Divisional Risk Managers felt that the ORMS programme was a very important component of the TSG Risk Management Programme as all the elements of the ORMS, as required by the Maturity Model, were issues that dealt with life safety and corporate assets. They were of the opinion that the standard of attainment had to be set high and that no half measures would be tolerated.

7.13 RECOGNITION

Business units received a specially designed certificate when they achieved different levels of the Maturity Model. The Group CEO, as well as the ORMS Auditor, approves and signs each certificate and the respective Divisional CEOs for Hotels and Gaming preside over the presentations. This senior level involvement ensures that the respective unit leaders remain constantly informed. ORMS now forms an action item on their agendas and the employees recognise that their work is both valued and acknowledged by the executive. The staff and managers included are directly involved in the ORMS process, which is an extremely important motivational tool. The business units have accepted the challenge of ORMS compliance, which has fostered a ‘competition’ between units. The units also have to report their respective status at their divisional meetings. Maintaining an average audit score of at least 80% takes very hard work as management and operational structures are flattened even more so in current harsh economic times.

7.14 CONCLUSION

Currently TSG continues to implement ORMS through a fully accepted company concept of Organisational Resilience Management as a requirement of doing business. The various business units are striving for achievement of the next levels including levels: four, five and six. Some of the outcomes of the ORMS implementation are discussed in the next chapter.

Full implementation Level 6 may not occur because of the additional requirements that are expected from the TSG supply chain. Over time it may however be possible to ensure that the main external supply chain vendors do become involved and start participating in the ORMS. There needs to be a more formal process between organisations and vendors to establish reactive guidelines and processes in the event

of a disruptive incident. This is not an easy process as there have never been any restrictive ‘governance’ requirements in this business sector before, but as all participants, at all levels of the organisation and the supply chain, get a better understanding of the process, it will evolve and improve.

The fact is that the acceptance of the implementation of the Maturity Model by TSG established the base from which the programme developed and was fully implemented over a period of time. The refinement of the requirements that were specific to the Tsogo Sun Group and the hospitality and gaming industry, were adapted and implemented as envisioned in the Maturity Model and the Organisational Resilience Management Standard.

CHAPTER 8
FINDINGS, RECOMMENDATIONS AND CONCLUSIONS

8.1 INTRODUCTION

In this final chapter the findings, recommendations and conclusions will be briefly discussed based on the information gathered and observed during the implementation of the Organisational Resilience Management System using a Maturity Model at the Tsogo Sun Group (TSG). Additionally there are other discussions and research regarding the possible and potential areas for the improvement of the Security Risk Management System (SMS).

8.2 RESEARCH QUESTIONS AND CONCLUSIONS

The research questions and interviews assisted in developing the results that are discussed here below. The Interview Questions and Interview Schedule are included as Appendix 'B' and 'C'.

8.2.1 Research problem

In Chapter 1 the research problem was set and the following research question posed:

> *Is it possible to bring about a paradigm shift in Security Risk Management using a Maturity Model based on the main elements required in the ANSI/ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with guidance for use?*

Finding

The question has been answered positively from the progressive results that have been attained by TSG through this project.

This Research Problem was followed by the following two items which also set the framework for the research as outlined in Chapter 1:

8.2.2 Research objectives

The objective of this research was to evaluate the effectiveness of using the Maturity Model with the *ANSI/ASIS SPC.1-2009*'s Organisational Resilience Management System Standard to manage security risks within the context of a Security Risk Management approach.

Findings

The effectiveness of the implementation of the Maturity Model based on the SPC.1 has proven to be successful.

TSG has been able to implement a programme that organises a previously fragmented approach to their safety, security and business continuity programmes into a consolidated, unified, single and better organised process.

Internal and external audit programmes have, as a result, become more focussed and give the organisation a more in-depth look at the value and impact their various risk management programmes have on their different lines of business.

TSG have been able to identify and deal with problem areas much quicker due to the manner in which the questions are dealt with during the Maturity Model audits and business unit reviews.

After implementation a noticeable improvement in TSG staff morale occurred. This, partially, as a result of the smoother working of the ORMS system, which reduced work pressures on them. They also gained a fuller grasp of their own environments and what risks they have to prepare for and deal with if required.

They are also now, as a result of the implementation, much better prepared and have had resources made available to them to improve the conditions that they may have been in previously before the ORMS was implemented.

Training programmes have been ongoing and this has assisted with each employee knowing what their task will be in the event of an emergency and how to react to get

the business back into operations again with as little disruption as possible. This has created a sense of confidence with management and staff.

8.2.3 Research questions

The following questions formed the framework of this research. (The numbering has been kept the same as per the original numbering in Chapter 1).

1.5.1 ***Do International Organisation for Standardisation (ISO) standards contribute to forming an organised framework for security risk management?***

Finding

Based on this research, ISO standards do form a good structure that provides organisations with a framework to improve their operations and to measure these improvements against international best practice.

1.5.2 ***Are there any benefits in implementing the ORMS in an organisation?***

Finding

This research has confirmed the organisational as well as financial benefits such as reduced insurance premiums and claims for damages against TSG if implemented in accordance with the ORMS.

1.5.3 ***Does the Maturity Model for the ORMS have any measurable benefits for an organisation?***

Finding

This research has shown that if the organisation uses the Maturity Model as per the intended use thereof, the organisation will have measureable benefits.

1.5.4 ***How does the use of recognised audit systems or procedures add value to the achievement of the paradigm shift in security risk management using the Maturity Model?***

Finding

The improvement of consistency by the various TSG business units had a significant impact on the results that have been achieved in a number of areas of the business. The Intervention Schedule created a framework for compliance. This added to the discipline that was required to ensure compliance with various legislative requirements. It also ensured that the correct legislation was identified with which to comply as well as establishing the review periods and responsible person who had to deal to the specific item. All line items in the Intervention Schedule formed part of the worksheet. This assisted the organisation to adequately service and thus protect its assets through regular checks and audits. Where applicable, Service Level Agreements (SLAs) were entered into with specialist suppliers to service and check the assets at predetermined times.

The results of the project have shown that a paradigm shift can be achieved at all levels of staff and implementing agents by following the guidelines of the ORMS and using the Maturity Model that was developed for it.

1.5.5 *Does an organisation's agility to identify and deal with risk incidents improve after implementing the ORMS using the Maturity Model?*

Finding

TSG has experienced improved ability to identify possible developing risk situations due to the improved risk management processes at all levels in the organisation, thereby improving the agility to timeously prevent and deal with any developing risk situation. This study of the TSG implementation has also demonstrated that an organisation is better equipped to deal with any incidents as discussed in this research after implementing the ORMS based on the Maturity Model.

8.2.4 Aim of the research

The **primary aim** of this research was to study the transition of an organisation's risk management approach from a fragmented approach to a comprehensive strategy using the Organisational Resilience Standard in tandem with a Maturity Model.

The **secondary aim** was to:

- establish whether resilient organisations are able to make a paradigm shift in order to improve the management of risks for the future by using the SPC.1, which included the development of plans to reduce risks that had not yet been established; and

- undertake a research examination of whether resilient organisations are more agile in managing risks and better prepared to face the risks of unexpected events.

Findings

The Maturity Model not only brought all the elements together under a single management process as required in the ORMS Standard, but has also created a programme where people have to interface with each other in order to grow to the next Level of Maturity.

Both the secondary aim questions have been discussed above and have had positive results.

8.3 INDUSTRY FEEDBACK

8.3.1 Lead Auditor Course, Centurion

In the period 28-30 June 2011 a five-day Lead Auditor/ISO 28000:2007 – Security in the supply chain course was held in Centurion, Tshwane. The course was facilitated by the researcher and Roger Warwick from Italy. who is an ISO 28000 Skills Examiner and has extensive experience in the field of security management standards. The course was attended by two specialists in the field of audits from ESKOM's Security Risk Management Department, the Head of Security for the Department of Transport and three other standards consultants. Although security systems formed a major part of the Lead Auditor course, the main focus areas were around auditing, the auditing of the SMS and audit methodologies.

On completion of the course and after the attendees had written their exams, they were also asked the following questions as part of a survey to see if they understood

the implementation of the ISO 28000:2007, the introduction to ORMS standards and whether the audit protocols would be useful for implementation in their respective organisations.

Question 1: *Would the implementation of a standard such as ISO 28000:2007 add value to your organisations Security Risk Management programme?*

Reply Analysis

All the respondents said that it would, if implemented as recommended.

Question 2: *Would the programme be applicable to all sectors of the organisation?*

Reply Analysis

All the respondents said that it would apply across the organisation but that certain areas required more attention than others. There full consensus on this answer.

Question 3: *Does your organisation have an up-to-date Security Management Policy? (Not older than a year).*

Reply Analysis

All the respondents said that they had a Security Management Policy in place. Two respondents indicated that their policies required updating (i.e. were older than one year) and understood the rationale of implementing the methodologies now that they had attended the course.

Question 4: *Would your organisation use a Maturity Model to save costs on implementation of a Security Management System based on ORMS and audits of the system?*

Reply Analysis

All the respondents replied in the affirmative since they would now be able to implement a standard without excessive cost implications.

Question 5: *Would you train your own organisations' Security Management System auditors in ISO 19011:2011 to conduct the audits?*

Reply Analysis

All the respondents confirmed that this would also save them costs.

The results were very positive and all participants were of the opinion that it gave a much better and organised base to work from in different sectors. The audit principles to be applied for any standards implementation would be the same as described in Chapter 6 but based on ISO 19011:2011.

In April 2012, ESKOM published a tender for the revision of their Security Management System (SMS). One of the main requirements of the tender was to align the SMS with ISO 28000:2007 so as to develop a resilient organisation. This is a very positive sign for the security industry, that such a mega organisation in South Africa is serious about aligning its Security Management System Plan to international best practices. It is also the first time that this standard has been requested to form part of a tender in South Africa.

ISO 28000:2007 was incorporated into the *ANSI/ASIS SPC.1-2009* to form part of the Organisational; Resilience Management System. ISO 28002:2011 Resilience in the supply chain, has now further refined the requirements of a Security Management System with all the elements incorporated into it again in the most recently published version of this standard.

8.3.2 Tsogo Sun Group

In an interview with Dr Gert Cruywagen, Director of Risk, Tsogo Sun Group, on 14 June 2012, he was asked by the researcher what value the ORMS programme had thus far brought to the TSG, exactly two years after the initial implementation. His reply was the following:

- The group had been able to reduce audit visits to business units. This had resulted in substantial cost savings for TSG;

- Audit visits now have focussed and set processes which are audited objectively in accordance with standardised checklists and self-assessment exercises;
- All managers and supervisors know what is required and thus ensure that these elements are adequately maintained for audit purposes;

- Elements are now measured that were previously not measured due to the fragmented approach of the 'old' risk management system;

- There is an increased level of motivation to improve the ORMS at all levels of management as this process now forms part of the group audit review process to enhance their compliance and resilience capacity; and

- The benchmarking process has allowed the TSG to measure the achievements of similar units against each other and deal with shortcomings more effectively.

However, and most importantly, Dr Cruywagen reported that TSG's insurance records show the following:

- There have been significant reductions (since implementation of the Maturity Model for the ORSMS) in internal insurance claims being raised, which has led to TSG being able to negotiate more favourable insurance rates with their insurers and re-insurers amounting to tens of millions of rand in savings for the Group.

- The TSG Executive Board believes that this programme is so valuable that it has allocated additional resources to ensure that the value to the Group is enhanced even further.

- The ORMS Programme forms an agenda item at all levels of the organisations operations.

These comments and the reported tangible results show that the initial implementation methodology and subsequent programme management of the Maturity Model have been very successful.

8.4 BENEFITS OF THE ORMS PROGRAMME

The programme soon teaches people that they are reliant on each other to make the system work. In the Tsogo Sun Group project it became clear soon after a start was made on implementing the Maturity Model that the more successful implementations occurred where there was full participation at all levels. It was not only participation, but the communication between all stakeholders both internal and external that had a positive effect on the results that were achieved.

The resilience approach enabled the organisation to better allocate resources and priorities. By simultaneously considering minimising likelihood and consequence, it was possible to build a layered approach of technical and administrative measures, balancing strategies to minimise the likelihood of consequences. The maturity model used a phased implementation approach that created the culture of “risk ownership” with employees and other stakeholders. In the TSG Project it was found that by addressing risk management in achievable steps led to a better and much improved collaboration between internal and external stakeholders.

The study confirmed that the phased approach of the Maturity Model supports the development of a top-down and bottom-up cultural and paradigm shift to support processes to enhance an organisation’s resilience. In other words, such organisation’s ability to respond quickly, change the way they do things (in risk management) and improve overall ‘agility’ and resilience. The sense of ownership appeared also to increase the capability of people to pre-emptively plan for and effectively manage potentially disruptive events.

Overall the Maturity Model provided a cost-effective approach to for implementation and maintenance of all the elements of the SPC.1 standard. The case study demonstrated that this approach could and can be tailored to organisations of any size.

The ORMS programme is new and has still to be properly entrenched in an organisation’s culture. It needs more time to settle down, mature and become more widely accepted as a method of cost-effective risk management. Future processes in its development as an overall management system (and also to its implementation in

TSG) would include moving from the present levels in the Maturity Model to the next and higher levels if so required. The advantage of implementing this programme is that an organisation can decide up to what level it wants to achieve and to maintain. The ultimate goal would be to reach Level Six of the Maturity Model but this may take years to achieve and may actually not be in the best organisational culture and financial interests of the company.

From results that have been achieved with its implementation at TSG over the past two years, using the ORMS Maturity Model, TSG should be able to sustain a minimum Level 3 and a maximum Level 5. This will give the group a very good balance to work with. Their future ORMS efforts should therefore be focussed on refining the disciplines of safety, security and business continuity through review processes and enhancing the strategic value and impact of their Intervention Schedule.

8.5 RECOMMENDATIONS

This is the first documented research into the use of a Maturity Model in applying the Organisational Resilience Management Standard. The research has opened up a number of new avenues for implementing and reviewing how effectively the Maturity Model can be used in practice. The initial implementation at TSG has already indicated that a paradigm shift is achievable by implementing and monitoring the project across the different spectrums of the organisation. The Organisational Resilience Maturity Model will become an important part of many local and international organisations' future safety, security and continuity strategies.

The new SPC.4 Maturity Model for ORMS can be followed, particularly the audit steps and used by future users and researchers in this environment by merely making a few changes to the older version.

The aspect of communication cannot be stressed strongly enough as that is probably the one element that will allow the programme to establish itself and to grow. This was achieved by using the formats as developed in the Maturity Model based on the guidelines in SPC.1. This included the formalisation of meetings, the use of the

focussed agenda items and the manner in which many more members of staff had become involved in the process of developing resilience in the organisation.

Organisational Resilience needs to become a permanent point on any organisation's Executive Board agenda. It will not only assist in the improvement of the organisation's management of all its risk elements, but will also improve the professionalism of the individual responsible for managing security risks. This individual will have to grasp a much wider scope of risk elements and will have to multi-task with more professional skill sets than before.

The security professional of the future will have to understand the risks facing an organisation at a totally different and higher level and must be able to guide the organisation in ways that have not been done by such an individual before. Without such skills and understanding of all the elements that make up Organisational Resilience, there will be no future for a "non-forward thinking" security professional in the organisations of tomorrow.

Organisations should start investing in the development of Organisational Resilience professionals. Resilient Organisations have already started looking at different ways of positioning their businesses to improve existing capacities and build new capabilities to combat the known and unknown threats of tomorrow.

The future will be the judge of the results of such implementations but in the future, corporates need to be asked to participate in research on this subject in order to ascertain what the real impact of implementation following a Maturity Model using the ORMS could be. The circumstances may be different in such organisations but the results will certainly be interesting for comparative purposes to experience and to validate against this initial study and methodology.

8.6 CONCLUSION

It was found that, by using the Maturity Model, all levels of management were allowed to have and experience a constant understanding of what level of resilience existed within the organisation. It also gave management and other stakeholders the confidence to know that the organisation could have a positive impact on and

extensively minimise the likelihood of potential disruptive events and other risk threats occurring. It was also found that in implementing the Maturity Model, would, in all likelihood, also mitigate the consequences should these actually occur and thereby enhance recovery time by allowing recovery to occur in an orderly and rapid fashion.

A paradigm shift in Security Risk Management using the Maturity model is thus possible in most resilient organisations willing to implement the Model.

LIST OF REFERENCES

American National Standards Institute (ANSI)/ASIS International (ASIS). 2009. *Organizational Resilience*: *Security, Preparedness and Continuity Management Systems – Requirements with Guidance for Use.* American National Standards Institute/ASIS International, USA. Available at http://ansi.org. Accessed 10 October 2010.

American National Standards Institute (ANSI)/ASIS International (ASIS). 2012. *ANSI/ASIS SPC.4-2012: Maturity Model for the Phased Implementation of the Organizational Resilience Management System.* American National Standards Institute/ASIS International, USA. Available at http://ansi.org. Accessed 5 March 2012.

ANON. 2010. *The Gartner IAM program maturity model*. Available at: http://www.slideshare.net/smooregartner/the-gartner-iam-program-maturity-model. Accessed 12 August 2011.

ANON. Nd. *Empirical*. Available at: http://en.wikipedia.org/wiki/Empirical. Accessed 18 April 2011.

ANON (Griffith University). 2011. *The RIMS risk maturity model*. Australia: Key Media. Available at: http://www.riskmanagementmagazine.com.au/articles/31/0c057531.asp. Accessed on: 15 August 2011.

Berrong, S. 2010. Hotel makes room for resilience. *Security Management.* Alexandria, Va: ASIS International

British Accreditation Bureau (BAB), 2012. *Introduction to accreditation and certification*. Available at: http://www.british-assessment.co.uk/articles/introduction-to-accreditation-and-certification.htm. Accessed 8 June 2012.

British Standards Institute (BSI). 2011. *What is a standard?* Available at: http://www.bsigroup.com/en/Standards-and-Publications/About-standards/What-is-a-standard/. Accessed 23 April 2011.

Creswell, J.W. 2008. *Research design: Qualitative, quantitative and mixed methods approaches*. Thousand Oaks, CA: Sage (Kindle Edition: Kindle Locations 4357-4360).

Crosby, P. 1979. *Quality is free*. New York: McGraw-Hill

Deming, W.E. 1986. *Out of the crisis*. Np. MIT Press

De Vos, A.S., Strydom, H., Fouche, C.B. & Delport, C.S.L., 2009. *Research at grassroots: For the social sciences and human service professions*. Pretoria: Van Schaik

Flyvbjerg, B. 2011. Case Study. In N.K. Denzin & Y.S. Lincoln (eds). *The Sage handbook of qualitative research*. 4th Edition. Thousand Oaks, CA: Sage

Godfrey, S. 2008. *What is CMMI?* NASA Presentation. Available at; http://ses.gsfc.nasa.gov/ses_data_2004/040601_Godfrey_Abstract.htm

Hamel, G. & Valikangas, L. 2003. The quest for resilience. *Harvard Business Review*. September: 1-13. Available at: http://www.gilbertacton.com/PDF/Other/The%20Quest%20for%20Resilience.pdf. Accessed on 7 May 2011.

Holling, C.S. (1973). *Resilience and stability of ecological systems.* IIASA Research Report RP-73-3. International Institute for Applied Systems Analysis, Vienna, Austria. Available at: http://www.iiasa.ac.at/Admin/PUB/Documents/RP-73-003.pdf. Accessed 11 April 2011.

Hopkin, P. 2010. *Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management.* Philadelphia: Kogan Page.

Humphrey, W. 1989. *Managing the software process*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Imas, L. 2010. *Designing and Conducting Case Studies for Development Evaluations*. Presentation at the Pre-conference Workshop for the IDEAS Global Assembly of the World Bank, Johannesburg. 2010.

International Organisation for Standardisation (ISO). 2012. *How the ISO develops standards.* (a) to (z) and (aa) to (ab). http://www.iso.org/iso/about/how_iso_develops_standards.htm. Accessed 22 June 2011.

Institute of Directors in Southern Africa (IOD) & King Committee on Governance. 2009. *King Code of Governance for South Africa 2009*. Johannesburg: IOD

Johnson-Lenz, P. and Johnson-Lenz, T. 2009. Six habits of highly resilient organisations. *People & Place,* 1(3). Ecotrust. Available at: http://www.peopleandplace.net/perspectives/2009/2/2/six_habits_of_highly_resilient_organizations/. Accessed 5 September 2011.

Juran, J. 1988. *Juran on planning for quality*. New York: Free Press

Kleppe, A. & Warmer, J.B & Bast, W., 2003. *MDA explained: The model driven architecture – Practice and promise.* Boston: Pearson Education/Addison-Wesley Professional.

Kocourek, P., Pasternack, B., Kelly, C., Newfrock, J., Bienenstock, M. Gregory, H. Messineo, R. & Powers, M. 2004. *Redefining the corporate governance agenda: From risk management to enterprise resilience*. Booz Allen Hamilton Inc./Well Gotshall & Manges, LLP. Available at: http://www.boozallen.com/media/file/Redefining_Corp_Gov_Agenda.pdf. Accessed on 12 April 2011.

Latour, A. 2001. Trial by fire: A blaze in Albuquerque sets off major crisis for cellphone giants. *The Wall Street Journal*, 29 January.

Lowe, R. 2011, *Business Continuity Professionals*. Discussion group on LinkedIn. http://www.linkedin.com/groupItem?trk=eml-anet_dig-b_pd-ttl-cn&gid=52866&view=&srchtype=discussedNews&item=65857888&type=member. Accessed 21 August 2011

Mettler, T., Rohner, P. & Winter, R., 2010. Towards a classification of maturity models in information systems (pp. 333-340). In: A. D'Atri, M. De Marco, A.M. Braccini, & F. Cabiddu, (eds.). *Management of the interconnected world*. Berlin/ Heidelberg: Physica-verlag.

Mingay, S. 2002. *Outlining the Gartner BCP Maturity Model*, Gartner Group Research Note.

Mitroff, I.I., Pauchant, T.C., Finney, M., & Pearson, C. (1989). Do (some) organisations cause their own crises? The cultural profiles of crisis-prone vs. crisis-prepared organisations. *Industrial Crisis Quarterly, 3*(4).

Moore, S. 2008. *IAM Program Maturity Model.* Slide presentation for Gartner Group.

Morgan Stanley Bank. 2001. *Annual Report, 2001*. Available at: http://www.morganstanley.com/about/ir/annual/2001/index.htm. Accessed on 2 April 2011.

Mouton, J. 2009. *How to succeed in your masters and doctoral studies.* Pretoria: Van Schaik.

Mouton, J. & Marais, H.C. 1996. *Basic concepts in the methodology of the social sciences.* Pretoria: Human Sciences Research Council.

Neuman, W.L. 2000. *Social research methods: Qualitative and quantitative approaches.* 5th Edition. Boston: Allyn & Bacon.

Nieuwenhuis, J. 2010. Qualitative research designs and data gathering techniques. In: K. Maree (ed.) *First steps in research*. Pretoria: Van Schaik

Oldfield, R. 2007: *Organisational Resilience*. Presentation to Council on Competitiveness, Australia.

Patton, M.Q. 2008. *Utilization-focused evaluation* (4th Edition). Thousand Oaks, CA: SAGE.

Patton, M.Q. 2012. *Essentials of utilization-focused evaluation*. Thousand Oaks, CA: SAGE.

Parker, B., Feblowitz, J. & Knickle, K. 2008. *Enterprise risk management: Keeping people, assets and the environment safe.* White Paper (SAP). IDC: Industry Insights. http://www.slideshare.net/findwhitepapers/idc-energy-insights-interprise-risk-management. Accessed 14 June 2012.

Paulk, M.C., Curtis, B., Chrissis, M.B. & Weber, C.V. 1993. *Capability maturity model for software, Version 1.1*. Technical Report. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Available at: http://www.sei.cmu.edu/reports/93tr024.pdf. Accessed 15 August 2011.

PricewaterhouseCoopers (PwC), South Africa. 2009. *King's counsel: Understanding and unlocking the benefits of sound corporate governance. Corporate governance Executive guide to King III*. Johannesburg: PricewaterhouseCoopers Inc. Available at: http://www.pwc.com/en_ZA/za/assets/pdf/Executive-Guide-to-KINGIII.pdf. Accessed 9 September 2011.

Registrar Accreditation Board (RAB)/Quality Society of Australasia (QSA) (RABQSA). 2012. *Explanation of abbreviation RABQSA*. http://www.rabqsa.com/. Accessed 13 June 2012.

Resilience Expert Advisory Group (REAG). 2011. *Organisational resilience: A position paper for critical infrastructure*. Australian Case Studies. Canberra: Attorney-General's Office, Commonwealth of Australia. Available at: http://www.emergency.qld.gov.au/publications/pdf/Organisational_Resilience.pdf. Accessed 5 May 2011.

Ross, A. (edited by Mitchell, R.). 2009. *Managing risk in perilous times: Practical steps to accelerate recovery*. London: *The Economist* Intelligence Unit. Available at:

http://www.acegroup.com/eu-en/assets/eiu-version-of-managing-risk.pdf. Accessed 8 August 2011.

Sarbanes-Oxley Act. 2002. http://www.soxlaw.com Accessed 15 June 2012.

Sarbanes-Oxley Act, USA. 2012. *Summary of legislation*. Available at: http://www.soxlaw.com. Accessed 14 June 2012.

Seddon, J. 2012. *Open Letter to Stevan Breeze*. http://www.systemsthinking.co.uk/EmailDownloads/StevanBreeze.pdf Accessed 8 June 2012.

Sheffi, Y. 2005. *The resilient enterprise*, Cambridge, Mass.: MIT Press.

Shewhart, W. 1931. *Economic control of quality of manufactured product.* Np. D. Von Nostrand. Reprint 1980. Milwaukee: Quality Press.

Siegel, M. (Marc) & Siegel, M. (Maya), 2010. *Maturity model for organizational resilience*. Alexandria, Va: ASIS International

Simpson, K. 2011. *[A]ge is not an indicator of resilience*. (Blog Business Continuity Professionals, 11 July). Available at: http://www.blog.vrg.net.au/resilience-thinking/age-is-not-an-indicator-of-resilience/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Contemplating+%28Contemplating+...%29&utm_content=FeedBurner. Accessed 5 September 2011.

Smit, N. 2005. *Business Continuity Management: A Maturity Model*. Masters dissertation, Erasmus University, Rotterdam, The Netherlands.

Sobon, J. 2011. *The United Nations and Resilience*. Presentation to the SARMA Annual Conference, Georgetown University, Washington, DC.

Software Engineering Institute (SEI). 2006. *Standard CMMI® Appraisal Method for Process Improvement (SCAMPISM) A, version 1.2: Method definition document*. (Standard CMMI Appraisal Method for Process Improvement (SCAMPI) upgrade team). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Available at: http://www.sei.cmu.edu/library/abstracts/reports/06hb002.cfm. Accessed 17 July 2011.

Software Engineering Institute (SEI). 2008. Capability Maturity Models® capability maturity models (CMMs). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Available at: http://www.sei.cmu.edu/cmmi/tools/cmmiv1-3/upload/DEV-Ch1-compare.pdf. Accessed 28 September 2011.

Stake, R, 1995. *The art of case study research*. Thousand Oaks: Sage

Stephenson, A., Seville, E., Vargo, J. & Roger, D. 2010. *Benchmarking resilience: A study of the resilience of organisations in the Auckland Region*. Resilient Organisations Research Report 2010/03b. Auckland: Resilient Organisations. Available at: http://www.stephensonresilience.co.uk/wordpress/wp-content/uploads/2010/12/Benchmark-Resilience-ResOrgs-Research-Reportb.pdf. Accessed on 12 May 2011.

Stimpson, W.A. (2012: 5-8), *The role of Sarbanes-Oxley and ISO9001 in corporate management. A plan for integration of governance operations*. Jefferson, NC: McFarland

The American Heritage Dictionary of the English Language, 2012, 4th Edition. Boston, MA: Houghton Mifflin.

The Risk Management Society (RIMS) (Australia). 2012. *Explanation of abbreviation- RIMS.* Available at: http://www.rims.org/aboutRIMS/Pages/MissionandDescription.aspx. Accessed 14 June 2012.

University of South Africa. (UNISA). 2012: *Research Ethics Policy.* Pretoria: UNISA http://www.unisa.ac.za/contents/research/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf. Accessed 16 May 2012.

Valsamakis, A.C., Vivian, R.W. & Du Toit, G.S. 2001. *Risk management*. 3rd edition. Durban: Heinemann.

INTERNATIONAL ORGANISATION FOR STANDARDS (ISO)

OFFICIAL STANDARDS DOCUMENTS

ANSI/ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with guidance for use. American National Standards Institute (ANSI)/ASIS International (ASIS), USA

ANSI/ASIS SPC.4-2012: Maturity Model for the Phased Implementation of the Organizational Resilience Management System. American National Standards Institute (ANSI)/ASIS International (ASIS), USA

ISO 9000:2008.: *The integrated use of management system standards*. ISO, Switzerland.

ISO 9001:2008. *Standard: Quality Management Systems: Requirements.* ISO, Switzerland.

ISO 9004:2000. *Standard: Quality Management Systems: Guidelines for performance improvements.* ISO, Switzerland.

ISO 14001:2004. *Standard: Environmental Management Systems: requirements for guidance with use.* ISO, Switzerland.

ISO 19011:2002. *Standard: Auditing systems guidelines.* ISO, Switzerland.

ISO 19011:2011. *Standard: Auditing systems guidelines.* ISO, Switzerland.

ISO/PAS 22399:2007. *Societal Security: Guidelines for incident preparedness and operational continuity management.* ISO, Switzerland.

ISO/IEC 27001:2005. *Standard: Information Technology: Security techniques: information security management systems: Requirements.* ISO, Switzerland.

ISO 28000:2007. *Standard: Specification for security management systems for the supply chain.* ISO, Switzerland.

ISO 28001:2007. *Standard: Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance.* ISO, Switzerland.

ISO 28002:2011. *Standard: Security management systems for the supply chain - Development of resilience in the supply chain - Requirements with guidance for use.* ISO, Switzerland.

ISO 28004:*2007. Security management systems for the supply chain: Guidelines for the implementation of ISO 28000.* ISO, Switzerland.

ISO 31000:2009. *Standard: Risk Management: Principles and guidelines.* ISO, Switzerland.

ISO 31010:2009. *Standard: Risk Management: Risk assessment techniques.* ISO, Switzerland.

ISO Guide 72:2001: Guidelines for the justification and development of management system standards, ISO, Switzerland.

ISO/IEC Guide 73:2002: *Risk Management: Vocabulary: Guidelines for use in standards.* ISO, Switzerland.

OHSAS 18001:2007: Occupational health and safety management. ISO, Switzerland

PD 25888:2011: Published Document: Business continuity management - Guidance on organisation recovery following disruptive incidents. BSI, United Kingdom.

INTERVIEWS

Warwick, R.L. 2011. Skills Assessor and Lead Auditor ISO 28000 and Security Management Systems, Centurion, 11 July.

Also see Annexure B.

ANNEXURE A: DEFINITIONS

The following definitions are applicable to this research as the terms of reference for the *ANSI/ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with guidance for use*. These definitions are descriptive of the elements mentioned throughout this research document.

This section has been copied directly from Annexure D and are used with the permission of the copyright holder, ASIS International and are based on the terms and definitions given in ISO/IEC Guide 73 and the following definitions apply. The numbers from ***Annexure D*** have been retained for ease of reference.

D.1 acceptable downtime: Maximum elapsed time between a disruption and restoration of needed operational capacity or capability.

D.2 alternate worksite: A work location, other than the primary location, to be used when the primary location is not accessible (ASIS International Business Continuity Guideline: 2005).

D.3 asset: Anything that has value to the organization (ISO/IEC 13335-1: 2004).

D.4 auditor: Person with competence to conduct an audit (ISO 9001: 2000).

D.5 continual improvement: Recurring process of enhancing the organizational resilience (OR) management system in order to achieve improvements in overall OR management performance consistent with the organization's OR management policy.

NOTE: The process need not take place in all areas of activity simultaneously.

D.6 corrective action: Action to eliminate the cause of a detected nonconformity (ISO 14001: 2004).

D.7 critical activity: Any function or process that is essential for the organization to deliver its products and/or services (ISO/PAS 22399: 2007).

D.8 criticality assessment: A process designed to systematically identify and evaluate an organization's assets based on the importance of its mission or function, the group of people at risk, or the significance of a disruption on the continuity of the organization.

D.9 conformity: Fulfilment of a requirement.

D.10 consequence: Outcome of an event (ISO/IEC Guide 73).

NOTE 1: There can be more than one consequence from one event.

NOTE 2: Consequences can range from positive to negative.

NOTE 3: Consequences can be expressed qualitatively or quantitatively.

D.11 continuity: Strategic and tactical capability, pre-approved by management, of an organization to plan for and respond to conditions, situations and events in order to continue operations at an acceptable predefined level.

NOTE: *Continuity*, as used in this *Standard*, is the more general term for operational and business continuity to ensure an organization's ability to continue operating outside of normal

operating conditions. It applies not only to for-profit companies, but organizations of all natures, such as non-governmental, public interest and governmental organizations.

D.12 continuity strategy: Approach by an organization intended to ensure continuity and ability to recover in the face of a disruptive event, emergency, crisis, or other major outage.

D.13 crisis: An unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment.

D.14 crisis management: Holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities – as well as effectively restoring operational capabilities.

NOTE: Crisis management also involves the management of preparedness, mitigation response and continuity or recovery in the event of an incident – as well as management of the overall program through training, rehearsals and reviews to ensure the preparedness, response and continuity plans stays current and up-to-date.

D.15 crisis management team: Group of individuals functionally responsible for directing the development and execution of the response and operational continuity plan, declaring an operational disruption or emergency/crisis situation and providing direction during the recovery process, both pre-and post-disruptive incident.

NOTE: The crisis management team may include individuals from the organization as well as immediate and first responders, stakeholders and other interested parties.

D.16 criticality: Of essential importance with respect to objectives and/or outcomes.

D.17 damaging potential: Harmful potential of an event, whether anticipated or unanticipated, that would impact on the ability of the organization to function effectively, cause critical harm to infrastructure, result in significant human or property losses to the organization or its stakeholders, or cause adverse effects to the reputation or integrity of the organization.

D.18 disaster: Event that causes great damage or loss (ISO/PAS 22399: 2007).

D.19 disruption: An event that interrupts normal business, functions, operations, or processes, whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a blackout, terror attack, technology failure, or earthquake).

NOTE: A disruption can be caused by either positive or negative factors that will disrupt normal functions, operations, or processes.

D.20 document: Information and supporting medium (ISO 9000: 2000).

NOTE: The medium can be paper, magnetic, electronic or optical computer disc, photography or master sample, or a combination thereof.

D.21 emergency: Sudden, urgent, usually unexpected occurrence or event requiring immediate action (ISO/PAS 22399: 2007).

NOTE: An emergency is usually a disruptive event or condition that can often be anticipated or prepared for, but seldom exactly foreseen.

D.22 exercises: Evaluating OR management programs, rehearsing the roles of team members and staff and testing the recovery or continuity of an organization's systems (e.g., technology, telephony, administration) to demonstrate OR management competence and capability.

NOTE 1: Exercises include activities performed for the purpose of training and conditioning team members and personnel in appropriate responses with the goal of achieving maximum performance.

NOTE 2: An exercise can involve invoking response and operational continuity procedures, but is more likely to involve the simulation of an response and/or operational continuity incident, announced or unannounced, in which participants role-play in order to assess what issues might arise, prior to a real invocation.

D.23 evacuation: Organized, phased and supervised dispersal of people from dangerous or potentially dangerous areas (ASIS International Business Continuity Guideline: 2005).

D.24 event: Occurrence or change of a particular set of circumstances (ISO/IEC Guide 73).

NOTE 1: Nature, likelihood and consequence of an event can not be fully knowable. NOTE 2: An event can be one or more occurrences and can have several causes. NOTE 3: Likelihood associated with the event can be determined.

NOTE 4: An event can consist of a non-occurrence of one or more circumstances.

NOTE 5: An event with a consequence is sometimes referred to as "incident".

D.25 facility (infrastructure): Plant, machinery, equipment, property, buildings, vehicles, information systems, transportation facilities and other items of infrastructure or plant and related systems that have a distinct and quantifiable function or service.

D.26 hazard: Possible source of danger, or conditions (physical or operational) that have a capacity to produce a particular type of adverse effects (ISO/PAS 22399: 2007).

D.27 impact: Evaluated consequence of a particular outcome (ISO/PAS 22399: 2007).

D.28 impact analysis: Process of analyzing all operational functions and the effect that an operational interruption might have upon them.

NOTE: Impact analysis includes *Business Impact Analysis* – the identification of critical business assets, functions, processes and resources as well as an evaluation of the potential damage or loss that may be caused to the organization resulting from a disruption (or a change in the business or operating environment). Impact analysis identifies: 1) how the loss or damage will manifest itself; 2) how that degree for potential escalation of damage or loss with time following an Incident; 3) the minimum services and resources (human, physical and financial) needed to enable business processes to continue to operate at a minimum

acceptable level; and 4) the timeframe and extent within which activities, functions and services of the organization should be recovered.

D.29 incident: Event that has the capacity to lead to human, intangible or physical loss, or a disruption of an organization's operations, services, or functions – which, if not managed, can escalate into an emergency, crisis, or disaster.

D.30 integrity: The property of safeguarding the accuracy and completeness of assets (ISO/IEC 13335- 1: 2004).

D.31 internal audit: Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the management system audit criteria set by the organization are fulfilled.

NOTE: In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited.

D.32 management plan: Clearly defined and documented plan of action, typically covering the key personnel, resources, services and actions needed to implement the incident management process.

D.33 mitigation: Limitation of any negative consequence of a particular incident (ISO/PAS 22399: 2007).

D.34 mutual aid agreement: Pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement (ISO/PAS 22399: 2007).

D.35 non-conformity: Non-fulfillment of a requirement (ISO 9000: 2000).

D.36 objective: Overall goal, consistent with the policy that an organization sets itself to achieve (ISO 14001: 2004).

D.37 organization: Group of people and facilities with an arrangement of responsibilities, authorities and relationships (ISO/PAS 22399: 2007).

NOTE: An organization can be a government or public entity, company, corporation, firm, enterprise, institution, charity, sole trade or association, or parts or combinations thereof.

D.38 organizational resilience (OR) management: Systematic and coordinated activities and practices through which an organization manages its operational risks and the associated potential threats and impacts therein.

D.39 organizational resilience (OR) management program: Ongoing management and governance process supported by top management; resourced to ensure that the necessary steps are taken to identify the impact of potential losses; maintain viable recovery strategies and plans; and ensure continuity of functions/products/services through exercising, rehearsal, testing, training, maintenance and assurance.

D.40 policy: Overall intentions and direction of an organization, as formally expressed by top management.

D.41 preparedness (readiness): Activities, programs and systems developed and implemented prior to an incident that may be used to support and enhance mitigation of, response to, and recovery from disruptions, disasters, or emergencies.

D.42 prevention: Measures that enable an organization to avoid, preclude, or limit the impact of a disruption (ISO/PAS 22399: 2007).

D.43 preventive action: Action to eliminate the cause of a potential non-conformity (ISO 14001: 2004).

D.44 prevention of hazards and threats: Process, practices, techniques, materials, products, services, or resources used to avoid, reduce, or control hazards and threats and their associated risks of any type in order to reduce their potential impact.

D.45 probability: Extent to which an event is likely to occur (ISO/IEC Guide 73).

NOTE 1: ISO 3534-1: 1993, Definition 1.1, gives the mathematical definition of probability as "a real number in the scale of 0 to 1 attached to a random event. It can be related to a long-run relative frequency of occurrence or to a degree of belief that an event will occur. For a high degree of belief, the probability is near 1."

NOTE 2: Frequency rather than probability may be used to describe risk.

NOTE 3: Degrees of belief about probability can be chosen as classes or ranks, such as:

- rare/unlikely/moderate/likely/almost certain; or
- incredible/improbable/remote/occasional/probable/frequent.

D.46 procedure: Specified way to carry out an activity (ISO 9000: 2000).

NOTE: Procedures can be documented or not.

D.47 record: Document stating results achieved or providing evidence of activities performed (ISO 9000: 2000).

D.48 recovery time objective (RTO): Time goal for the restoration and recovery of functions or resources based on the acceptable down time and acceptable level of performance in case of a disruption of operations.

D.49 residual risk: Risk remaining after risk treatment (ISO/PAS 22399: 2007).

D.50 resilience: The adaptive capacity of an organization in a complex and changing environment.

NOTE 1: Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.

NOTE 2: Resilience is the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.

D.51 resources: Any asset (human, physical, information or intangible), facilities, equipment, materials, products or waste that has potential value and can be used.

D.52 response plan: Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident.

D.53 response program: Plan, processes and resources to perform the activities and services necessary to preserve and protect life, property, operations and critical assets (ISO/PAS 22399: 2007).

NOTE: Response steps generally include incident recognition, notification, assessment, declaration, plan execution, communications and resources management

D.54 response team: Group of individuals responsible for developing, executing, rehearsing and maintaining the response plan, including the processes and procedures.

D.55 risk: Effect of uncertainty on objectives (ISO/IEC Guide 73).

NOTE 1: An effect is a deviation from the expected – positive and/or negative.

NOTE 2: Objectives can have different aspects such as financial, health and safety and environmental goals and can apply at different levels such as strategic, organization-wide, project, product and process.

NOTE 3: Risk is often characterized by reference to potential events, consequences, or a combination of these and how they can affect the achievement of objectives.

NOTE 4: Risk is often expressed in terms of a combination of the consequences of an event or a change in circumstances and the associated likelihood of occurrence.

D.56 risk acceptance: Informed decision to take a particular risk (ISO/IEC Guide 73).

NOTE 1: Risk acceptance can occur without risk treatment or during the process of risk treatment.

NOTE 2: Risk acceptance can also be a process.

NOTE 3: Risks accepted are subject to monitoring and review.

D.57 risk analysis: Process to comprehend the nature of risk and to determine the level of risk (ISO/IEC Guide 73).

NOTE: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

D.58 risk assessment: Overall process of risk identification, risk analysis and risk evaluation.

NOTE: Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the probability and impact of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure and evaluating the cost of such controls.

D.59 risk communication: Exchange or sharing of information about risk between the decision-maker and other stakeholders (ISO/IEC Guide 73).

NOTE: The information can relate to the existence, nature, form, probability, severity, acceptability, treatment, or other aspects of risk.

D.60 risk criteria: Terms of reference by which the significance of risk is assessed (ISO/IEC Guide 73).

NOTE: Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic and environmental aspects, the concerns of stakeholders, priorities and other inputs to the assessment.

D.61 risk management: Coordinated activities to direct and control an organization with regard to risk (ISO/IEC Guide 73).

NOTE: Risk management generally includes risk assessment, risk treatment, risk acceptance and risk communication.

D.62 risk reduction: Actions taken to lessen the probability, negative consequences, or both, associated with a risk (ISO/IEC Guide 73).

D.63 risk tolerance: Organization's readiness to bear the risk after risk treatments in order to achieve its objectives (ISO/IEC Guide 73).

NOTE Risk tolerance can be limited by legal or regulatory requirements.

D.64 risk transfer: Sharing with another party the burden of loss or benefit or gain, for a risk (ISO/IEC Guide 73).

NOTE 1: Legal or statutory requirements can limit, prohibit,or mandate the transfer of certain risk.

NOTE 2: Risk transfer can be carried out through insurance or other agreements.

NOTE 3: Risk transfer can create new risks or modify existing risks.

NOTE 4: Relocation of the source is not risk transfer.

D.65 risk treatment: Process of selection and implementation of measures to modify risk (ISO/IEC Guide 73).

NOTE 1: The term "risk treatment" is sometimes used for the measures themselves.

NOTE 2: Risk treatment measures can include avoiding, optimizing, transferring, or retaining risk.

D.66 security: The condition of being protected against hazards, threats, risks, or loss.

NOTE 1: In the general sense, security is a concept similar to safety. The distinction between the two is an added emphasis on being protected from dangers that originate from outside.

NOTE 2: The term "security" means that something not only is secure but that it has been secured.

D.67 security aspects: Those characteristics, elements, or properties which reduce the risk of unintentionally, intentionally and naturally-caused crises and disasters that disrupt and have consequences on the products and services, operation, critical assets and continuity of the organization and its stakeholders.

D.68 simulation exercise: Test performed under conditions as close as practicable to real world conditions (ISO/PAS 22399: 2007).

D.69 source: Anything which alone or in combination has the intrinsic potential to give rise to risk (ISO/IEC Guide 73).

NOTE: A risk source can be tangible or intangible.

D.70 stakeholder (interested party): Person or group having an interest in the performance or success of an organization (ISO/PAS 22399: 2007).

NOTE: The term includes persons and groups with an interest in an organization, its activities and its achievements: e.g., customers, clients, partners, employees, shareholders, owners, vendors, the local community, first responders, government agencies and regulators.

D.71 supply chain: The linked set of resources and processes that begins with the acquisition of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include suppliers, vendors, manufacturing facilities, logistics providers, internal distribution centres, distributors, wholesalers and other entities that lead to the end user.

D.72 target: Detailed performance requirement applicable to the organization (or parts thereof) that arises from the objectives and that needs to be set and met in order to achieve those objectives (ISO 14001: 2004).

D.73 testing: Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties, and to reveal weaknesses in the preparedness and response/continuity/recovery plans (ASIS International Business Continuity Guideline: 2005).

D.74 threat: Potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community.

D.75 top management: Directors, managers and officers of an organization that can ensure effective management systems – including financial monitoring and control systems – have been put in place to protect assets, earning capacity and the reputation of the organization.

D.76 vulnerability: Intrinsic properties of something that create susceptibility to a source of risk (D.53) that can lead to a consequence (ISO/IEC Guide 73).

D.77 vulnerability assessment: The process of identifying and quantifying vulnerabilities.

ANNEXURE B: INTERVIEW SCHEDULE

The interview schedule only shows the position of the individual interviewed. Tsogo Sun Group allowed the use of the names of the venues and positions of the individuals but not the person's name.

INTERVIEW REFERENCE	DATE OF INTERVIEW	TITLE OF PERSON INTERVIEWED
TSOGO SUN GROUP, HEAD OFFICE, SANDTON, GAUTENG		
Interview 1	**13 Oct 2009**	Director of Risk, Tsogo Sun Group
Interview 2	**14 Dec 2009**	Risk Manager, Southern Sun Hotels
Interview 3	**14 Dec 2009**	Risk Manager, Tsogo Sun Gaming
ELANGENI SUN, DURBAN, KWA-ZULU NATAL		
Interview 4	**15-16 Jan 2010**	General Manager
		Administration Manager
		Deputy General Manager
		Senior Food and Beverage Manager
		Housekeeping
		Maintenance
		Front Office Manager
		Health and Safety Manager
		Risk Manager, Southern Sun Hotels
		Municipal Fire Safety Liaison Officer
		Municipal Health Inspector
THE RIDGE CASINO, EMALAHLENI, MPUMALANGA		
Interview 5	**20-21 Jan 2010**	General Manager
		Surveillance and Security Manager
		Maintenance Manager
		Cash Desk Manager
		Health and Safety Manager
		Risk Manager, Tsogo Sun Gaming
		Municipal Fire Safety Liaison Officer
		Municipal Health Inspector

SANDTON SUN AND TOWERS, SANDTON, GAUTENG		
Interview 6	**19-20 Jan 2010**	General Manager: Sandton Sun
		Divisional Security Manager: Sandton Sun and Towers
		Financial Controller: Sandton Sun
		Food and Beverage: Sandton Sun
		General Manager: Sandton Towers
		Security Manager: Sandton Towers
		Facilities Manager: Sandton Sun
		Executive Chef: Sandton Sun
		Executive Housekeeper: Sandton Sun and Towers
		Health and Safety Manager
		Risk Manager, Southern Sun Hotels
		Municipal Fire Safety Liaison Officer
		Municipal Health Inspector
SUNCOAST CASINO, DURBAN, KAWZULU-NATAL SUN		
Interview 7	**26-27 Jan 2010**	Executive Director
		Director of Gaming
		GM Suncoast Towers
		Finance Manager
		HR Manager
		Marketing Manager
		IT Manager
		Food and Beverage Manager
		Cash Desk Manager
		Surveillance Manager
		Compliance Manager
		Security Manager
		Assistant Security Manager
		Maintenance Manager
		Occupational Health and Safety Manager
		Risk Manager, Tsogo Sun Gaming
		Municipal Fire Safety Liaison Officer

		Municipal Health Inspector
GARDEN COURT, MORNINGSIDE, SANDTON, GAUTENG		
Interview 8	**29 Jan 2010**	General Manager
		Security Manager
		Maintenance Manager
		Risk Manager, Southern Sun Hotels
		Municipal Fire Safety Liaison Officer
		Municipal Health Inspector
THE RIDGE HOTEL, EMALAHLENI, MPUMALANGA		
Interview 9	**2 Feb 2010**	General Manager
		Security Manager
		Risk Manager, Tsogo Sun Gaming
		Municipal Fire Safety Liaison Officer
ISO 28000 TRAINING COURSE AT NOSA, CENTURION, GAUTENG		
Interview 10	**27 Jun-1 Jul 2010**	Security Compliance Manager, Eskom
		Safety and Security Programme Manager, Eskom
		Security Manager, Department of Transport
		Risk Consultants (2): Security Management Systems: Temi Group
		Risk Consultant and Trainer: Security Management Systems: Pyramid International, Italy
TSOGO SUN GROUP, HEAD OFFICE, SANDTON, GAUTENG		
Interview 11	**14 June, 2012**	Director of Risk, Tsogo Sun Group
Interview 12	**14 June, 2012**	Risk Manager, Tsogo Sun Group: Hotels

ANNEXURE C: INTERVIEW QUESTIONS: BUSINESS UNITS

1. Do you have a **corporate security policy**?
2. Have you implemented the **Corporate Security Policy**?
3. When last was it updated and revised?
4. Do you have a **Risk Management Plan**?
5. When last was it updated and revised?
6. Do you have **Security Plan**?
7. When last was it updated and revised?
8. Do you have a **Business Continuity Plan**?
9. When last was it updated and revised?
10. Do you have a **Fire Safety Plan**?
11. When last was it updated and revised?
12. Is your Occupational Health and Safety program operated and updated as required by law?
13. Do you conduct table-top exercises to educate the management to requirements of the plans?
14. Do you involve third parties (i.e. first responders) in the exercises as participants?
15. Do third parties (i.e. civil defence) serve as observers to the exercises?
16. Have you formulated and updated an Intervention Schedule?
17. When was it last reviewed and updated?
18. Who ratifies the Intervention Schedule?
19. How often is the safety/security programme audited?
20. Who reviews the adequacy of the programme?

ANNEXURE D: International harmonized stage codes: Table 1

STAGE	SUBSTAGE						
				90 Decision Sub-stages			
	00 Registrat-ion	**20** Start of main action	**60** Completion of main action	**92** Repeat an earlier phase	**93** Repeat current phase	**98** Abandon	**99** Proceed
00 Preliminary stage	**00.00** Proposal for new project received	**00.20** Proposal for new project under review	**00.60** Close of review			**00.98** Proposal for new project abandoned	**00.99** Approval to ballot proposal for new project
10 Proposal stage	**10.00** Proposal for new project registered	**10.20** New project ballot initiated	**10.60** Close of voting	**10.92** Proposal returned to submitter for further definition		**10.98** New project rejected	**10.99** New project approved
20 Preparatory stage	**20.00** New project registered in TC/SC work programme	**20.20** Working draft (WD) study initiated	**20.60** Close of comment period			**20.98** Project deleted	**20.99** WD approved for registration as CD
30 Committee stage	**30.00** Committee draft (CD) registered	**30.20** CD study/ballot initiated	**30.60** Close of voting/ comment period	**30.92** CD referred back to Working Group		**30.98** Project deleted	**30.99** CD approved for registration as DIS

Standard and/or project					Stage		ICS
40 Enquiry stage	**40.00** DIS registered	**40.20** DIS ballot initiated: *5 months*	**40.60** Close of voting	**40.92** Full report circulated: DIS referred back to TC or SC	**40.93** Full report circulated: decision for new DIS ballot	**40.98** Project deleted	**40.99** Full report circulated: DIS approved for registration as FDIS
50 Approval stage	**50.00** FDIS registered for formal approval	**50.20** FDIS ballot initiated: *2 months*. Proof sent to secretariat	**50.60** Close of voting. Proof returned by secretariat	**50.92** FDIS referred back to TC or SC		**50.98** Project deleted	**50.99** FDIS approved for publication
60 Publication stage	**60.00** International Standard under publication		**60.60** International Standard published				
90 Review stage	**90.20** International Standard under periodical review	**90.60** Close of review	**90.92** International Standard to be revised	**90.93** International Standard confirmed		**90.99** Withdrawal of International Standard proposed by TC or SC	
95 Withdrawal stage	**95.20** Withdrawal ballot initiated	**95.60** Close of voting	**95.92** Decision not to withdraw International Standard			**95.99** Withdrawal of International Standard	

ANNEXURE E: **Standards Development Stages and Processes: Table 2**

Standard and/or project	Stage	ICS
ISO/DIS 22300 Societal security: Vocabulary	40.20	03.100.01 01.040.03
ISO/DIS 22301 Societal security: Preparedness and continuity management systems - Requirements	40.20	03.100.01
ISO/CD 22311 Societal security - Video-surveillance Format for Interoperability	30.20	03.100.01
ISO/PRF TR 22312 Societal Security: Technological Capabilities	50.00	03.100.01
ISO/DIS 22320 Societal security: Emergency management: Requirements for command and control	40.99	03.100.01
ISO/WD 22323 Organisational resilience management systems - Requirements with guidance for use	20.20	03.100.01
ISO/CD 22398 Societal security - Guidelines for exercises and testing	30.20	03.100.01
ISO/PAS 22399: 2007 Societal security - Guideline for incident preparedness and operational continuity management	90.93	03.100.01

ANNEXURE F: COMPATIBILITY WITH OTHER MANAGEMENT SYSTEMS

This Standard (ORMS) is aligned with ISO 9001:2008, ISO 14001:2004, ISO/IEC 27001:2005 and ISO 28000:2007 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management system can support the requirements of all these standards.

Correspondence between ISO Management System Standards, The ANSI/ASIS SPC.1 Organizational Resilience Standard, ASIS/BSI BCM01-2010 Business Continuity Management System Standard and the BS25999-2:2007

ISO Standards						
ISO 9001:2008	**ISO 14001:2004**	**ISO 27001:2005**	**ISO 28000-2007**	**ANSI/ASIS SPC.1-2009**	**ASIS/BSI BCM.01-2010**	**BS 25999-2:2007**
0 Introduction 0.1 General 0.2 Process approach 0.3 Relationship with ISO 9004 0.4 Compatibility with other management systems	**Introduction**	**0 Introduction** 0.1 General 0.2 Process approach 0.3 Compatibility with other management systems	**Introduction**	**0 Introduction** 0.1 General 0.2 Process approach	**0 Introduction** 0.1 General 0.2 Plan-Do-Check-Act Cycle	**Introduction**
1 Scope 1.1 General 1.2 Application	**1 Scope**	**1 Scope** 1.1 General 1.2 Application	**1 Scope**	**1 Scope**	**1 Scope of Standard**	**1 Scope**
2 Normative reference	**2 Normative reference**	**2 Normative references**	**2 Normative references**	**2 Normative references**	**2 Normative reference**	
3 Terms and definitions	**3 Terms and definitions**	**3 Terms and definitions**	**3 Terms and definitions**	**3 Terms and definitions**	**3 Terms and definitions**	**2 Terms and definitions**
ISO Standards						
ISO 9001:2008	**ISO 14001:2004**	**ISO 27001:2005**	**ISO 28000-2007**	**ANSI/ASIS SPC.1-2009**	**ASIS/BSI BCM.01-2010**	**BS 25999-2:2007**
4 Quality management system 4.1 General requirements **5 Management responsibility** 5.1 Management commitment 5.2 Customer focus 5.3 Quality policy 5.4 Planning 5.5 Responsibility, authority and communication	**4 Environmental management system requirements** 4.1 General requirements 4.2 Environmental policy	**4 Information security management system (ISMS)** 4.1 General requirements 4.2 Establishing and managing the ISMS 4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS 4.2.4 Maintain and improve the ISMS 5 Management responsibility 5.1 Management commitment	**4 Security management system elements** 4.1 General requirements 4.2 Security management policy	**4 Organizational resilience (OR) management system requirements** 4.1 General requirements 4.1.1 Scope of OR management system 4.2 Organizational resilience (or) management policy 4.2.1 Policy statement 4.2.2 Management commitment	**4 Business continuity management system requirements**. 4.1 General Requirements 4.2 Establishing the context 4.3 Policy and management commitment	**3 Planning the business continuity management system** 3.1 General 3.2 Establishing and managing the BCMS 3.2.1 Scope and objectives of BCMS 3.2.2 BCM policy 3.2.3 Provision of resources 3.2.4 Competency of BCM personnel

7 Product realization 7.1 Planning of product realization 7.2 Customer-related processes 7.2.1 Determination of requirements related to the product 7.2.2 Review of requirements related to the product	**4.3 Planning** 4.3.1 Environmental aspects 4.3.2 Legal and other requirements 4.3.3 Objectives, targets and program(s)	**4.2 Establishing and managing the ISMS** 4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS	**4.3 Security risk assessment and planning** 4.3.1 Security risk assessment 4.3.2 Legal, statutory and other security regulatory requirements 4.3.3 Security management objectives 4.3.4 Security management targets 4.3.5 Security management programmes	**4.3 Planning** 4.3.1 Risk assessment and impact analysis 4.3.2 Legal and other requirements 4.3.3 Objectives, targets, and program(s)	**4.4 Planning** 4.4.1 Business impact analysis and risk assessment 4.4.1.1 Business impact analysis 4.4.1.2 Risk assessment 4.4.2 Business continuity objectives and targets 4.4.3 Business continuity strategies	**4 Implementation and operation of the BCMS** 4.1 Understanding the organization 4.1.1 Business impact analysis 4.1.2 Risk assessment 4.1.3 Determining choices Determining business continuity strategy
ISO Standards						
ISO 9001:2008	**ISO 14001:2004**	**ISO 27001:2005**	**ISO 28000-2007**	**ANSI/ASIS SPC.1-2009**	**ASIS/BSI BCM.01-2010**	**BS 25999-2:2007**
6 Resource management 6.1 Provision of resources 6.2 Human resources 6.2.2 Competence, training and awareness 6.3 Infrastructure 6.4 Work environment 7.2.3 Customer communication 4.2 Documentation requirements 4.2.1 General 4.2.2 Quality manual 4.2.3 Control of documents 7.3 Design and development 7.4 Purchasing 7.5 Product and service provision	**4.4 Implementation and operation** 4.4.1 Resources, roles, responsibility and authority 4.4.2 Competence, training, and awareness 4.4.3 Communication and warning 4.4.4 Documentation 4.4.5 Control of documents 4.4.6 Operational control 4.4.7 Emergency preparedness and response	**5.2 Resource management** 5.2.1 Provision of resources 5.2.2 Training, awareness and competence 4.3 Documentation requirements 4.3.1 General 4.3.2 Control of documents	**4.4 Implementation and operation** 4.4.1 Structure, authority and responsibilities for security management 4.4.2 Competence, training and awareness 4.4.3 Communication 4.4.4 Documentation 4.4.5 Document and data control 4.4.6 Operational control 4.4.7 Emergency preparedness, response and security recovery	**4.4 Implementation and operation** 4.4.1 Resources, roles, responsibility, and authority 4.4.2 Competence, training, and awareness 4.4.3 Communication and warning 4.4.4 Documentation 4.4.5 Control of documents 4.4.6 Operational control 4.4.7 Incident prevention, preparedness, and response	**4.5 Implementation and operation** 4.5.1 Resources 4.5.2 Roles, responsibility and authority 4.5.3 Competence, training and awareness 4.5.4 Documentation 4.5.5 Control of documents 4.5.6 Developing and implementing a business continuity response 4.5.6.1 Response structure 4.5.6.2 Business continuity plans 4.5.7 Communication and notification	**4.3 Developing and implementing a BCM response** 4.3.1 General 4.3.2 Incident response structure 4.3.3 Business continuity plans and incident management plans 3.2.4 Competency of BCM personnel 3.3 Embedding BCM in the organization's culture 3.4 BCMS documentation and records 3.4.2 Control of BCMS records 3.4.3 Control of BCMS documentation
8 Measurement, monitoring and improvement 8.1 General 8.2 Monitoring and measurement 8.2.2 Internal audit 8.2.3 Monitoring and measurement of processes 8.2.4 Monitoring and measurement of product 8.3 Control of nonconforming product 8.5.3 Corrective actions 8.5.3 Preventive actions 4.2.4 Control of records 8.4 Analysis of data	**4.5 Checking** 4.5.1 Monitoring and measurement 4.5.2 Evaluation of compliance 4.5.3 Non- conformity, corrective action and preventive action 4.5.4 Control of records 4.5.5 Internal audits	4.2.3 Monitor and review the ISMS 8.2 Corrective action 8.3 Preventive action 4.3.3 Control of records 6 Internal ISMS audits	**4.5 Checking and corrective action** 4.5.1 Security performance measurement and monitoring 4.5.2 System evaluation 4.5.3 Security-related failures, incidents, non-conformances and corrective and preventive action 4.5.4 Control of records 4.5.5 Audit	**4.5 Checking (evaluation)** 4.5.1 Monitoring and measurement 4.5.2 Evaluation of compliance and system performance 4.5.2.1 Evaluation of compliance 4.5.2.2 Exercises and testing 4.5.3 Nonconformity, corrective action, and preventive action 4.5.4 Control of records 4.5.5 Internal audits	**4.6 Checking and corrective action** 4.6.1 Monitoring and measurement 4.6.2 Evaluation of conformance and system performance 4.6.2.1 Evaluation of conformance 4.6.2.2 Exercises and testing 4.6.3 Non-conformity, corrective action and preventive action 4.6.4 Control of records 4.6.5 Internal audits	**4.4 Exercising, maintaining and reviewing BCM arrangements** 4.4.1 General 4.4.2 BCM exercising 4.4.3 Maintaining and reviewing BCM arrangements **5 Monitoring and reviewing BCMS** 5.1 internal audit **6 Maintaining and improving the BCMS** 6.1 Preventive and corrective actions

ISO Standards						
ISO 9001:2008	**ISO 14001:2004**	**ISO 27001:2005**	**ISO 28000-2007**	**ANSI/ASIS SPC.1-2009**	**ASIS/BSI BCM.01-2010**	**BS 25999-2:2007**
5.6 Management review 8.5 Improvement 8.5.1 Continual improvement	**4.6 Management review**	**7 Management review of the ISMS** 7.1 General 7.2 Review input 7.3 Review output 4.2.4 Maintain and improve 8 ISMS improvement 8.1 Continual improvement he ISMS	**4.6 Management review and continual improvement**	**4.6 Management review** 4.6.1 General 4.6.2 Review input 4.6.3 Review output 4.6.4 Maintenance 4.6.5 Continual improvement	**4.7 Management review** 4.7.1 General 4.7.2 Review input 4.7.3 Review output 4.7.4 Opportunities for improvement	**5.2 Management review of the BCMS** 5.2.1 General 5.2.2 Review Input 5.2.3 Review output 6.2 Continual improvement
Annex A Correspondence between ISO 9001:2000 and ISO 14001:2004 Annex B Changes between ISO 9001:2000 and ISO 9001:2008	**Annex A Guidance on the use of this International Standard Annex B Correspondence between ISO 14001:2004 and ISO 9001:2000**	**Annex A Control objectives and controls Annex B OECD principles and this International Standard Annex C Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard**		**Annex A Guidance on the use of the standard Annex B Compatibility with other management systems Annex C Terminology conventions Annex D Glossary Annex E Qualifications Annex F Bibliography**	**Annex A Guidance on the use of this Standard Annex B Compatibility with other management system standards and PS-Prep standards C Terminology convention D Glossary E Bibliography**	**Annex A Correspondence with BS EN ISO 9001:2000, BS EN ISO 14001:2004, BS ISO/IEC 27001:2005**
Management System Standard	**Management System Standard**	**Management System Standard**	**Management System Standard**	**Management System Standard**	**Management System Standard**	**Management System Standard**

ANNEXURE G: ASIS SELF-ASSESSMENT SCORECARD FOR ORMS

***ANSI/ASIS SPC.1-2009 ORGANISATIONAL RESILIENCE: SECURITY, PREPAREDNESS AND CONTINUITY MANAGEMENT SYSTEMS: REQUIREMENTS WITH GUIDANCE FOR USE*. SELF ASSESSMENT SCORECARD**

Criteria	Level of Conformance						Opportunity for Improvement	Score
	0	1	2	3	4	5		
	Nonexistent	Conducted Ad-Hoc	Partially Developed	Process Evident but Fails to meet Criteria in Systems Development	Need For Improvement in Systems Development	Full Conformance with Standard Requirements		
4.1.1 Define Scope of ORMS								
Scope of the ORMS defined and documented appropriate to the size, nature, and complexity of the Organisation.								
Internal and external context and obligations (including legal responsibilities) considered in setting scope.								
Consider critical operational objectives, assets, functions, services, and products.								
Potential internal and external events, as well as unforeseen events and their potential impact that could adversely affect the critical operations and functions of the Organisation considered in setting scope.								
Strategic weighting of likelihood and/or consequence reduction strategies defined based on the risk assessment and impact analysis.								

4.2.1 Policy								
Top management defined, documented and provided resources for the Organisation's ORMS policy appropriate to the nature and scale of potential risks.								
Iincludes a commitment to continual improvement and risk prevention, reduction and mitigation								
Includes a commitment to comply with applicable legal requirements and with other requirements to which the Organisation subscribes								
Provides framework for setting and reviewing IPOCM objectives and targets								
Communicated to all persons working for or on behalf of the Organisation								
Reviewed at planned intervals and when significant changes occur								
Documented, implemented and maintained								
4.2.2 Management Commitment								
Management provided evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement								
Establish policy, targets and objectives								
Establish roles, responsibilities and competencies								
Appointed person(s) responsible for the ORMS								
Communicate to Organisation importance of ORMS								
Provide sufficient resources to establish, implement, operate, monitor, review, maintain and improve ORMS								
Set the criteria for accepting risks and the acceptable levels of risk								
Management participation in ORMS								
4.3.1 Risk Assessment and Impact Analysis								
Formal and documented process for risk assessment and impact analysis established, implemented, and maintained.								
Asset identification and valuation conducted to identify the Organisation's critical activities, functions, services, products, partnerships, supply chains, stakeholder relationships, and the potential impact of disruptions.								
Risk identification (threat assessment, vulnerability assessment, criticality assessment) conducted considering intentional, unintentional and naturally-caused disruptions.								

Systematic risk analysis conducted.								
Systematic risk evaluation conducted								
Recovery time objectives and priorities determined								
Cost-benefit analysis for risk treatment conducted.								
Risk assessment taken into account in establishing, implementing, and operating the ORMS								
Risk assessment e-evaluated with changing context.								
Risk assessment inputs and outputs documented and kept up to date and confidential.								
4.3.2 Legal and Other Requirements								
Procedures established and maintained to identify legal, regulatory, and other requirements to which the Organisation subscribes related to the Organisation's risks, assets, activities, functions, products, services, supply chain, the environment, and stakeholders								
Procedures established and maintained to determine how these requirements apply to the Organisation.								
Information documented and keep it up to date.								
Applicable legal, regulatory, and other requirements to which the Organisation subscribes considered in ORMS.								
4.3.3 Objectives, Targets and Programmes								
Documented objectives and targets established and maintained to avoid, prevent, protect from, mitigate, respond to, and recover from disruptive incidents.								
Programs based on risk assessment and impact analysis; and consistent with ORMS policy.								
Establish expectations for other ORGANISATIONAL relationships outside the boundary of the Organisation (such as suppliers) that are critical to mission accomplishment and functional operations.								
Objectives and targets are measurable.								
Risk treatment options selected based on legal, regulatory, and other requirements; risk assessment; technological options; its financial, operational, and business requirements; mutual aid agreements; and the views of stakeholders and other interested parties.								
Programs include designation of responsibility and resources for achieving								

objectives and targets at relevant functions and levels of the Organisation.								
Programs designate a means and time-frame.								
Establish and maintain program for prevention and deterrence - Avoid, eliminate, deter, or prevent the likelihood of a disruptive incident and its consequences.								
Establish and maintain program for mitigation - minimize the impact of a disruptive incident								
Establish and maintain program for emergency response - the initial response to a disruptive incident involving the protection of people and property from immediate harm.								
Establish and maintain program for continuity - processes, controls, and resources are made available to ensure that the Organisation continues to meet its critical operational objectives.								
Establish and maintain program for recovery - processes, resources, and capabilities of the Organisation are re-established to meet ongoing operational requirements within the time period specified in the objectives.								
4.4.1 Resources, Roles, Responsibility and Authority								
Management shall ensure the availability of resources essential for the implementation and control of ORMS.								
Roles, responsibilities, and authorities defined, documented, and communicated for effective ORM.								
Top management appointed specific ORMS management representative(s)								
ORM team established with appropriate authority to oversee incident prevention and management.								
Logistical capabilities and procedures established to locate, acquire, store, distribute, maintain, test, and account for services, personnel, resources, materials, and facilities produced or donated to support ORMS.								
Resource management objectives established for response times, personnel, equipment, training, facilities, funding, insurance, liability control, expert knowledge, interdependencies, materials, and the time frames within which they will be needed.								
Procedures established for stakeholder assistance, communications, strategic alliances, and mutual aid.								

Financial and administrative procedures established to support the ORM program before, during, and after an incident.								
4.4.2 Competence, Training and Awareness								
Ensured that any persons performing tasks who have the potential to prevent, cause, respond to, mitigate, or be affected by significant risks are competent (based on appropriate education, training, or experience).								
Identify training competencies and needs associated with incident prevention and management; and ORMS.								
Provide training or take other action to meet these needs and retain associated records.								
Establish, implement, and maintain procedures to ensure persons working for it or on its behalf are aware of: a) The significant hazards, threats, and risks, and related actual or potential impacts, associated with their work and the benefits of improved personal performance; b) The procedures for incident prevention, deterrence, mitigation, self-protection, evacuation, response, continuity, and recovery; c) The importance of conformity with the ORM policy and procedures and with the requirements of the ORMS; d) Their roles and responsibilities in achieving conformity with the requirements of the ORMS; e) The potential consequences of departure from specified procedures; and f) The benefits of improved personal performance.								
Build, promote, and embed an ORM culture that: a) Ensures the ORM culture becomes part of the Organisation's core values and Organisation governance; and b) Makes stakeholders aware of the ORM policy and their role in any plans.								
4.4.3 Communication and Warning								
Procedures established, implemented and maintained for internal communication and consultation between the various levels and functions of the Organisation.								
Procedures established, implemented and maintained for external communication and consultation with partner entities and other stakeholders.								
Procedures established, implemented and maintained for receiving,								

documenting, and responding to communication from external stakeholders								
Procedures established, implemented and maintained for adapting and integrating a national or regional risk or threat advisory system into planning and operations.								
Procedures established, implemented and maintained for alerting stakeholders potentially impacted by an actual or impending disruptive incident.								
Procedures established, implemented and maintained for assuring availability of the means of communication during a crisis situation and disruption.								
Procedures established, implemented and maintained for facilitating structured communication with emergency responders.								
Procedures established, implemented and maintained assuring the interoperability of multiple responding Organisations and personnel								
Procedures established, implemented and maintained for recording of vital information about the incident, actions taken, and decisions made.								
Procedures established, implemented and maintained for operations of a communications facility.								
Procedures established, implemented and maintained for external communication, alerts, and warnings (including with the media).								
Communications systems tested regularly.								
4.4.4 Documentation								
Documentation includes: a) The ORM policy, objectives, and targets; b) Description of the scope of the ORMS; c) Description of the main elements of the ORMS and their integration with related documents; d) Documents, including records, required by the Standard; e) Documents, including records, determined by the Organisation to be necessary to ensure the effective planning, operation, and control of processes that relate to its significant risks.								

4.4.5 Control of Documentation								
Establish, implement, and maintain (a) procedure(s) to: a) Approve documents for adequacy prior to issue; b) Review, update and re-approve documents as necessary; c) Ensure that changes and the current revision status of documents are identified; d) Ensure that relevant versions of applicable documents are available at points of use; e) Establish document retention and archival parameters; f) Ensure that original and archival copies of documents, data, and information remain legible and readily identifiable; g) Ensure that documents of external origin determined by the Organisation to be necessary for the planning and operation of the ORMS are identified and their distribution controlled; h) Identify as obsolete all out-of-date documents that the Organisation is required to retain; and i) Ensure the integrity of the documents by ensuring they are tamperproof, securely backed-up, accessible only to authorized personnel, and protected from damage, deterioration, or loss.								
4.4.6 Operational Control								
Operating criteria stipulated by establishing, implementing, and maintaining documented procedures to minimizing the likelihood and/or consequences of a disruptive incident related to the Organisation's internal and external activities.								
Adaptive and proactive procedures established, implemented, documented and maintained for operations related to the identified risks to the activities, functions, products, and services of the Organisation and communicating applicable procedures and requirements to suppliers (including contractors).								
Procedures established, implemented and maintained related to control potential incidents consistent with the ORM policy, risk assessment, objectives, and targets.								
Establish, implement and maintain procedures to address reliability and resiliency, the safety and health of people, and the protection of property and the environment impacted by a disruptive incident.								

4.4.7 Incident Prevention, Preparedness, and Response								
Procedures established, implemented, and maintained to prevent and manage disruptive events that have the potential to harm the Organisation and its supply chain partners based on risk assessment.								
Procedures established, implemented, documented and maintained to: a) avoid, remove or reduce the likelihood of a disruptive event; b) reduce the consequences of a disruptive event; c) protect people, physical assets and critical information including records from immediate harm; d) maintain continuity of essential services; and e) recover from a disruptive event.								
Develop and implement incident prevention and management procedures to minimize the likelihood of a disruptive event or to minimize the potential for the severity of the consequences of the event. a) Prevention procedures should describe how the Organisation will take proactive steps to protect its assets by establishing architectural, administrative, design, operational and technological approaches to avoid, eliminate or reduce the likelihood of risks materializing, including the protection of assets from unforeseen threats and hazards. b) Mitigation procedures should describe how the Organisation will take proactive steps to protect its assets by establishing immediate, interim and long-term approaches to reduce the consequences of risks before they materialize, including the protection of assets from unforeseen threats and hazards.								
Develop and implement response plans that describe how the Organisation will respond to one or more types of disruptive event.								
Develop and implement continuity plans that describe how the Organisation will maintain and/or re-establish critical activities in the period immediately following the response/emergency phase.								
Develop and implement incident prevention and management procedures with regard to: a) The nature of onsite hazards (e.g., flammable and toxic materials, storage tanks and compressed gases) and measures to be taken in the event of a disruptive incident or accidental releases;								

b) The nature of local, nearby, or other external hazards with a potential impact on the Organisation; c) The most likely type and scale of a disruptive incident; d) Procedures to prevent environmental damage,								
Develop and implement incident response and management procedures with regard to: a) The most appropriate method(s) for mitigation and emergency response to a disruptive incident to avoid escalation to a crisis or disaster; b) Command and control procedures for and structure of pre-defined chain of command, (an) emergency operations centre(s), and/or (an) alternate worksite(s); c) Procedures and authority to declare an emergency situation, initiate emergency procedures, activate plans and actions, assess damage, and make financial decisions; d) Internal and external communication plans including notification of appropriate authorities and stakeholders; e) Procedures to acquire and/or provide appropriate medical care; f) The action(s) required to minimize human casualties, and physical and environmental damage; g) The action(s) required to secure vital information, information systems, facilities, and people; h) Mitigation and response action(s) to be taken for different types of disruptive incident(s) or emergency situation(s); i) The need for (a) process(es) for post-event evaluation to establish and implement corrective and preventive actions; j) Periodic testing of incident and emergency management and response procedure(s) and processes;								
Develop and implement incident management procedures addressing: a) Training of incident and emergency response personnel; b) A list of key personnel and aid agencies, including contact details (e.g., fire department, emergency medical services, law enforcement, hazardous material clean-up services); c) Evacuation routes and assembly points including lists of personnel and contact details; d) The potential for (a) disruptive incident or emergency situation(s) to affect								

or be affected by critical infrastructure (e.g., electricity, water, communications, transportation); e) The possibility of mutual assistance to and from neighbouring Organisations.								
Develop and implement recovery plans that describe how the Organisation will re-establish all necessary operational and support activities, replace damaged and/or destroyed assets and information, rebuild the brand and reputation of the Organisation, and assist staff to recover from the event..								
Periodically review and, where necessary, revise its incident prevention and management procedures - in particular, after the occurrence of accidents or incidents that can escalate into an emergency, crisis, or disaster.								
Ensure that any person(s) performing incident prevention and management measures on its behalf are competent on the basis of appropriate education, training, or experience, and retain associated records.								
Document this information and updated it at a regular interval or as changes occur.								
4.5 Checking								
ORM plans, procedures, and capabilities evaluated through periodic assessments, testing, post-incident reports, lessons learned, performance evaluations, and exercises. Significant changes in these factors are reflected immediately in the procedures.								
Keep records of the results of the periodic evaluations.								
4.5.1 Monitoring and Measurement								
Performance metrics and procedures established, implemented, and maintained to monitor and measure, on a regular basis, those characteristics of its operations that have material impact on its performance (including partnership and supply chain relationships).								
Documented information to monitor performance, applicable operational controls, and conformity with the Organisation's ORM objectives and targets.								
Performance of procedures and systems which protect its assets, activities, communications and information systems, evaluated, documented and reviewed.								

4.5.2.1 Evaluation of Compliance								
Procedures for periodically evaluating compliance with applicable legal, regulatory and other requirements to which it subscribes established, implemented, and maintained								
Non-conformances in compliance are reviewed and address with corrective and preventive actions.								
Keep records of the results of the periodic evaluations								
4.5.2.2 Exercises and Testing								
Exercise and testing procedures established, implemented, documented and maintained to evaluate the appropriateness and efficacy of ORMS, its programs, processes, and procedures (including partnership and supply chain relationships).								
Validate the ORMS using exercises and testing that: a) Are consistent with the scope of the ORMS and objectives of the Organisation; b) Are based on realistic scenarios that are well planned with clearly defined aims and objectives; c) Minimize the risk of disruption to operations and the potential to cause risk to operations and assets; d) Produce a formalized post-exercise report that contains outcomes, recommendations, and arrangements to implement improvements in a timely fashion; e) Are reviewed within the context of promoting continual improvement; and f) Are conducted at planned intervals, and from time to time on a non-periodic basis as determined by the management of the Organisation, as well as when significant changes occur within the Organisation and the environment it operates in.								
4.5.3 Nonconformity, Corrective Action, and Preventive Action								
Procedures established, implemented, and maintained for dealing with actual and potential nonconformities and for taking corrective action and preventive action.								
Procedures established that define requirements for: a) Identifying and correcting nonconformity(ies) and taking action(s) to mitigate their impacts;								

b) Investigating nonconformity(ies), determining their cause(s), and taking actions in order to avoid their recurrence; c) Evaluating the need for action(s) to prevent nonconformity(ies) and implementing appropriate actions designed to avoid their occurrence; d) Recording the results of corrective action(s) and preventive action(s) taken; and e) Reviewing the effectiveness of corrective action(s) and preventive action(s) taken.								
Actions taken are appropriate to the impact of the potential problems, and conducted in an expedited fashion.								
Identify changed risks, and identify preventive action requirements focusing attention on significantly changed risks.								
Priority of preventive actions are determined based on the results of the risk assessment and impact analysis.								
Make any necessary changes to the ORMS documentation.								
4.5.4 Control of Records								
Establish and maintain records to demonstrate conformity to the requirements of its ORMS and of the Standard and the results achieved.								
Establish, implement, and maintain (a) procedure(s) to protect the integrity of records including access to, identification, storage, protection, retrieval, retention, and disposal of records.								
Records are legible, identifiable, and traceable.								
4.5.5 Internal Audits								
ORM audit program and procedures established, implemented and maintained ensure that internal audits of the ORMS are conducted at planned intervals.								
Audit procedures determine whether objectives, controls, processes, and procedures of its ORMS:: a) Conform to the requirements of the Standard and relevant legislation or regulations; b) Conform to risk management requirements; c) Are effectively implemented and maintained; and d) Perform as expected.								
Audit criteria, scope, frequency, and methods are defined.								

Selection of auditors and conduct of audits ensures objectivity and impartiality of the audit process.								
Responsibilities and requirements for planning and conducting audits, reporting results and maintaining records are defined in a documented procedure.								
Management ensures actions taken without delay to eliminate detected nonconformities and their causes.								
Follow-up activities include the verification of the actions taken and the reporting of verification results.								
4.6 Management Review								
Management reviews ORMS system at planned intervals to ensure its continuing suitability, adequacy, and effectiveness.								
Review includes assessing opportunities for improvement and the need for changes to ORMS, including the ORMS policy and objectives.								
Input to management review includes: a) Results of ORMS audits and reviews; b) Feedback from interested parties; c) Techniques, products, or procedures that could be used in the Organisation to improve the ORMS performance and effectiveness; d) Status of preventive and corrective actions; e) Results of exercises and testing; f) Vulnerabilities or threats not adequately addressed in the previous risk assessment; g) Results from effectiveness measurements; h) Follow-up actions from previous management reviews; i) Any changes that could affect the ORMS; j) Adequacy of policy and objectives; and k) Recommendations for improvement.								
Output from the management review includes any decisions and actions related to the following: a. Improvement of the effectiveness of the ORMS; b. Update of the risk assessment, impact analysis, and incident preparedness and response plans; c. Modification of procedures and controls that effect risks, as necessary, to								

respond to internal or external events that may impact on the ORMS, including changes to: i. Business and operational requirements; ii. Risk reduction and security requirements; iii. Operational conditions processes effecting the existing operational requirements; iv. Regulatory or legal requirements; v. Contractual obligations; vi. Levels of risk and/or criteria for accepting risks. d. Resource needs; and e. Improvement to how the effectiveness of controls is being measured.								

4.6.4 Maintenance								
Top management establishes a defined and documented ORMS maintenance program to ensure that any internal or external changes that impact the Organisation are reviewed in relation to the ORMS.								
Identify any new critical activities that need to be included in the ORMS maintenance program.								
4.6.5 Continual Improvement								
Continually improve the effectiveness of the ORMS through the use of the ORM policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review.								

(ASIS ORMS SELF-ASSESSMENT FORM: Used with permission of ASIS International)

ANNEXURE H: POSITION ADVERITISEMENT: ORGANISATIONAL RESILIENCE PROGRAMME MANAGER

Organisational Resilience Programme Manager

Level: VP level

Status: Full-time, Permanent

Location: Singapore: Local Candidates Preferred. No Relocation Assistance Provided

Salary: Based on Experience

Agency: BC Management, Inc: Job Posting #2313

Role Description: This position is the primary coordinator of all business continuity, crisis management and emergency management activity at one of Singapore's Significantly Important Institutions, as defined by the Monetary Authority of Singapore. The Organisation's business is driven by information technology. The position reports to an Executive Vice President of the company. The single most important skill the company seeks, is the ability to inspire colleagues to care about preparation, mitigation, response and recovery planning. The company wants someone with gravitas, someone who can lead by example, someone who can show a record of excitement and commitment to all facets of Organisational Resilience. The person must be able to make a no-nonsense presentation to the Executive Committee, be able to discuss BCM strategy with a unit head, and pay attention the details of a departmental BIA.

Strategic responsibilities

- Business continuity, crisis- and emergency management, and physical security for a medium-sized non-manufacturing company with high visibility.
- Develop, manage and evaluate progress on a 5-year 'road map' toward uninterruptible operation.
- Review & refine corporate BCM Policy as the Organisation grows and develops.
- Be the champion for enterprise contingency planning across all departments.

- Act as resilience liaison among business, operations and technology units and functions.
- Engage the company's executives and Board members in supporting Organisational Resilience.
- Lead, inspire and cajole industry partners to achieve fewer interruptions and faster recovery.
- Develop & execute a continuing resilience awareness program for company employees.
- Determine training requirements and deliver appropriate training for senior executives, departmental BCM coordinators and other employees.
- Determine self-assessed risks of the Organisation for BCM and provide appropriate directions to mitigate the risks.
- Ensure compliance to the MAS Business Continuity guidelines at all times and liaise with MAS as needed and forge a working relationship.

Tactical Responsibilities Note: some tasks may be assigned to or performed, in part, by a contractor and designated BCM coordinators from different units within the enterprise.

Business continuity

- Understand the business well enough to maintain current list of 'critical' processes and departments.
- Update BIAs at least once a year, complete BIAs for new units and teams
- Review continuity strategies, looking for consolidation opportunities and cost savings.
- Participate in selection, build-out of suitable recovery site(s) (not including IT disaster recovery)

- Manage updating of departmental business continuity plans and related documents.
- Exercise & test business continuity plans, data centre recovery plans.
- Oversee maintenance of recovery sites, EOCs & command centres, including key service providers.
- Manage compliance with regulatory mandates for business continuity.

Disaster Recovery

- Work closely with I.T. disaster recovery teams to ensure alignment with business continuity plans.

Crisis management

- Organize, evaluate and report on regular crisis management exercises.

Emergency management

- Maintain & text emergency notification system (ENS).
- Liaison with public-sector emergency services.

Security

- Annual facilities security risk assessment & review.
- Liaison with property managers where company has facilities.

Operational Responsibilities

- BCM Committee meetings: scheduling, arrangements, minutes.
- Ensure Unit Coordinators are continuously engaged and are prepared to meet continuity challenges." (Continuity Central. 2010).

ANNEXURE I: MATURITY MODEL FOR THE PHASED IMPLEMENTATION OF THE *ANSI/ASIS SPC.1-2009 ORGANIZATIONAL RESILIENCE: SECURITY, PREPAREDNESS AND CONTINUITY MANAGEMENT SYSTEMS – REQUIREMENTS WITH GUIDANCE FOR USE*

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
Generic Concepts	Key elemental theme	Description of element	- No formal incident or resilience management - Actions are reactionary in nature - Not yet recognizing the importance of elements	- Initiates a project to address specific issue(s) by partially implementing core elements - Actions generally reactionary in nature focusing on pre-identified issue(s). - Recognizes the importance of elements and the need for some pre-planning - May be in reaction to an incident or near miss or be driven by external concerns	- Establishes a division or Organisation wide program to address resilience issues by partially implementing core elements - Recognizes the importance of elements and the need for pre-planning, however focus is on individual elements and not their interrelationship and integration - May be in reaction to an incident or near miss or be driven by external concerns - Risk management applications selected for their chances of demonstrating success - Program driven by "Program Manager" who applies a program management approach	- Resilience management is viewed as a matter of strategic value to the Organisation - Focuses on integration and interrelationships between core elements - Focuses on proactive management of risks to minimize both likelihood and consequences of a disruptive incident - Resilience management is viewed as part of a continual improvement process using PDCA model - Managing risk is seen as important at all levels and roles in Organisation - Integration and feedback loops of systems approach ensures effective	- The Organisation is conformant with the requirements of the standard - The Organisation establishes, documents, implements, maintains, and continually improves an Organisation resilience management system in accordance with the requirements of the ORMS Standard, and determines how it will fulfill the requirements. - Examines the linkages and interactions between the elements that compose the entirety of the system - Manages risk using balanced strategies to adaptively, proactively and reactively address minimization of both likelihood and consequences of disruptive events - Resilience management becomes	- The Organisation goes beyond conformance to the standard to fully integrate resilience management into its overall risk management strategy - The Organisation emphasizes enterprise-wide and supply chain relationships in all aspects of it resilience management system. - The Organisation mentors other stakeholder (in its supply chain and community) recognizing that Organisational resilience is an integral part of community resilience - Resilience management culture is well developed and considered a inseparable part of

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
						learning from experiences - Resilience management culture is developing and part of decision making	part of the routine management of projects and business processes	decision making - Resilience management and systems principles are expanded to all areas of business and activities
4.1.1 Scope of OR Management System	- Understands the Organisation and its context - Scope of ORMS	- Establishes the internal, external and risk management context of the Organisation - Defines scope and boundaries for development and implementation of ORMS.	- No formal process - No definition of scope or internal or external context - No clear concept of business context or benefits	- Projects of limited scope focusing on one or a limited number of issues identified as of particular or immediate interest - Internal and external context and interactions considered within project scope definition	- Programs are established to address core elements based on evaluation of the internal, external and resilience management context of all or part of the Organisation - Scope defined based on protecting and preserving critical activities, functions and services	- Organisation defines and documents the internal, external and resilience management context - Critical operational objectives, assets, activities, functions, services, and products are defined - Boundaries of scope are defined and documented based on protecting and preserving critical activities, functions and services, as well as relations with stakeholders - Weighting of risk management strategies is defined	- Organisation defines and documents the internal, external and resilience management context, as well as Organisation-wide risk management interactions - Boundaries of scope defined and documented considering the Organisation's mission, goals, internal and external obligations, and legal responsibilities	- Organisation defines and documents the internal, external and resilience management context, as well as enterprise-wide risk management interactions and supply chain tier, commitments and relationships - Boundaries of scope defined and documented

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
4.2.1 Policy Statement	- Setting a policy framework	- Establishes a policy to provide a framework for setting objectives and provide the direction and principles for action. - Demonstrates management commitment	- No defined policy - Lack of top level governance	- Policy limited to addressing identified issue(s) - Driven by "Project Leader", may or may not have top management involvement beyond approval of project	- Drafted by "Program Manager" and signed by top management - Policy addresses resilience management in divisions defined in scope - Communicates to relevant divisions	- Policy establishes framework for resilience management by setting objectives and providing direction - Endorsed by top management - Communicated throughout Organisation	- Policy establishes framework for resilience management by setting objectives and providing direction - Clear commitment to comply with applicable legal and other requirements - Endorsed and promoted by top management - Communicated throughout Organisation and to stakeholders making them aware of content and meaning	- Policy establishes framework for internal and external resilience management by setting objectives and providing direction - Clear commitment to comply with applicable legal and other requirements - Endorsed and promoted by top management - Communicated throughout Organisation, enterprise and supply chain
4.2.2 Management Commitment	- Management mandate and commitment	-Demonstrates top management and the Organisation's commitment to meeting the requirements of resilience management. - Establishes the project to address resilience management including the provision of appropriate resources and authorities for conduct project.	- Management ambivalent to unreceptive - Concerned that acknowledging risk and uncertainty may be seen of admission of problems or weakness - No guidance from the top or Organisation - Ad hoc leadership - Ostrich effect	- Management authorization and resources provided to "Project Leader" to conduct project including in-house training and/or external expertise - Resources restricted to address limited scope. - Resource allocation liked to perceived return on investment - Project aims to encourage more management	- Top management sponsorship - Endorsement of established programs for resilience management - One or more individuals appointed as Project Manager - Set asset prioritization and timeframes for recovery in event of disruption - Resources allocated to support program	- Top management participation - Visible endorsement of top management - Establishes an ORMS policy - One or more individuals appointed to be responsible for ORMS - Decides criteria for accepting risk, acceptable levels of risk - Sets asset prioritization and timeframes for	- Documents evidence of its mandate and commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ORMS - Defines and documents criteria to be used to evaluate the significance of risk, determination of appropriate risk treatments, and setting of timeframes for recovery - Sufficient resources	- Documents evidence of its mandate and commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ORMS - Defines and documents criteria to be used to evaluate the significance of risk, determination of appropriate risk treatments, and setting of timeframes

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
				support and buy-in		recovery in event of disruption - Resources allocated to support system	allocated and competencies assured	for recovery for the Organisation and relevant stakeholders
4.3.1 Risk Assessment and Impact Analysis	- Identification and valuation of asset, activities, functions and services - Risk identification - Risk Analysis - Risk Evaluation	- Establishes a process for risk identification, analysis and evaluation. - Identifies assets, activities, needs, requirements and analysis of critical issues related to business disruption risks that are relevant to the Organisation and stakeholders. - Identifies hazards threats, vulnerabilities and consequences. - Evaluates the effect of uncertainty on the Organisation's objectives. - Evaluates the likelihood of a disruptive event and its consequences on assets (human, physical, cyber, environmental, information, and intangible). - Evaluates dependencies and interdependencies with other assets and sectors, and consequences a disruptive event. - Evaluates and establishes timeframes for response and recovery.	- No formal process - Indications of problems, near misses and warning signs identified in an ad hoc manner as they materialize - Risks are identified after they materialize	- No formal process - Reactive in nature with issue(s) addressed having been identified due to indications of problems, near misses, warning signs, an event, and/or external concerns - The analysis is more of a gap analysis than a risk assessment examining what is need to address project issues	- Develops and implements a procedure to identify, analyse and evaluate critical assets, risks, and impacts - Priorities based on outcomes of risk analysis or business impact analysis	- Establishes, implements, and maintains an ongoing formal and documented risk assessment process - Prioritizes risks and their impacts are taken into account in establishing, implementing, and operating the ORMS - Risk assessment and impact analysis recognized as providing the foundation for elements of the ORMS and for Organisational decision-making	- Establishes, implements, and maintains an ongoing formal and documented risk assessment process - Prioritizes risks and their impacts are taken into account in establishing, implementing, and operating the ORMS - Periodically reviews whether OR management scope, policy, and risk assessment are still appropriate given the Organisations' internal and external context - Re-evaluates risk and impacts within the context of changes within the Organisation or made to the Organisation's operating environment, procedures, functions, services, partnerships, and supply chains	- Establishes, implements, and maintains an ongoing formal and documented risk assessment process - Establishes, implements, and maintains a formal and documented communication and consultation process with stakeholders and supply chain partners in the risk assessment process - Establishes, implements, and maintains a formal and documented process for monitoring and reviewing the risk assessment process

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
4.3.2 Legal and Other Requirements	- Identifies legal, regulatory, and other requirements to which the Organisation subscribes - Determines how these requirements apply to the Organisation, its risks and their potential impacts.	- Identifies legal and other requirements which govern the Organisation's activity. - Establishes a procedure or process for identifying, registering and evaluating internal and external requirements pertinent to the Organisation's functions, activities and operations. - Understands and communicates the potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to location and industry.	-No understanding of legal and other requirements	- Informal process initiated to identify legal and other requirements related to identified issue being addressed - The main legal requirements applicable to the activities, functions and services in the scope of the project are identified	- Identifies legal and other requirements	- Establishes and maintains procedures to identify legal and other requirements - Determines how the legal and other requirements apply to the Organisation - Communicates requirements to appropriate parties	- Establishes and maintains procedures to identify legal and other requirements - Determines how the legal and other requirements apply to the Organisation risks and obligations - Ensures that applicable legal, regulatory, and other requirements are considered in developing, implementing, and maintaining its Organisational resilience management system - Documents information and keeps it up-to-date	- Establishes and maintains procedures to identify legal and other requirements relevant to the Organisation and appropriate stakeholders - Determines how the legal and other requirements apply to the Organisation and stakeholder risks and obligations
4.3.3 Objectives, Targets, and Program(s)	- Sets objectives and develops risk and incident prevention, protection, preparedness, mitigation, response, continuity and recovery management strategies - Risk prioritization	- Prioritizes the issues identified as a result of the risk assessment and impact analysis. - Sets objectives and targets (including time frames) based on the prioritization of issues within the context of an Organisation's policy and mission. - Develops strategic plans for incident prevention, protection, preparedness, mitigation, response, continuity and recovery.	- Objectives and targets not defined - No risk prioritization	- Defines targets and objectives based on the supporting demonstration of perceived factors for project success in dealing with identified issue(s) - Develops targets, objectives and programs to achieve immediate resilience performance improvement	- Resilience performance objectives for program management are set based on the risk assessment and impact analysis - Strategic action plans designate actions, responsibilities, accountability, resources and timeframes for achieving objectives	- Objectives shall be derived from and are consistent with the OR management policy and risk assessment - Documents objectives and targets to manage risks in order to avoid, prevent, protect, deter, mitigate, respond to, and recover from disruptive	- Documented objectives and targets are established to manage resilience by avoiding, accepting, removing the source, changing the likelihood, changing the consequences, sharing and/or retaining the risk - Objectives provide a basis for selecting one or more options for modifying risks considering asset value, opportunities for	- Documented objectives and targets establish internal and external expectations for the Organisation and its stakeholders that are critical to mission accomplishment, product and service delivery, and functional operations

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
	and treatment	- Identifies the resources needed and the availability of adequate human, infrastructure, processing and financial resources. - Identifies roles, responsibilities, authorities and their interrelationships within the Organisation as far as needed to ensure effective and efficient operations. - Plans the operational processes for actions effecting how the objectives and targets are achieved. - Makes internal and external arrangements, agreements, and contingency plans that need to be in place to manage foreseeable emergencies.		related to identified issue(s) and to demonstrate business benefit - Addresses issue(s) using rudimentary PDCA model approach focusing on limited scope - Action plans include actions necessary, required human and financial resources, responsibilities and timescales	and targets	incidents are established - Targets are measurable and derived from the objectives - Establishes and maintains one or more strategic programs (action plans) for prevention, protection, deterrence, mitigation, response, continuity and recovery - Strategic plans designate actions, responsibilities, accountability, resources and timeframes for achieving objectives and targets	reducing likelihood and/or consequences, cost/benefit, and tolerable levels of residual risk - Targets are measurable, achievable, relevant and time-based - Establishes, implements and maintains one or more program(s) for risk treatment in order to achieve its objectives and targets - Risk treatment options (defined in action plans) consider the prevention, protection, deterrence, mitigation, respond, and recover from disruptive incidents. The programs shall be optimized and prioritized in order to control and treat risks associated with threats, hazards and impacts of disruptions to the Organisation and its stakeholders	
4.4.1 Resources, Roles, Responsibility, and Authority	- Ensures the availability of resources essential for the implementation and control of the ORMS. - Roles,	- Establishes procedures, roles and responsibilities to cover all normal and abnormal operating conditions, including disruptions and emergencies. - Establishes management processes and procedures for human resources	- Not defined - No dedicated personnel for resilience management - Needed resources not identified - Lack of time, energy and	- Assigns roles and responsibilities to specific persons to address issue(s) in the limited scope - Allocates adequate resources in accordance with action plan	- Identifies and defines authorities, roles, responsibilities and appropriate resources within the Organisation - Identifies internal and external departments, division, business	- Top management appoints a specific management representative responsible for the ORMS - Formal resilience management responsibilities and relationships are	- Roles, responsibilities, and authorities are defined, documented, and communicated in order to facilitate effective Organisational resilience management, consistent with the	- Roles, responsibilities, and authorities are defined, documented, and communicated in order to facilitate effective Organisational resilience

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
	responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective OR management.	including employees, contractors, temporary staff, etc. - Identifies and assures availability of human, infrastructure and financial resources in the event of a disruption. - Establishes and documents provisions for adequate finance and administrative resources and procedures to support the management program or system normal and abnormal conditions. - Makes arrangements for supply chain obligations, mutual aid and community assistance. - Determines the local, regional and public authorities' roles, relationships and interactions with the Organisation's management system implementation plans.	resources to adequately prepare for and respond to disruptions	- A "Project Leader" is designated to oversee the conduct of the project - Participation based on project scope (only divisions and individuals within the scope actively engaged)	units and partners that will pay a role in addressing a disruptive incident - Identifies an incident management team and team leader - Allocates adequate resources in accordance with the action plan	defined and adhered to - Teams with defined roles and adequate resources are established to support resilience action plans - Establishes arrangements for stakeholder assistance, communication, strategic alliances and mutual aid - Identifies financial and administrative procedures needed to support the resilience programs and meet objectives and targets - Roles, relationships and interactions with local regional and public authorities (including first responders) are defined - Adequate resources allocated in accordance with action plan	achievement of its Organisational resilience management policy, objectives, targets and programs - Resilience, crisis, and response team(s) with defined roles, appropriate authority, and adequate resources to oversee incident management are established - Establishes logistical capabilities and procedures to locate, acquire, store, distribute, maintain, test, and account for services, personnel, resources, materials, and facilities produced or donated to support the Organisational resilience management system - Establishes procedures for stakeholder assistance, communications, strategic alliances, and mutual aid	management within the Organisation, enterprise-wide and within the community consistent with achieving Organisation, stakeholder, supply chain and community resilience objectives, targets and programs
4.4.2 Competence, Training, and Awareness	Awareness, competence and training strategies, plans,	- Identifies and establishes skills, competency requirements, and qualifications needed by the Organisation to	- Lack of cultural awareness - Competencies and skills not identified	- Competence, skills and training needs identified to achieve objectives and targets	- Determines competence requirements that are necessary for activities defined in	- Identifies competencies and training needs associated with achieving the	- Ensures that any person(s) performing tasks who have the potential to prevent, cause, respond to,	- Builds, promotes, and embeds a resilience management culture within the

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
	programs and procedures	maintain operations. - Assesses, develops and implements training/ and education program for the Organisation's personnel, contractors, and other relevant stakeholders. - Develops Organisational awareness and establish a culture to support resilience management. - Determines Organisational interface protocol, identification and training requirements and assign appropriate internal staff or support representatives. - Develops tools to enhance situational awareness.	- No formal training program - Little or no in-house expertise or experience - General workforce unaware of risk management needs and lack training to adequately take ownership and control risks	- Conducts training with some measure of competence to achieve objectives and targets - Focuses on addressing the identified issue(s) in the scope - Emphasizes awareness within the scope of the project	programs - Develops and implements an awareness program	resilience objectives, targets and programs - Develops and implements a program to address competence and training needs - Assesses competence against requirements and ensure they are met	mitigate, or be affected by significant hazards, threats, and risks are competent (on the basis of appropriate education, training, or experience - Retains associated training and competence records - Builds, promotes, and embeds a resilience management culture within the Organisation	Organisation, enterprise, supply chain and community - Ensures that the resilience management culture becomes part of the Organisation's core values and Organisation governance - Stakeholders are aware of the Organisational resilience management policy and their role in any plans
4.4.3 Communicatio n and Warning	Communicati on and warning strategies, plans, programs and procedures	- Establishes procedures and makes arrangements for communication both within the Organisation and to/from external sources. - Documents procedures and identifies tools to manage relationships and communications processes with external stakeholders including supply chain business partners, first responders, governmental agencies, vendors, etc. - Develops, coordinates, evaluates and exercises plans to communicate information and warnings	- No formal procedures - Not coordinated internally or externally - Reactive in nature within predefined guidelines - Driven by demands for information	- Communication procedures address project objectives, target and scope - Develops communication procedures for internal and external stakeholders (including authorities and media) consistent with the project scope	- Identifies what will be communicated and to whom - Determines communications and warning needs - Establishes, implements, and maintains procedures for internal and external communications and warnings - Establishes calling trees and contact lists with authorities and roles in which to use them	- Identifies what will be communicated and to whom regarding the resilience policy, risks, objectives, targets and programs - Establishes communications feedback mechanisms - Identifies target audiences for communications and warnings to ensure effective two-way dialogue	- Decides how proactive each type of communication should be with each audience - Develops key messages and set communication targets, objectives and performance indicators - Assigns responsibilities and establish timelines for communications - Establishes, documents and maintains procedures for internal and external	- Identifies external communications and warning needs and capacity of stakeholders supply chain and community - Determines reliability of external communications infrastructure and to augment system internally and externally in the event of a disruption

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
		with internal stakeholders, external stakeholders (including the media) for normal and abnormal conditions. - Develops and maintains reliable communications and a warning capability in the event of a disruption.				- Determines information sharing and security needs - Ensures ongoing communications capacity in the event of a disruptive incident	communications - Communication on resilience issues occurs throughout the Organisation and with appropriate stakeholders - Structures communication with emergency and first responders - Determines needs and establish a communication facility - Sets communications protocols for normal and abnormal conditions - Regularly tests communications system	
4.4.4 Documentation	Organisational resilience documentation	- Establishes processes and procedures for management of documents which are essential to the successful implementation and operation of the resilience management system and programs. - Documents the procedures, processes, work plans and forms to support the management system and its elements, as well as for use before, during and after a disruptive incident.	- Informal if any	- Develops documented procedures to support action plans - Maintains documentation to support project scope - Documentation supports elements addressed in project	- Develops a documents management program - Documentation supports elements address in program action plans	- Establishes resilience management documentation system - Determines security, sensitivity and information integrity needs and take appropriate steps to protect information and documentation	- Develops and organizes documentation system - Prepares a resilience manual outlining the structure of the ORMS - Documentation supports the establishment, definition and implementation of the ORMS	- Evaluates document and information sharing needs with stakeholders, supply chain and community
4.4.5 Control of	Documentation control	- Establishes processes and procedures for control	- No document control system	- Documents control using	- Establishes processes and	- Establishes processes and	- Establishes processes and	- Evaluates stakeholder and

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
Documents		of documents and records (including back-up) to protect the integrity and access to documentation and essential information.	other than that used in general Organisational operations	existing system with some procedures developed to help demonstrate success and business benefit - Rudimentary back-up of critical information	procedures for control of documents and records	procedures for control of documents and records for access, back-up confidentiality, storage, retention, archiving and destruction	procedures for control of documents and records including information security and protection and document integrity	supply chain information needs
4.4.6 Operational Control	Developing and implementing operational and risk control strategies, plans, procedures and programs	- Establishes operational control measures needed to implement the strategic plans and maintain control of activities and functions against defined targets, as well as the unexpected. - Develops procedures for controlling key activities, functions and operations that are associated with the Organisation. - Establishes processes and procedures for operational management and maintenance of infrastructure, plant, facilities, technologies, finance, etc. which have an impact on the Organisation's performance, its supply chain and stakeholders. - Establishes operational control measures needed to implement the strategic programs and maintain control of activities and functions.	- Procedures and processes are undefined - Some individuals may address perceived potential problems on an ad-hoc basis	- Gives proper attention to operational controls and procedures to assure they will be performed properly to achieve objectives and target of issue(s) addressed within the scope	- Plans ways in which operations related to the Organisations critical operations can be controlled based on outcomes of risk analysis or business impact analysis	- Identifies where controls are needed and what they will achieve in terms of risk reduction based on the risk assessment, objectives, targets and programs - Considers ways of minimizing risk in day-to-day operations - Priority is given to proactive approaches - Controls specify how to conduct activities and functions including engineering controls, administrative controls, technical specifications and contractual agreements	- Establishes, implements, and maintains adaptive and proactive procedures for those operations that are associated with the identified significant risks, consistent with its Organisational resilience management policy, risk assessment, supply chain requirements, objectives, and targets, in order to ensure that they are carried out under specified conditions minimizing the risk - Control procedures are written and/or reviewed by persons involved in operations and communicated effectively to others such as contractors and suppliers	- Addresses reliability and resiliency, the safety and health of people, and the protection of property, supply chain and other stakeholder needs, and the environment potentially impacted by a disruptive incident - Ensures demand signals are comprehended in capacity planning - Priority is given to adaptive approaches - Ensures processes are in place to validate supplier responses

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
		- Establishes and implements risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident.						
4.4.7 Incident Prevention, Preparedness, and Response	- Risk avoidance, mitigation, reduction, sharing and treatment procedures - Reactive, proactive, and adaptive incident management	- Establishes and implements risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident. - Establishes, documents and implements procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event using personnel. - Establishes, implements, and maintains procedures to avoid, prevent, protect from and mitigate a disruptive event. - Develops action plans for increased threat levels. - Establishes, implements, and maintains procedures to manage a disruptive event and continue its activities based on recovery objectives. - Establishes and documents procedures for	- Little or no defined procedures - Dependence on the reactive behaviour of individuals in the Organisation (and hope for the best)	- Defines procedures to assure they will be performed properly to achieve objectives and target of issue(s) addressed within the scope - Develops procedures to support action plans (including measures to reduce likelihood and/or consequences - Develops procedures based on identified issue(s) - may be predominately reactive in nature given that no formal risk assessment was conducted	- Identifies what emergency situations may occur and their potential impacts on critical assets, activities, services and functions - Develops procedures that prevent if possible, respond to and recover from potential disruptive events - Implements and tests the procedures - Considers measures that minimize both likelihood and consequences of a disruption but typically emphasis is on addressing consequences	- Based on the risk assessment, objectives, targets and programs, establishes, implements, and maintains procedures to identify potential disruptive incidents that can have impacts on the Organisation, its activities, functions, services, stakeholders, and the environment - Proactively documents with detailed procedures and work plans how the Organisation will prevent, prepare for, and respond to disruptive incidents - Periodically reviews and, where necessary, revises its incident prevention,	- Establishes, implements, and maintains procedures to avoid, prevent, protect from mitigate, respond to and recover from a disruptive event and continue its activities based on resilience objectives developed through the risk assessment process - Prepares for and responds to actual disruptive incidents to prevent the incident, minimize likelihood of its occurrence, or mitigate associated adverse consequences - Ensures that any persons performing incident prevention and management measures on its behalf are competent - Establishes, documents and implements procedures and a management	- Identifies the Organisations potential role in supporting the capacity of stakeholders, the supply chain and the community to avoid, prevent, protect from mitigate, respond to and recover from a disruptive event - Establishes detailed procedures for stakeholders, the supply chain and the community support

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
		how the Organisation will manage a disruptive event; and recover or maintain its activities to a predetermined level.				preparedness, and response procedures	structure to prevent, prepare for, mitigate, and respond to a disruptive event - Establishes detailed procedures for how the Organisation will respond to and manage a disruptive event and how it will recover or maintain its activities to a predetermined level, based on management-approved recovery objectives	
4.5.1 Monitoring and Measurement	Performance evaluation	- Establishes metrics and mechanisms by which the Organisation assesses its ability to achieve its objectives and targets on an ongoing basis. - Monitors, measures, and assesses the Organisation's resilience performance on an ongoing basis.	- No formal monitoring - No formal measurement	- Progress against specific indicators are assess periodically with persons involved in relevant activities - Project indicators and metrics are established and monitored to demonstrate progress and performance improvement relative to identified issue(s)	- Identifies key characteristics that need monitoring and measuring - Plans what will be measured, where and when it will be measured and what methods will be used	- Establishes, implements, and maintains performance metrics and procedures to monitor and measure, on a regular basis, those characteristics of its operations that have material impact on its resilience performance	- Monitors performance, applicable operational controls, and conformity with the Organisation's Organisational resilience management objectives and targets - Evaluates and documents the performance of the systems which protect assets, communications and information systems	- Includes partnership and supply chain relationships
4.5.2.1 Evaluation of Compliance	Compliance evaluation	- Monitors, measures, and assesses the Organisation's legal and regulatory compliance performance on an ongoing basis.	- No formal procedures established beyond those already in place as part of normal business	- Compliance evaluated related to issue(s) identified and the project scope	- Identifies and plans methods used to monitor and measure compliance	- Establishes, implements, and maintains procedure(s) for periodically evaluating compliance with	- Records and reports the results of the evaluation with corrective measures and recommendations for improvement	- Reports to relevant stakeholders as appropriate

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
			operations			applicable legal and other requirements		
4.5.2.2 Exercises and Testing	Testing and system evaluation	- Tests and evaluates appropriateness and efficacy of its ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies.) - Plans, coordinates, and conducts tests and exercises, and evaluates and documents results. - Reviews exercise results with management to ensure lessons learned and appropriate action is taken.	- No exercising and testing	- Develops procedures for exercises and testing related to the identified project issue(s) - Results of exercises and texting are prepared in a report to demonstrate project performance and benefit in terms of enhanced resilience performance and business benefits	- Exercises and tests designed to evaluate the efficacy and implementation of action plans and procedures	- Validates the ORMS using testing and exercises - Tests and evaluates appropriateness and effectiveness of action plans and procedures as well as interrelationship of elements in ORMS - Includes appropriate external parties (e.g. first responders) and stakeholders	- Tests and evaluates the appropriateness and efficacy of ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies) - Produces a formalized post-exercise report that contains outcomes, recommendations, and arrangements to implement improvements in a timely fashion	- Tests and evaluates the appropriateness and efficacy of ORMS with stakeholders, supply chain and community
4.5.3 Nonconformity, Corrective Action, and Preventive Action	- Analyses and handles nonconformities - Improvement	- Determines nonconformities and the manner in which these are dealt with. - Establishes and implements mechanisms for eliminating the causes of detected nonconformities both in the management system and the operational processes. - Establishes and implements mechanisms for instigating action to eliminate potential causes of nonconformities in both the management system and the operational processes.	- Not defined	- Identifies deviations from action plans - Deviations from action plans, programs, objectives and targets are evaluated for opportunities for improvement - Adequate corrective and preventative actions taken if necessary to ensure the project progresses according to plan	- Identifies deviations from action plans - Establishes a corrective action process -Identifies what went wrong and corrects it	- Determines nonconformities in the ORMS, risk assessment, objectives, targets programs, action plans, and their implementation - Analyses why something went wrong - Determines the manner in which they are dealt with to eliminate the causes and prevent their recurrence - Identifies what could go wrong and take actions to	- Establishes, implements, and maintains procedures for dealing with actual and potential nonconformities and for taking corrective action and preventive action - Reviews effectiveness of corrective actions and take preventative actions	

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
						prevent occurrence		
4.5.4 Control of Records	Control of records	- Establishes and maintains records to demonstrate conformity to the requirements of its ORMS and the results achieved.	- Not defined	- Collects and retains evidence addressing project implementation and results	- Collects and retains evidence addressing program implementation and results	- Collects and retains evidence addressing ORMS implementation and results	- Collects and retains evidence addressing ORMS implementation and results	
4.5.5 Internal Audits	System audits	- Conducts internal audits of system and programs. - Reports audits and verification results in management review.	- Not conducted	- Performance of project audited informally - Project Leader oversees development of audit procedures	- Conducts audit of program within defined scope and including all elements of the program	- Determines what needs to be audited - Plans and implements an audit program - Reports audit findings to management and acts upon them	- Responsibility of audit program assigned to an individual that has knowledge and understanding of audit principles - Determines whether the control objectives, risk controls, processes, and procedures of ORMS are conducted properly and achieving the desired results - Identifies opportunities for improvement - Ensures that actions are taken without undue delay to eliminate detected nonconformities and their causes	- Audit includes stakeholder and community interactions, as well the supply chain
4.6 Management Review	Management review	- Management review of the system determines its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary.	- No formal management review outside of existing fiscal reviews	- Project Leader supervisor (and other appropriate members of the management team) formally reports and reviews the performance of project	- Uses review to demonstrate business case for resilience management and provide a basis to seek further efficiencies by linking core	- Identifies inputs to review process - Reviews the suitability, adequacy and effectiveness of the ORMS	- Top management reviews the ORMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness - Assesses opportunities for improvement and the	- Integrates review with overall risk management and business review processes - Review includes evaluation of suitability, adequacy, and effectiveness

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard								
ANSI/ASIS. SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach Phase One**	**Project Approach Phase Two**	**Program Approach Phase Three**	**Systems Approach Phase Four**	**Management System Phase Five**	**Holistic Management Phase Six**
		- Sets priorities, policy, objectives and targets to support continual improvement.			elements in a systems approach - Management reviews the policies, objectives, evaluation of program implementation, audit results and changes resulting from preventive and corrective actions		need for changes to ORMS, including the Organisational resilience management system policy and objectives, target and risk criteria	with regard to stakeholders, community and supply chain
4.6.4 Maintenance	System maintenance	- Makes provisions for improvement of programs, systems, and/or operational processes.	- Not defined	- Project outcomes that improve resilience performance become standard operating procedures	- Program and action plans outcomes that improve resilience performance become standard operating procedures	- Ensures that any internal or external changes that impact the Organisation are reviewed in relation to the ORMS	- Identifies any new critical activities that need to be included in the ORMS program	- Ensures that any internal or external changes that impact the Organisation, the overall enterprise, stakeholders and the supply chain are reviewed in relation to the ORMS
4.6.5 Continual Improvement	Continual improvement	- Provisions made for continual improvement of the management system and resilience performance.	- Not defined	- Evaluation of project(s) - Evaluation of extension of scope to identify additional issues and expand project to management system	- Evaluation of program - Evaluation of extension of scope to identify additional issues and expand program to management system	- Continually improves the effectiveness of ORMS through the use of the Organisational resilience management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review	- Continually improves the effectiveness of ORMS through the use of the Organisational resilience management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review	- Continually improves the effectiveness of ORMS through the use of the Organisational resilience management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review

ANNEXURE J: MATURITY MODEL FOR THE PHASED IMPLEMENTATION OF THE *ANSI/ASIS SPC.1-2009 ORGANIZATIONAL RESILIENCE: SECURITY, PREPAREDNESS AND CONTINUITY MANAGEMENT SYSTEMS - REQUIREMENTS WITH GUIDANCE FOR USE*

TABLE 1: PHASE 1 Ad Hoc Approach: BASE LEVEL 1 (Copper)

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard						
PHASE 1 Ad Hoc Approach: BASE LEVEL 1 (Copper)						
ANSI/ASIS SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Ad Hoc Approach**	**Documentary or Other Proof Requirements**	**Score**	
Generic Concepts	Key elemental theme	Description of element	- No formal incident or resilience management - Actions reactionary in nature - Not yet recognizing importance of elements			
4.1.1 Scope of OR Management System	- Understanding the Organisation and its context - Scope of ORMS	- Establish the internal, external and risk management context of the Organisation - Define scope and boundaries for development and implementation of ORMS.	- No formal process - No definition of scope or internal or external context - No clear concept of business context or benefits			
4.2.1 Policy Statement	- Setting a policy framework	- Establish a policy to provide a framework for setting objectives and provide the direction and principles for action. - Demonstrates management commitment	- No defined policy - Lack of executive level governance			

4.2.2 Management Commitment	- Management mandate and commitment	- Demonstrate executive management and the Organisation's commitment to meeting the requirements of resilience management. - Establish the project to address resilience management including provision of appropriate resources and authorization to conduct project.	- Management ambivalent to unreceptive - Concern that acknowledging risk and uncertainty may be seen of admission of problems or weakness - No guidance from the executive or Organisation - Ad hoc leadership - Ostrich effect			
4.3.1 Risk Assessment and Impact Analysis	- Asset, activities, functions and services identification and valuation - Risk identification - Risk Analysis - Risk Evaluation	- Establish a process for risk identification, analysis and evaluation. - Identify assets, activities, needs, requirements and analysis of critical issues related to business disruption risks that are relevant to the Organisation and stakeholders. - Identify of hazards threats, vulnerabilities and consequences. - Evaluate of the effect of uncertainty on the Organisation's objectives. - Evaluate of the likelihood of a disruptive event and its consequences on assets (human, physical, cyber, environmental, information, and intangibles). - Evaluate dependencies and interdependencies with other assets and sectors, and consequences a disruptive event. - Evaluate and establish timeframes for response and recovery.	- No formal process - Indications of problems, near misses and warning signs identified in an ad hoc manner as they materialize - Risk identified after they materialize			

4.3.2 Legal and Other Requirements	- Identify legal, regulatory, and other requirements to which the Organisation subscribes - Determine how these requirements apply to the Organisation, its risks and their potential impact.	- Identify legal and other requirements which govern the Organisation's activity. - Establish a procedure or process for identifying, registering and evaluating internal and external requirements pertinent to the Organisation's functions, activities and operations. - Understand and communicate potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to location and industry.	- No understanding of legal and other requirements			

4.3.3 Objectives, Targets, and Program(s)	- Setting objectives and developing risk and incident prevention, protection, preparedness, mitigation, response, continuity and recovery management strategies - Risk prioritization and treatment	- Prioritize the issues identified as a result of the risk assessment and impact analysis. - Set objectives and targets (including time frames) based on the prioritization of issues within the context of an Organisation's policy and mission. - Develop strategic plans for incident prevention, protection, preparedness, mitigation, response, continuity and recovery. - Identify resources needed and the availability of adequate human, infrastructure, processing and financial resources. - Identify roles, responsibilities, authorities and their interrelationships within the Organisation as far as needed to ensure effective and efficient operations. - Plan the operational processes for actions effecting how the objectives and targets are achieved. - Make internal and external arrangements, agreements, and contingency plans that need to be in place to manage foreseeable emergencies.	- Objectives and targets not defined - No risk prioritization			

4.4.1 Resources, Roles, Responsibility, and Authority	- Ensure the availability of resources essential for the implementation and control of the ORMS. - Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective OR management.	- Establish procedures, roles and responsibilities to cover all normal and abnormal operating conditions, including disruptions and emergencies. - Establish management processes and procedures for human resources including employees, contractors, temporary staff, etc. - Identify and assure availability of human, infrastructure and financial resources in the event of a disruption. - Establish and document provisions for adequate finance and administrative resources and procedures to support the management program or system normal and abnormal conditions. - Make arrangements for supply chain obligations, mutual aid and community assistance. - Determine the local, regional and public authorities' roles, relationships and interactions with the Organisation's management system implementation plans.	- Not defined - No dedicated personnel for resilience management - Needed resources not identified - Lack of time, energy and resources to adequately prepare for and respond to disruptions.			

4.4.2 Competence, Training, and Awareness	Awareness, competence and training strategies, plans, programs and procedures	- Identify and establish skills, competency requirements, and qualifications needed by the Organisation to maintain operations. - Assess, develop and implement training/ and education program for the Organisation's personnel, contractors, and other relevant stakeholders. - Develop Organisational awareness and establish a culture to support resilience management. - Determine Organisational interface protocol, identification and training requirements and assign appropriate internal staff or support representatives. - Develop tools to enhance situational awareness.	- Lack of cultural awareness - Competencies and skills not identified - No formal training program - Little or no in-house expertise or experience - General workforce unaware of risk management needs and lack training to adequately take ownership and control risks			

4.4.3 Communication and Warning	Communication and warning strategies, plans, programs and procedures	- Establish procedures and make arrangements for communications both within the Organisation and to/from external sources. - Document procedures and identify tools to manage relationships and communications processes with external stakeholders including supply chain business partners, first responders, governmental agencies, vendors, etc. - Develop, coordinate, evaluate and exercise plans to communicate information and warnings with internal stakeholders, external stakeholders (including the media) for normal and abnormal conditions. - Develop and maintain reliable communications and warning capability in the event of a disruption.	- No formal procedures - Not coordinated internally or externally - Reactive in nature within predefined guidelines - Driven by demands for information			
4.4.4 Documentation	Organisational resilience documentation	- Establish processes and procedures for management of documents which are essential to the successful implementation and operation of the resilience management system and programs. - Document the procedures, processes, work plans and forms to support the management system and its elements, as well as for use before, during and after a disruptive incident.	- Informal if any			

4.4.5 Control of Documents	Documentation control	- Establish processes and procedures for control of documents and records (including back-up) to protect the integrity and access to documentation and essential information.	- No document control system other than that used in general Organisational operations			

4.6 Operational Control	Developing and implementing operational and risk control strategies, plans, procedures and programs	- Establish operational control measures needed to implement the strategic plans and maintain control of activities and functions against defined targets, as well as the unexpected. - Develop procedures for controlling key activities, functions and operations that are associated with the Organisation. - Establish processes and procedures for operational management and maintenance of infrastructure, plant, facilities, technologies, finance, etc. which have an impact on the Organisation's performance, its supply chain and stakeholders. - Establish operational control measures needed to implement the strategic programs and maintain control of activities and functions. - Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident.	- Procedures and processed undefined - Some individuals may address perceived potential problems on an ad-hoc basis			

4.4.7 Incident Prevention, Preparedness, and Response	- Risk avoidance, mitigation, reduction, sharing and treatment procedures - Reactive, proactive, and adaptive incident management	- Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident. - Establish, document and implement procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event using personnel. - Establish, implement, and maintain procedures to avoid, prevent, protect from and mitigate a disruptive event. - Develop action plans for increased threat levels. - Establish, implement, and maintain procedures to manage a disruptive event and continue its activities based on recovery objectives. - Establish, documented procedures for how the Organisation will manage a disruptive event; and recover or maintain its activities to a predetermined level.	- Little or no defined procedures - Dependence on the reactive behaviour of individuals in the Organisation (and hope for the best)			

4.5.1 Monitoring and Measurement	Performance evaluation	- Establish metrics and mechanisms by which the Organisation assesses its ability to achieve its objectives and targets on an ongoing basis. - Monitor, measure, and assess the Organisation's resilience performance on an ongoing basis.	- No formal monitoring - No formal measurement			
4.5.2.1 Evaluation of Compliance	Compliance evaluation	- Monitor, measure, and assess the Organisation's legal and regulatory compliance performance on an ongoing basis.	- No formal procedures established beyond those already in place as part of normal business operations			
4.5.2.2 Exercises and Testing	Testing and system evaluation	- Test and evaluate appropriateness and efficacy of its ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies) - Plan, coordinate, and conduct tests and exercises, and evaluate and document results. - Review exercise results with management to ensure lessons learned and appropriate action is taken.	- No exercising and testing			

4.5.3 Non-conformity, Corrective Action, and Preventive Action	- Analysing and handling non-conformities - Improvement	- Determine nonconformities and the manner in which these are dealt with. - Establish and implement mechanism for eliminating the causes of detected nonconformities both in the management system and the operational processes. - Establish and implement mechanism for instigating action to eliminate potential causes of non-conformities in both the management system and the operational processes.	- Not defined			
4.5.4 Control of Records	Control of records	- Establish and maintain records to demonstrate conformity to the requirements of its ORMS and the results achieved.	- Not defined			
4.5.5 Internal Audits	System audits	- Conduct internal audits of system and programs. - Report audits and verification results in management review.	- Not conducted			

4.6 Management Review	Management review	- Management review of the system to determine its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary. - Set priorities, policy, objectives and targets to support continual improvement.	- No formal management review outside of existing fiscal reviews			
4.6.4 Maintenance	System maintenance	- Make provisions for improvement of programs, systems, and/or operational processes.	- Not defined			
4.6.5 Continual Improvement	Continual improvement	- Provisions made for continual improvement of the management system and resilience performance.	- Not defined			
				TOTAL POSSIBLE SCORE		
				ACTUAL SCORE		
				PERCENTAGE ACHIEVED		

TABLE 2: PHASE 2: Project Approach: BASE LEVEL 2 (Bronze)

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard						
PHASE 2: Project Approach: BASE LEVEL 2 (Bronze)						
ANSI/ASIS SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Project Approach**	**Documentary or Other Proof Requirements**	**Score**	
Generic Concepts	Key elemental theme	Description of element	- Initiating a project to address a specific issue(s) by partially implementing core elements - Actions generally reactionary in nature focusing on pre-identified issue(s) - Recognizing importance of elements and the need for some pre-planning - May be in reaction to an incident or near miss or driven by external concerns			
4.1.1 Scope of OR Management System	- Understanding the Organisation and its context - Scope of ORMS	- Establish the internal, external and risk management context of the Organisation - Define scope and boundaries for development and implementation of ORMS.	- Project of limited scope focusing on one or a limited number of issues identified as of particular or immediate interest - Internal and external context and interactions considered within project scope definition			

4.2.1 Policy Statement	- Setting a policy framework	- Establish a policy to provide a framework for setting objectives and provide the direction and principles for action. - Demonstrates management commitment	- Policy limited to addressing identified issue(s) - Driven by "Project Leader", may or may not have top management involvement beyond approval of project			
4.2.2 Management Commitment	- Management mandate and commitment	- Demonstrate executive management and the Organisation's commitment to meeting the requirements of resilience management. - Establish the project to address resilience management including provision of appropriate resources and authorization to conduct project.	- Management authorization and resources provided to "Project Leader" to conduct project including in-house training and/or external expertise - Resources restricted to address limited scope - Resource allocation liked to perceived return on investment - Project aims to encourage more management support and buy-in			

4.3.1 Risk Assessment and Impact Analysis	- Asset, activities, functions and services identification and valuation - Risk identification - Risk Analysis - Risk Evaluation	- Establish a process for risk identification, analysis and evaluation. - Identify assets, activities, needs, requirements and analysis of critical issues related to business disruption risks that are relevant to the Organisation and stakeholders. - Identify of hazards threats, vulnerabilities and consequences. - Evaluate of the effect of uncertainty on the Organisation's objectives. - Evaluate of the likelihood of a disruptive event and its consequences on assets (human, physical, cyber, environmental, information, and intangibles). - Evaluate dependencies and interdependencies with other assets and sectors, and consequences a disruptive event. - Evaluate and establish timeframes for response and recovery.	- No formal process - Reactive in nature with issue(s) addressed having been identified due to Indications of problems, near misses, warning signs, an event, and/or external concerns - The analysis is more of a gap analysis than a risk assessment examining what is need to address project issues			

4.3.2 Legal and Other Requirements	- Identify legal, regulatory, and other requirements to which the Organisation subscribes - Determine how these requirements apply to the Organisation, its risks and their potential impact.	- Identify legal and other requirements which govern the Organisation's activity. - Establish a procedure or process for identifying, registering and evaluating internal and external requirements pertinent to the Organisation's functions, activities and operations. - Understand and communicate potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to location and industry.	- Informal process initiated to identify legal and other requirements related to identified issue being addressed - The main legal requirements applicable to the activities, functions and services in the scope of the project are identified			

4.3.3 Objectives, Targets, and Program(s)	- Setting objectives and developing risk and incident prevention, protection, preparedness, mitigation, response, continuity and recovery management strategies - Risk prioritization and treatment	- Prioritize the issues identified as a result of the risk assessment and impact analysis. - Set objectives and targets (including time frames) based on the prioritization of issues within the context of an Organisation's policy and mission. - Develop strategic plans for incident prevention, protection, preparedness, mitigation, response, continuity and recovery. - Identify resources needed and the availability of adequate human, infrastructure, processing and financial resources. - Identify roles, responsibilities, authorities and their interrelationships within the Organisation as far as needed to ensure effective and efficient operations. - Plan the operational processes for actions effecting how the objectives and targets are achieved. - Make internal and external arrangements, agreements, and contingency plans that need to be in place to manage foreseeable emergencies.	- Targets and objectives defined based on supporting demonstration of perceived factors for project success in dealing with identified issue(s) - Targets, objectives and programs developed to achieve immediate resilience performance improvement related to identified issue(s) and to demonstrate business benefit - Issue(s) addressed using rudimentary PDCA model approach focusing on limited scope - Action plans include actions necessary, required human and financial resources, responsibilities and timescales			

4.4.1 Resources, Roles, Responsibility, and Authority	- Ensure the availability of resources essential for the implementation and control of the ORMS. - Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective OR management.	- Establish procedures, roles and responsibilities to cover all normal and abnormal operating conditions, including disruptions and emergencies. - Establish management processes and procedures for human resources including employees, contractors, temporary staff, etc. - Identify and assure availability of human, infrastructure and financial resources in the event of a disruption. - Establish and document provisions for adequate finance and administrative resources and procedures to support the management program or system normal and abnormal conditions. - Make arrangements for supply chain obligations, mutual aid and community assistance. - Determine the local, regional and public authorities' roles, relationships and interactions with the Organisation's management system implementation plans.	- Roles and responsibilities assigned to specific persons to address issue(s) in the limited scope - Adequate resources allocated in accordance with action plan - A "Project Leader" is designated to oversee the conduct of the project - Participation based on project scope (only divisions and individuals within the scope actively engaged			

4.4.2 Competence, Training, and Awareness	Awareness, competence and training strategies, plans, programs and procedures	- Identify and establish skills, competency requirements, and qualifications needed by the Organisation to maintain operations. - Assess, develop and implement training/ and education program for the Organisation's personnel, contractors, and other relevant stakeholders. - Develop Organisational awareness and establish a culture to support resilience management. - Determine Organisational interface protocol, identification and training requirements and assign appropriate internal staff or support representatives. - Develop tools to enhance situational awareness.	- Competence, skills and training needs identified to achieve objectives and targets - Training conducted with some measure of competence to achieve objectives and targets - Focus is on addressing the identified issue(s) in the scope - Awareness emphasized within the scope of the project			

4.4.3 Communication and Warning	Communication and warning strategies, plans, programs and procedures	- Establish procedures and make arrangements for communications both within the Organisation and to/from external sources. - Document procedures and identify tools to manage relationships and communications processes with external stakeholders including supply chain business partners, first responders, governmental agencies, vendors, etc. - Develop, coordinate, evaluate and exercise plans to communicate information and warnings with internal stakeholders, external stakeholders (including the media) for normal and abnormal conditions. - Develop and maintain reliable communications and warning capability in the event of a disruption.	- Communication procedures address project objectives, target and scope - Communication procedures developed for internal and external stakeholders (including authorities and media) consistent with the project scope			

4.4.4 Documentation	Organisational resilience documentation	- Establish processes and procedures for management of documents which are essential to the successful implementation and operation of the resilience management system and programs. - Document the procedures, processes, work plans and forms to support the management system and its elements, as well as for use before, during and after a disruptive incident.	- Documented procedures developed to support action plans - Documentation maintained to support project scope - Documentation supports elements address in project			
4.4.5 Control of Documents	Documentation control	- Establish processes and procedures for control of documents and records (including back-up) to protect the integrity and access to documentation and essential information.	- Document control using existing system with some procedures developed to help demonstrate success and business benefit - Rudimentary back-up of critical information			

4.4.6 Operational Control	Developing and implementing operational and risk control strategies, plans, procedures and programs	- Establish operational control measures needed to implement the strategic plans and maintain control of activities and functions against defined targets, as well as the unexpected. - Develop procedures for controlling key activities, functions and operations that are associated with the Organisation. - Establish processes and procedures for operational management and maintenance of infrastructure, plant, facilities, technologies, finance, etc. which have an impact on the Organisation's performance, its supply chain and stakeholders. - Establish operational control measures needed to implement the strategic programs and maintain control of activities and functions. - Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident.	- Proper attention given to operational controls and procedures to assure they will be performed properly to achieve objectives and target of issue(s) addressed within the scope			

4.4.7 Incident Prevention, Preparedness, and Response	- Risk avoidance, mitigation, reduction, sharing and treatment procedures - Reactive, proactive, and adaptive incident management	- Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident. - Establish, document and implement procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event using personnel. - Establish, implement, and maintain procedures to avoid, prevent, protect from and mitigate a disruptive event. - Develop action plans for increased threat levels. - Establish, implement, and maintain procedures to manage a disruptive event and continue its activities based on recovery objectives. - Establish, documented procedures for how the Organisation will manage a disruptive event; and recover or maintain its activities to a predetermined level.	- Procedures defined to assure they will be performed properly to achieve objectives and target of issue(s) addressed within the scope - Procedures developed to support action plans (including measures to reduce likelihood and/or consequences - Procedures developed based on identified issue(s) – May be predominately reactive in nature given that no formal risk conducted assessment was			

4.5.1 Monitoring and Measurement	Performance evaluation	- Establish metrics and mechanisms by which the Organisation assesses its ability to achieve its objectives and targets on an ongoing basis. - Monitor, measure, and assess the Organisation's resilience performance on an ongoing basis.	- Progress against specific indicators are assess periodically with persons involved in relevant activities - Project indicators and metrics established and monitored to demonstrate progress and performance improvement relative to identified issue(s)			
4.5.2.1 Evaluation of Compliance	Compliance evaluation	- Monitor, measure, and assess the Organisation's legal and regulatory compliance performance on an ongoing basis.	- Compliance evaluated related to issue(s) identified and the project scope			
4.5.2.2 Exercises and Testing	Testing and system evaluation	- Test and evaluate appropriateness and efficacy of its ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies) - Plan, coordinate, and conduct tests and exercises, and evaluate and document results. - Review exercise results with management to ensure lessons learned and appropriate action is taken.	- Procedures developed for exercises and testing related to the identified project issue(s) - Results of exercises and texting are prepared in a report to demonstrate project performance and benefit in terms of enhanced resilience performance and business benefit			

4.5.3 Non-conformity, Corrective Action, and Preventive Action	- Analysing and handling non-conformities - Improvement	- Determine nonconformities and the manner in which these are dealt with. - Establish and implement mechanism for eliminating the causes of detected nonconformities both in the management system and the operational processes. - Establish and implement mechanism for instigating action to eliminate potential causes of non-conformities in both the management system and the operational	- Deviations from action plans identified - Deviations from action plans, programs, objectives and targets evaluated for opportunities for improvement - Adequate corrective and preventative actions taken if necessary to ensure the project progresses according to plan			
4.5.4 Control of Records	Control of records	- Establish and maintain records to demonstrate conformity to the requirements of its ORMS and the results achieved.	- Evidence addressing project implementation and results are collected and retained			
4.5.5 Internal Audits	System audits	- Conduct internal audits of system and programs. - Report audits and verification results in management review.	- Performance of project audited informally - Project Leader oversees development of audit procedures			

4.6 Management Review	Management review	- Management review of the system to determine its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary. - Set priorities, policy, objectives and targets to support continual improvement.	- Performance of project formally reported and reviewed by Project Leader supervisor (and other appropriate members of the management team)			
4.6.4 Maintenance	System maintenance	- Make provisions for improvement of programs, systems, and/or operational processes.	- Project outcomes that improve resilience performance become standard operating procedures			
4.6.5 Continual Improvement	Continual improvement	- Provisions made for continual improvement of the management system and resilience performance.	- Evaluation of project - Evaluation of extension of scope to identify additional issues and expand project to management system			
				TOTAL POSSIBLE SCORE		
				ACTUAL SCORE		
				PERCENTAGE ACHIEVED		

TABLE 3: PHASE 3: Program Approach: BASE LEVEL 3 (Silver)

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard				
PHASE 3: Program Approach: BASE LEVEL 3 (Silver)				
ANSI/ASIS SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Program Approach**	**Documentary or Other Proof Requirements**
Generic Concepts	Key elemental theme	Description of element	- Establishing a division or Organisation wide program to address resilience issues by partially implementing core elements - Recognizing importance of elements and the need for pre-planning, however focus is on individual elements and not their interrelationship and integration - May be in reaction to an incident or near miss or driven by external concerns - Risk management applications selected for chances of demonstrating success - Program driven by "Program Manager" applying a program management approach	

4.1.1 Scope of OR Management System	- Understanding the Organisation and its context - Scope of ORMS	- Establish the internal, external and risk management context of the Organisation - Define scope and boundaries for development and implementation of ORMS.	- Programs are established to address core elements based on evaluation of the internal, external and resilience management context of all or part of the Organisation - Scope defined based on protecting and preserving critical activities, functions and services			
4.2.1 Policy Statement	- Setting a policy framework	- Establish a policy to provide a framework for setting objectives and provide the direction and principles for action. - Demonstrates management commitment	- Drafted by "Program Manager" and signed by executive management - Policy addresses resilience management in divisions defined in scope - Communicated to relevant divisions			
4.2.2 Management Commitment	- Management mandate and commitment	- Demonstrate executive management and the Organisation's commitment to meeting the requirements of resilience management. - Establish the project to address resilience management including provision of appropriate resources and authorization to conduct project.	- Executive management sponsorship - Endorsement of establishing programs for resilience Management - One or more individuals appointed as Project Manager - Set asset prioritization and timeframes for recovery in event of disruption - Resources allocated to support program			

4.3.1 Risk Assessment and Impact Analysis	- Asset, activities, functions and services identification and valuation - Risk identification - Risk Analysis - Risk Evaluation	- Establish a process for risk identification, analysis and evaluation. - Identify assets, activities, needs, requirements and analysis of critical issues related to business disruption risks that are relevant to the Organisation and stakeholders. - Identify of hazards threats, vulnerabilities and consequences. - Evaluate of the effect of uncertainty on the Organisation's objectives. - Evaluate of the likelihood of a disruptive event and its consequences on assets (human, physical, cyber, environmental, information, and intangibles). - Evaluate dependencies and interdependencies with other assets and sectors, and consequences a disruptive event. - Evaluate and establish timeframes for response and recovery.	- Develop and implement a procedure to identify, analyze and evaluate critical assets, risks, and impacts - Priorities based on outcomes of risk analysis or business impact analysis			

4.3.2 Legal and Other Requirements	- Identify legal, regulatory, and other requirements to which the Organisation subscribes - Determine how these requirements apply to the Organisation, its risks and their potential impact.	- Identify legal and other requirements which govern the Organisation's activity. - Establish a procedure or process for identifying, registering and evaluating internal and external requirements pertinent to the Organisation's functions, activities and operations. - Understand and communicate potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to location and industry.	- Identify legal and other requirements			

4.3.3 Objectives, Targets, and Program(s)	- Setting objectives and developing risk and incident prevention, protection, preparedness, mitigation, response, continuity and recovery management strategies - Risk prioritization and treatment	- Prioritize the issues identified as a result of the risk assessment and impact analysis. - Set objectives and targets (including time frames) based on the prioritization of issues within the context of an Organisation's policy and mission. - Develop strategic plans for incident prevention, protection, preparedness, mitigation, response, continuity and recovery. - Identify resources needed and the availability of adequate human, infrastructure, processing and financial resources. - Identify roles, responsibilities, authorities and their interrelationships within the Organisation as far as needed to ensure effective and efficient operations. - Plan the operational processes for actions effecting how the objectives and targets are achieved. - Make internal and external arrangements, agreements, and contingency plans that need to be in place to manage foreseeable emergencies.	- Resilience performance objectives for program management are set based on the risk assessment and impact analysis - Strategic action plans designate actions, responsibilities, accountability, resources and timeframes for achieving objectives and targets			

4.4.1 Resources, Roles, Responsibility, and Authority	- Ensure the availability of resources essential for the implementation and control of the ORMS. - Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective OR management.	- Establish procedures, roles and responsibilities to cover all normal and abnormal operating conditions, including disruptions and emergencies. - Establish management processes and procedures for human resources including employees, contractors, temporary staff, etc. - Identify and assure availability of human, infrastructure and financial resources in the event of a disruption. - Establish and document provisions for adequate finance and administrative resources and procedures to support the management program or system normal and abnormal conditions. - Make arrangements for supply chain obligations, mutual aid and community assistance. - Determine the local, regional and public authorities' roles, relationships and interactions with the Organisation's management system implementation plans.	- Identify and define authorities, roles, responsibilities and appropriate resources within the Organisation - Identify internal and external departments, division, business units and partners that will pay a role in addressing a disruptive incident - Identify and incident management team and team leader - Adequate resources allocated in accordance with action plan			

4.4.2 Competence, Training, and Awareness	Awareness, competence and training strategies, plans, programs and procedures	- Identify and establish skills, competency requirements, and qualifications needed by the Organisation to maintain operations. - Assess, develop and implement training/ and education program for the Organisation's personnel, contractors, and other relevant stakeholders. - Develop Organisational awareness and establish a culture to support resilience management. - Determine Organisational interface protocol, identification and training requirements and assign appropriate internal staff or support representatives. - Develop tools to enhance situational awareness.	- Determine competence requirements that are necessary for activities defined in programs - Develop and implement an awareness program			

4.4.3 Communication and Warning	Communication and warning strategies, plans, programs and procedures	- Establish procedures and make arrangements for communications both within the Organisation and to/from external sources. - Document procedures and identify tools to manage relationships and communications processes with external stakeholders including supply chain business partners, first responders, governmental agencies, vendors, etc. - Develop, coordinate, evaluate and exercise plans to communicate information and warnings with internal stakeholders, external stakeholders (including the media) for normal and abnormal conditions. - Develop and maintain reliable communications and warning capability in the event of a disruption.	- Identify what will be communicated and to whom - Determine communications and warning needs - Establish, implement, and maintain procedures for internal and external communications and warnings - Establish calling trees and contact lists with authorities and roles to use them			
4.4.4 Documentation	Organisational resilience documentation	- Establish processes and procedures for management of documents which are essential to the successful implementation and operation of the resilience management system and programs. - Document the procedures, processes, work plans and forms to support the management system and its elements, as well as for use before, during and after a disruptive incident.	- Develop a documents management Program Documentation supports elements address in program action plans			

4.4.5 Control of Documents	Documentation control	- Establish processes and procedures for control of documents and records (including back-up) to protect the integrity and access to documentation and essential information.	- Establish processes and procedures for control of documents and records			

4.4.6 Operational Control	Developing and implementing operational and risk control strategies, plans, procedures and programs	- Establish operational control measures needed to implement the strategic plans and maintain control of activities and functions against defined targets, as well as the unexpected. - Develop procedures for controlling key activities, functions and operations that are associated with the Organisation. - Establish processes and procedures for operational management and maintenance of infrastructure, plant, facilities, technologies, finance, etc. which have an impact on the Organisation's performance, its supply chain and stakeholders. - Establish operational control measures needed to implement the strategic programs and maintain control of activities and functions. - Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident.	- Plan ways in which operations related to the Organisations critical operations can be controlled based on outcomes of risk analysis or business impact analysis			

4.4.7 Incident Prevention, Preparedness, and Response	- Risk avoidance, mitigation, reduction, sharing and treatment procedures - Reactive, proactive, and adaptive incident management	- Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident. - Establish, document and implement procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event using personnel. - Establish, implement, and maintain procedures to avoid, prevent, protect from and mitigate a disruptive event. - Develop action plans for increased threat levels. - Establish, implement, and maintain procedures to manage a disruptive event and continue its activities based on recovery objectives. - Establish, documented procedures for how the Organisation will manage a disruptive event; and recover or maintain its activities to a predetermined level.	- Identify what emergency situations may occur and their potential impacts on critical assets, activities, services and functions - Develop procedures that prevent if possible, respond to and recover from potential disruptive events - Implement and test the procedures - Consider measures that minimize both likelihood and consequences of a disruption but typically emphasis is on addressing consequences			

4.5.1 Monitoring and Measurement	Performance evaluation	- Establish metrics and mechanisms by which the Organisation assesses its ability to achieve its objectives and targets on an ongoing basis. - Monitor, measure, and assess the Organisation's resilience performance on an ongoing basis.	- Identify key characteristics that need monitoring and measuring - Plan what will be measured, where and when it will be measured and what methods will be used			
4.5.2.1 Evaluation of Compliance	Compliance evaluation	- Monitor, measure, and assess the Organisation's legal and regulatory compliance performance on an ongoing basis.	- Identify and plan methods used to monitor and measure compliance			
4.5.2.2 Exercises and Testing	Testing and system evaluation	- Test and evaluate appropriateness and efficacy of its ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies) - Plan, coordinate, and conduct tests and exercises, and evaluate and document results. - Review exercise results with management to ensure lessons learned and appropriate action is taken.	- Exercising and testing designed to evaluate the efficacy and implementation of action plans and procedures			

4.5.3 Non-conformity, Corrective Action, and Preventive Action	- Analysing and handling non-conformities - Improvement	- Determine nonconformities and the manner in which these are dealt with. - Establish and implement mechanism for eliminating the causes of detected nonconformities both in the management system and the operational processes. - Establish and implement mechanism for instigating action to eliminate potential causes of non-conformities in both the management system and the operational processes	- Identify deviations from action plans - Establish a corrective action process - Identify what went wrong and correct it			
4.5.4 Control of Records	Control of records	- Establish and maintain records to demonstrate conformity to the requirements of its ORMS and the results achieved.	- Evidence addressing program implementation and results are collected and retained			
4.5.5 Internal Audits	System audits	- Conduct internal audits of system and programs. - Report audits and verification results in management review.	- Audit conducted of program within defined scope and including all elements of the program			

4.6 Management Review	Management review	- Management review of the system to determine its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary. - Set priorities, policy, objectives and targets to support continual improvement.	- Review used to demonstrate business case for resilience management and provide a basis to seek further efficiencies by linking core elements in a systems approach - Management review of the policies, objectives, evaluation of program implementation, audit results and changes resulting from preventive and corrective actions			
4.6.4 Maintenance	System maintenance	- Make provisions for improvement of programs, systems, and/or operational processes.	- Program and action plans outcomes that improve resilience performance become standard operating procedures			
4.6.5 Continual Improvement	Continual improvement	- Provisions made for continual improvement of the management system and resilience performance.	- Evaluation of program - Evaluation of extension of scope to identify additional issues and expand program to management system			
				TOTAL POSSIBLE SCORE		
				ACTUAL SCORE		
				PERCENTAGE ACHIEVED		

TABLE 4: PHASE 4: Systems Approach - BASE LEVEL 4 (Gold)

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard						
PHASE 4: Systems Approach - BASE LEVEL 4 (Gold)						
ANSI/ASIS SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Systems Approach**	**Documentary or Other Proof Requirements**	**Score**	
Generic Concepts	Key elemental theme	Description of element	- Resilience management viewed as a matter of strategic value to the Organisation - Focus on integration and interrelationships between core Elements - Focus on proactive management of risks to minimize both likelihood and consequences of a disruptive incident - Resilience management viewed as part of a continual improvement process using PDCA model - Managing risk seen as important at all levels and roles in Organisation - Integration and feedback loops of systems approach ensures effective learning from experiences - Resilience management culture is developing and part of decision making			

4.1.1 Scope of OR Management System	- Understanding the Organisation and its context - Scope of ORMS	- Establish the internal, external and risk management context of the Organisation - Define scope and boundaries for development and implementation of ORMS.	- Organisation defines and documents the internal, external and resilience management context - Critical operational objectives, assets, activities, functions, services, and products defined - Boundaries of scope defined and documented based on protecting and preserving critical activities, functions and services, as well as relations with stakeholders - Weighting of risk management strategies defined			
4.2.1 Policy Statement	- Setting a policy framework	- Establish a policy to provide a framework for setting objectives and provide the direction and principles for action. - Demonstrates management commitment	- Policy establishes framework for resilience management by setting objectives and providing direction - Endorsed by executive management - Communicated throughout Organisation			
4.2.2 Management Commitment	- Management mandate and commitment	- Demonstrate executive management and the Organisation's commitment to meeting the requirements of resilience management. - Establish the project to address resilience management including provision of appropriate resources and authorization to conduct project.	- Executive management participation Visible endorsement of executive management - Establishing an ORMS policy - One or more individuals appointed to be responsible for ORMS - Deciding criteria for accepting risk, acceptable levels of risk - Set asset prioritization and timeframes for recovery in event of disruption - Resources allocated to support system			

4.3.1 Risk Assessment and Impact Analysis	- Asset, activities, functions and services identification and valuation - Risk identification - Risk Analysis - Risk Evaluation	- Establish a process for risk identification, analysis and evaluation. - Identify assets, activities, needs, requirements and analysis of critical issues related to business disruption risks that are relevant to the Organisation and stakeholders. - Identify of hazards threats, vulnerabilities and consequences. - Evaluate of the effect of uncertainty on the Organisation's objectives. - Evaluate of the likelihood of a disruptive event and its consequences on assets (human, physical, cyber, environmental, information, and intangibles). - Evaluate dependencies and interdependencies with other assets and sectors, and consequences a disruptive event. - Evaluate and establish timeframes for response and recovery.	- Establish, implement, and maintain an ongoing formal and documented risk assessment process - Prioritize risks and impacts are taken into account in establishing, implementing, and operating the ORMS - Risk assessment and impact analysis recognized as provided the foundation for elements of the ORMS and for Organisational decision-making			

4.3.2 Legal and Other Requirements	- Identify legal, regulatory, and other requirements to which the Organisation subscribes - Determine how these requirements apply to the Organisation, its risks and their potential impact.	- Identify legal and other requirements which govern the Organisation's activity. - Establish a procedure or process for identifying, registering and evaluating internal and external requirements pertinent to the Organisation's functions, activities and operations. - Understand and communicate potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to location and industry.	- Establish and maintain procedures to identify legal and other requirements - Determine how the legal and other requirements apply to the Organisation - Communicate requirements to appropriate parties			

4.3.3 Objectives, Targets, and Program(s)	- Setting objectives and developing risk and incident prevention, protection, preparedness, mitigation, response, continuity and recovery management strategies - Risk prioritization and treatment	- Prioritize the issues identified as a result of the risk assessment and impact analysis. - Set objectives and targets (including time frames) based on the prioritization of issues within the context of an Organisation's policy and mission. - Develop strategic plans for incident prevention, protection, preparedness, mitigation, response, continuity and recovery. - Identify resources needed and the availability of adequate human, infrastructure, processing and financial resources. - Identify roles, responsibilities, authorities and their interrelationships within the Organisation as far as needed to ensure effective and efficient operations. - Plan the operational processes for actions effecting how the objectives and targets are achieved. - Make internal and external arrangements, agreements, and contingency plans that need to be in place to manage foreseeable emergencies.	- Objectives shall be derived from and consistent with the OR management policy and risk assessment - Documented objectives and targets to manage risks in order to avoid, prevent, protect, deter, mitigate, respond to, and recover from disruptive incidents are established - Targets are measurable and derived from the objectives - Establish and maintain one or more strategic programs (action plans) for prevention, protection, deterrence, mitigation, response, continuity and recovery - Strategic plans designate actions, responsibilities, accountability, resources and timeframes for achieving objectives and targets			

4.4.1 Resources, Roles, Responsibility, and Authority	- Ensure the availability of resources essential for the implementation and control of the ORMS. - Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective OR management.	- Establish procedures, roles and responsibilities to cover all normal and abnormal operating conditions, including disruptions and emergencies. - Establish management processes and procedures for human resources including employees, contractors, temporary staff, etc. - Identify and assure availability of human, infrastructure and financial resources in the event of a disruption. - Establish and document provisions for adequate finance and administrative resources and procedures to support the management program or system normal and abnormal conditions. - Make arrangements for supply chain obligations, mutual aid and community assistance. - Determine the local, regional and public authorities' roles, relationships and interactions with the Organisation's management system implementation plans.	- Executive management appoints a specific management representative responsible for the ORMS - Formal resilience management responsibilities and relationships are defined and adhered to - Teams with defined roles and adequate resources are established to support resilience action plans - Establish arrangements for stakeholder assistance, communication, strategic alliances and mutual aid - Identify financial and administrative procedures needed to support the resilience programs and meet objectives and targets - Roles, relationships and interactions with local regional and public authorities (including first responders) are defined - Adequate resources allocated in accordance with action plan			

4.4.2 Competence, Training, and Awareness	Awareness, competence and training strategies, plans, programs and procedures	- Identify and establish skills, competency requirements, and qualifications needed by the Organisation to maintain operations. - Assess, develop and implement training/ and education program for the Organisation's personnel, contractors, and other relevant stakeholders. - Develop Organisational awareness and establish a culture to support resilience management. - Determine Organisational interface protocol, identification and training requirements and assign appropriate internal staff or support representatives. - Develop tools to enhance situational awareness.	- Identify competencies and training needs associated with achieving the resilience objectives, targets and programs - Develop and implement a program to address competence and training needs - Assess competence against requirements and ensure they are met			

4.4.3 Communication and Warning	Communication and warning strategies, plans, programs and procedures	- Establish procedures and make arrangements for communications both within the Organisation and to/from external sources. - Document procedures and identify tools to manage relationships and communications processes with external stakeholders including supply chain business partners, first responders, governmental agencies, vendors, etc. - Develop, coordinate, evaluate and exercise plans to communicate information and warnings with internal stakeholders, external stakeholders (including the media) for normal and abnormal conditions. - Develop and maintain reliable communications and warning capability in the event of a disruption.	- Identify what will be communicated and to whom regarding the resilience policy, risks, objectives, targets and programs - Establish communications feedback mechanisms - Identify target audiences for communications and warnings to ensure effective two-way dialogue - Determine information sharing and security needs - Ensure ongoing communications capacity in the event of a disruptive incident			
4.4.4 Documentation	Organisational resilience documentation	- Establish processes and procedures for management of documents which are essential to the successful implementation and operation of the resilience management system and programs. - Document the procedures, processes, work plans and forms to support the management system and its elements, as well as for use before, during and after a disruptive incident.	- Establish resilience management documentation system - Determine security, sensitivity and information integrity needs and take appropriate steps to protect information and documentation			

4.4.5 Control of Documents	Documentation control	- Establish processes and procedures for control of documents and records (including back-up) to protect the integrity and access to documentation and essential information.	- Establish processes and procedures for control of documents and records for access, back-up confidentiality, storage, retention, archiving and destruction			

4.4.6 Operational Control	Developing and implementing operational and risk control strategies, plans, procedures and programs	- Establish operational control measures needed to implement the strategic plans and maintain control of activities and functions against defined targets, as well as the unexpected. - Develop procedures for controlling key activities, functions and operations that are associated with the Organisation. - Establish processes and procedures for operational management and maintenance of infrastructure, plant, facilities, technologies, finance, etc. which have an impact on the Organisation's performance, its supply chain and stakeholders. - Establish operational control measures needed to implement the strategic programs and maintain control of activities and functions. - Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident.	- Based on the risk assessment, objectives, targets and programs identify where controls are needed and what they will achieve in terms of risk reduction - Consider ways of minimizing risk in day-to-day operations - Priority is given to proactive Approaches - Controls specify how to conduct activities and functions including engineering controls, administrative controls, technical specifications and contractual agreements			

4.4.7 Incident Prevention, Preparedness, and Response	- Risk avoidance, mitigation, reduction, sharing and treatment procedures - Reactive, proactive, and adaptive incident management	- Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident. - Establish, document and implement procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event using personnel. - Establish, implement, and maintain procedures to avoid, prevent, protect from and mitigate a disruptive event. - Develop action plans for increased threat levels. - Establish, implement, and maintain procedures to manage a disruptive event and continue its activities based on recovery objectives. - Establish, documented procedures for how the Organisation will manage a disruptive event; and recover or maintain its activities to a predetermined level.	- Based on the risk assessment, objectives, targets and programs establish, implement, and maintain procedures to identify potential disruptive incidents that can have impacts on the Organisation, its activities, functions, services, stakeholders, and the environment - Proactively document with detailed procedures and work plans how the Organisation will prevent, prepare for, and respond to disruptive incidents - Periodically review and, where necessary, revise its incident prevention, preparedness, and response procedures			

4.5.1 Monitoring and Measurement	Performance evaluation	- Establish metrics and mechanisms by which the Organisation assesses its ability to achieve its objectives and targets on an ongoing basis. - Monitor, measure, and assess the Organisation's resilience performance on an ongoing basis.	- Establish, implement, and maintain performance metrics and procedures to monitor and measure, on a regular basis, those characteristics of its operations that have material impact on its resilience performance			
4.5.2.1 Evaluation of Compliance	Compliance evaluation	- Monitor, measure, and assess the Organisation's legal and regulatory compliance performance on an ongoing basis.	- Establish, implement, and maintain (a) procedure(s) for periodically evaluating compliance with applicable legal and other requirements			
4.5.2.2 Exercises and Testing	Testing and system evaluation	- Test and evaluate appropriateness and efficacy of its ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies) - Plan, coordinate, and conduct tests and exercises, and evaluate and document results.	- Validate the ORMS using testing and exercises - Test and evaluate appropriateness and effectiveness of action plans and procedures as well as interrelationship of elements in ORMS - Include appropriate external parties (e.g. first responders) and stakeholders			

4.5.3 Non-conformity, Corrective Action, and Preventive Action	- Analysing and handling non-conformities - Improvement	- Determine non-conformities and the manner in which these are dealt with. - Establish and implement mechanism for eliminating the causes of detected non-conformities both in the management system and the operational processes. - Establish and implement mechanisms for instigating action to eliminate potential causes of non-conformities in both the management system and the operational processes.	- Determine non-conformities in the ORMS, risk assessment, objectives, targets programs, action plans, and their implementation - Analyze why something went wrong - Determine the manner in which these are dealt with to eliminate the causes and prevent their recurrence - Identify what could go wrong and take actions to prevent occurrence			
4.5.4 Control of Records	Control of records	- Establish and maintain records to demonstrate conformity to the requirements of its ORMS and the results achieved.	- Evidence addressing ORMS implementation and results are collected and retained			
4.5.5 Internal Audits	System audits	- Conduct internal audits of system and programs. - Report audits and verification results in management review.	- Determine what needs to be audited - Plan and implement an audit program - Report audit findings to management and act upon them			

4.6 Management Review	Management review	- Management review of the system to determine its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary. - Set priorities, policy, objectives and targets to support continual improvement.	- Identify inputs to review process - Review the suitability, adequacy and effectiveness of the ORMS			
4.6.4 Maintenance	System maintenance	- Make provisions for improvement of programs, systems, and/or operational processes.	- Ensure that any internal or external changes that impact the Organisation are reviewed in relation to the ORMS			
4.6.5 Continual Improvement	Continual improvement	- Provisions made for continual improvement of the management system and resilience performance.	- Continually improve the effectiveness of ORMS through the use of the Organisational resilience management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review.			
				TOTAL POSSIBLE SCORE		
				ACTUAL SCORE		
				PERCENTAGE ACHIEVED		

TABLE 5: PHASE 5: Management System: LEVEL 5 (Platinum)

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard						
PHASE 5: Management System: LEVEL 5 (Platinum)						
ANSI/ASIS SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Management System**	**Documentary or Other Proof Requirements**	**Score**	
Generic Concepts	Key elemental theme	Description of element	- The Organisation is in conformance with the requirements of the standard - The Organisation establishes, documents, implements, maintains, and continually improves an Organisation resilience management system in accordance with the requirements of the ORMS Standard, and determines how it will fulfil the requirements. - Examines the linkages and interactions between the elements that compose the entirety of the system - Manage risk using balanced strategies to adaptively, proactively and reactively address minimization of both likelihood and consequences of disruptive events - Resilience management becomes part of the routine management of projects and business processes - Manage risk using balanced strategies to adaptively, proactively and reactively address minimization of both likelihood and consequences of disruptive events - Resilience management becomes part of the routine management of projects and business processes			

4.1.1 Scope of OR Management System	- Understanding the Organisation and its context - Scope of ORMS	- Establish the internal, external and risk management context of the Organisation - Define scope and boundaries for development and implementation of ORMS.	- Organisation defines and documents the internal, external and resilience management context, as well as Organisation-wide risk management Interactions - Boundaries of scope defined and documented considering the Organisation's mission, goals, internal and external obligations, and legal responsibilities			
4.2.1 Policy Statement	- Setting a policy framework	- Establish a policy to provide a framework for setting objectives and provide the direction and principles for action. Demonstrates management commitment	- Policy establishes framework for resilience management by setting objectives and providing direction - Clear commitment to comply with applicable legal and other requirements - Endorsed and promoted by top management - Communicated throughout Organisation and to stakeholders making them aware of content and meaning			
4.2.2 Management Commitment	- Management mandate and commitment	- Demonstrate executive management and the Organisation's commitment to meeting the requirements of resilience management. - Establish the project to address resilience management including provision of appropriate resources and authorization to conduct project.	- Documented evidence of its mandate and commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ORMS - Defined and documented criteria to be used to evaluate the significance of risk, determination of appropriate risk treatments, and setting of timeframes for recovery - Sufficient resources allocated and competencies assured			

4.3.1 Risk Assessment and Impact Analysis	- Asset, activities, functions and services identification and valuation - Risk identification - Risk Analysis - Risk Evaluation	- Establish a process for risk identification, analysis and evaluation. - Identify assets, activities, needs, requirements and analysis of critical issues related to business disruption risks that are relevant to the Organisation and stakeholders. - Identify of hazards threats, vulnerabilities and consequences. - Evaluate of the effect of uncertainty on the Organisation's objectives. - Evaluate of the likelihood of a disruptive event and its consequences on assets (human, physical, cyber, environmental, information, and intangibles). - Evaluate dependencies and interdependencies with other assets and sectors, and consequences a disruptive event. - Evaluate and establish timeframes for response and recovery.	- Establish, implement, and maintain an ongoing formal and documented risk assessment process - Prioritize risks and impacts are taken into account in establishing, implementing, and operating the ORMS - Periodically review whether OR management scope, policy, and risk assessment are still appropriate given the Organisations' internal and external context - Re-evaluate risk and impacts within the context of changes within the Organisation or made to the Organisation's operating environment, procedures, functions, services, partnerships, and supply chains			

4.3.2 Legal and Other Requirements	- Identify legal, regulatory, and other requirements to which the Organisation subscribes - Determine how these requirements apply to the Organisation, its risks and their potential impact.	- Identify legal and other requirements which govern the Organisation's activity. - Establish a procedure or process for identifying, registering and evaluating internal and external requirements pertinent to the Organisation's functions, activities and operations. - Understand and communicate potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to location and industry.	- Establish and maintain procedures to identify legal and other requirements - Determine how the legal and other requirements apply to the Organisation risks and obligations - Ensure that applicable legal, regulatory, and other requirements are considered in developing, implementing, and maintaining its Organisational resilience management system - Document information and keep it up-to-date			

4.3.3 Objectives, Targets, and Program(s)	- Setting objectives and developing risk and incident prevention, protection, preparedness, mitigation, response, continuity and recovery management strategies - Risk prioritization and treatment	- Prioritize the issues identified as a result of the risk assessment and impact analysis. - Set objectives and targets (including time frames) based on the prioritization of issues within the context of an Organisation's policy and mission. - Develop strategic plans for incident prevention, protection, preparedness, mitigation, response, continuity and recovery. - Identify resources needed and the availability of adequate human, infrastructure, processing and financial resources. - Identify roles, responsibilities, authorities and their interrelationships within the Organisation as far as needed to ensure effective and efficient operations. - Plan the operational processes for actions effecting how the objectives and targets are achieved. - Make internal and external arrangements, agreements, and contingency plans that need to be in place to manage foreseeable emergencies.	- Documented objectives and targets are established to manage resilience by avoiding, accepting, removing the source, changing the likelihood, changing the consequences, sharing and/or retaining the risk - Objectives provide a basis for selecting one or more options for modifying risks considering asset value, opportunities for reducing likelihood and/or consequences, cost/benefit, and tolerable levels of residual risk - Targets are measurable, achievable, relevant and time-based - Establish, implement and maintain one or more program(s) for risk treatment in order to achieve its objectives and targets - Risk treatment options (defined in action plans) consider the prevention, protection, deterrence, mitigation, respond, and recover from disruptive incidents. The programs shall be optimized and prioritized in order to control and treat risks associated with threats, hazards and impacts of disruptions to the Organisation and its stakeholders			

4.4.1 Resources, Roles, Responsibility, and Authority	- Ensure the availability of resources essential for the implementation and control of the ORMS. - Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective OR management.	- Establish procedures, roles and responsibilities to cover all normal and abnormal operating conditions, including disruptions and emergencies. - Establish management processes and procedures for human resources including employees, contractors, temporary staff, etc. - Identify and assure availability of human, infrastructure and financial resources in the event of a disruption. - Establish and document provisions for adequate finance and administrative resources and procedures to support the management program or system normal and abnormal conditions. - Make arrangements for supply chain obligations, mutual aid and community assistance. - Determine the local, regional and public authorities' roles, relationships and interactions with the Organisation's management system implementation plans.	- Roles, responsibilities, and authorities are defined, documented, and communicated in order to facilitate effective Organisational resilience management, consistent with the achievement of its Organisational resilience management policy, objectives, targets and programs - Resilience, crisis, and response team(s) with defined roles, appropriate authority, and adequate resources to oversee incident management are established - Logistical capabilities and procedures to locate, acquire, store, distribute, maintain, test, and account for services, personnel, resources, materials, and facilities produced or donated to support the Organisational resilience management system are established - Procedures for stakeholder assistance, communications, strategic alliances, and mutual aid are established			

4.4.2 Competence, Training, and Awareness	Awareness, competence and training strategies, plans, programs and procedures	- Identify and establish skills, competency requirements, and qualifications needed by the Organisation to maintain operations. - Assess, develop and implement training/ and education program for the Organisation's personnel, contractors, and other relevant stakeholders. - Develop Organisational awareness and establish a culture to support resilience management. - Determine Organisational interface protocol, identification and training requirements and assign appropriate internal staff or support representatives. - Develop tools to enhance situational awareness.	- Ensure that any person(s) performing tasks who have the potential to prevent, cause, respond to, mitigate, or be affected by significant hazards, threats, and risks are competent (on the basis of appropriate education, training, or experience - Retain associated training and competence records - Build, promote, and embed a resilience management culture within the Organisation			

4.4.3 Communication and Warning	Communication and warning strategies, plans, programs and procedures	- Establish procedures and make arrangements for communications both within the Organisation and to/from external sources. - Document procedures and identify tools to manage relationships and communications processes with external stakeholders including supply chain business partners, first responders, governmental agencies, vendors, etc. - Develop, coordinate, evaluate and exercise plans to communicate information and warnings with internal stakeholders, external stakeholders (including the media) for normal and abnormal conditions. - Develop and maintain reliable communications and warning capability in the event of a disruption.	- Decide how proactive each type of communication should be with each audience - Develop key messages and set communication targets, objectives and performance indicators - Assign responsibilities and establish timelines for communications - Establish, document and maintain procedures for internal and external communications - Communication on resilience issues occurs throughout the Organisation and with appropriate stakeholders - Structured communication with emergency and first responders - Determine needs and establish a communication facility - Set communications protocols for normal and abnormal conditions			

4.4.4 Documentation	Organisational resilience documentation	- Establish processes and procedures for management of documents which are essential to the successful implementation and operation of the resilience management system and programs. - Document the procedures, processes, work plans and forms to support the management system and its elements, as well as for use before, during and after a disruptive incident.	- Develop and organize documentation system - Prepare a resilience manual outlining the structure of the ORMS - Documentation supports the establishment, definition and implementation of the ORMS			
4.4.5 Control of Documents	Documentation control	- Establish processes and procedures for control of documents and records (including back-up) to protect the integrity and access to documentation and essential information.	- Establish processes and procedures for control of documents and records including information security and protection and document integrity			

4.4.6 Operational Control	Developing and implementing operational and risk control strategies, plans, procedures and programs	- Establish operational control measures needed to implement the strategic plans and maintain control of activities and functions against defined targets, as well as the unexpected. - Develop procedures for controlling key activities, functions and operations that are associated with the Organisation. - Establish processes and procedures for operational management and maintenance of infrastructure, plant, facilities, technologies, finance, etc. which have an impact on the Organisation's performance, its supply chain and stakeholders. - Establish operational control measures needed to implement the strategic programs and maintain control of activities and functions. - Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident.	- Establish, implement, and maintain adaptive and proactive procedures for those operations that are associated with the identified significant risks, consistent with its Organisational resilience management policy, risk assessment, supply chain requirements, objectives, and targets, in order to ensure that they are carried out under specified conditions minimizing the risk - Control procedures are written and/or reviewed by persons involved in operations and communicated effectively to others such as contractors and suppliers			

4.4.7 Incident Prevention, Preparedness, and Response	- Risk avoidance, mitigation, reduction, sharing and treatment procedures - Reactive, proactive, and adaptive incident management	- Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident. - Establish, document and implement procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event using personnel. - Establish, implement, and maintain procedures to avoid, prevent, protect from and mitigate a disruptive event. - Develop action plans for increased threat levels. - Establish, implement, and maintain procedures to manage a disruptive event and continue its activities based on recovery objectives. - Establish, documented procedures for how the Organisation will manage a disruptive event; and recover or maintain its activities to a predetermined level.	- Establish, implement, and maintain procedures to avoid, prevent, protect from mitigate, respond to and recover from a disruptive event and continue its activities based on resilience objectives developed through the risk assessment process - Prepare for and respond to actual disruptive incidents to prevent the incident, minimize likelihood of its occurrence, or mitigate associated adverse consequences - Ensure that any persons performing incident prevention and management measures on its behalf are competent - Establish, document and implement procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event - Establish detailed procedures for how the Organisation will respond to and manage a disruptive event and how it will recover or maintain its activities to a predetermined level, based on management-approved recovery objectives			

4.5.1 Monitoring and Measurement	Performance evaluation	- Establish metrics and mechanisms by which the Organisation assesses its ability to achieve its objectives and targets on an ongoing basis. - Monitor, measure, and assess the Organisation's resilience performance on an ongoing basis.	- Monitor performance, applicable operational controls, and conformity with the Organisation's Organisational resilience management objectives and targets - Evaluate and document the performance of the systems which protect assets, communications and information systems			
4.5.2.1 Evaluation of Compliance	Compliance evaluation	- Monitor, measure, and assess the Organisation's legal and regulatory compliance performance on an ongoing basis.	- Record and report the results of the evaluation with corrective measures and recommendations for improvement			
4.5.2.2 Exercises and Testing	Testing and system evaluation	- Test and evaluate appropriateness and efficacy of its ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies) - Plan, coordinate, and conduct tests and exercises, and evaluate and document results. - Review exercise results with management to ensure lessons learned and appropriate action is taken.	- Test and evaluate the appropriateness and efficacy of ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies) - Produce a formalized post-exercise report that contains outcomes, recommendations, and arrangements to implement improvements in a timely fashion			

4.5.3 Non-conformity, Corrective Action, and Preventive Action	- Analysing and handling non-conformities - Improvement	- Determine nonconformities and the manner in which these are dealt with. - Establish and implement mechanism for eliminating the causes of detected nonconformities both in the management system and the operational processes. - Establish and implement mechanism for instigating action to eliminate potential causes of non-conformities in both the management system and the operational processes.	- Establish, implement, and maintain procedures for dealing with actual and potential nonconformities and for taking corrective action and preventive action - Review effectiveness of corrective actions and take preventative actions			
4.5.4 Control of Records	Control of records	- Establish and maintain records to demonstrate conformity to the requirements of its ORMS and the results achieved.	- Evidence addressing ORMS implementation and results are collected and retained			
4.5.5 Internal Audits	System audits	- Conduct internal audits of system and programs. - Report audits and verification results in management review.	- Responsibility of audit program assign to individual that has knowledge and understanding of audit principles - Determine whether the control objectives, risk controls, processes, and procedures of ORMS are conducted properly and achieving the desired results - Identify opportunities for improvement - Ensure that actions are taken without undue delay to eliminate detected non-conformities and their causes			

4.6 Management Review	Management review	- Management review of the system to determine its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary. - Set priorities, policy, objectives and targets to support continual improvement.	- Top management review the ORMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness - Assess opportunities for improvement and the need for changes to ORMS, including the Organisational resilience management system policy and objectives, target and risk criteria			
4.6.4 Maintenance	System maintenance	- Make provisions for improvement of programs, systems, and/or operational processes.	- Identify any new critical activities that need to be included in the ORMS program			
4.6.5 Continual Improvement	Continual improvement	- Provisions made for continual improvement of the management system and resilience performance.	- Continually improve the effectiveness of ORMS through the use of the Organisational resilience management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review			
				TOTAL POSSIBLE SCORE		
				ACTUAL SCORE		
				PERCENTAGE ACHIEVED		

TABLE 6: PHASE 6: Holistic Management: LEVEL 6 (Diamond)

Maturity Model for the Phased Implementation of the *ANSI/ASIS SPC.1-2009* Organisational Resilience Standard						
PHASE 6: Holistic Management: LEVEL 6 (Diamond)						
ANSI/ASIS SPC.1 Standard Clause	**Core Element**	**Issues Addressed by Core Element**	**Holistic Management**	**Documentary or Other Proof Requirements**	**Score**	
Generic Concepts	Key elemental theme	Description of element	- The Organisation goes beyond conformance to the standard to fully integrate resilience management into its overall risk management strategy - The Organisation emphasizes enterprise-wide and supply chain relationships in all aspects of it resilience management system. - The Organisation mentors other stakeholder (in its supply chain and community) recognizing that Organisational resilience is an integral part of community resilience - Resilience management culture is well developed and considered a inseparable part of decision making - Resilience management and systems principles are expanded to all areas of business and activities			
4.1.1 Scope of OR Management System	- Understanding the Organisation and its context - Scope of ORMS	- Establish the internal, external and risk management context of the Organisation - Define scope and boundaries for development and implementation of ORMS.	- Organisation defines and documents the internal, external and resilience management context, as well as enterprise-wide risk management interactions and supply chain tier, commitments and relationships - Boundaries of scope defined and documented			

4.2.1 Policy Statement	- Setting a policy framework	- Establish a policy to provide a framework for setting objectives and provide the direction and principles for action. - Demonstrates management commitment	- Policy establishes framework for internal and external resilience management by setting objectives and providing direction - Clear commitment to comply with applicable legal and other requirements - Endorsed and promoted by executive management - Communicated throughout Organisation, enterprise and supply chain			
4.2.2 Management Commitment	- Management mandate and commitment	- Demonstrate executive management and the Organisation's commitment to meeting the requirements of resilience management. - Establish the project to address resilience management including provision of appropriate resources and authorization to conduct project.	- Documented evidence of its mandate and commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ORMS - Defined and documented criteria to be used to evaluate the significance of risk, determination of appropriate risk treatments, and setting of timeframes for recovery for the Organisation and relevant stakeholders			

4.3.1 Risk Assessment and Impact Analysis	- Asset, activities, functions and services identification and valuation - Risk identification - Risk Analysis - Risk Evaluation	- Establish a process for risk identification, analysis and evaluation. - Identify assets, activities, needs, requirements and analysis of critical issues related to business disruption risks that are relevant to the Organisation and stakeholders. - Identify of hazards threats, vulnerabilities and consequences. - Evaluate the effect of uncertainty on the Organisation's objectives. - Evaluate the likelihood of a disruptive event and its consequences on assets (human, physical, cyber, environmental, information, and intangibles). - Evaluate dependencies and interdependencies with other assets and sectors, and consequences a disruptive event. - Evaluate and establish timeframes for response and recovery.	- Establish, implement, and maintain an on going formal and documented risk assessment process - Establish, implement, and maintain a formal and documented communication and consultation process with stakeholders and supply chain partners in the risk assessment process - Establish, implement, and maintain a formal and documented process for monitoring and reviewing the risk assessment process			

4.3.2 Legal and Other Requirements	- Identify legal, regulatory, and other requirements to which the Organisation subscribes - Determine how these requirements apply to the Organisation, its risks and their potential impact.	- Identify legal and other requirements which govern the Organisation's activity. - Establish a procedure or process for identifying, registering and evaluating internal and external requirements pertinent to the Organisation's functions, activities and operations. - Understand and communicate potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to location and industry.	- Establish and maintain procedures to identify legal and other requirements relevant to the Organisation and appropriate stakeholders - Determine how the legal and other requirements apply to the Organisation and stakeholder risks and obligations			

4.3.3 Objectives, Targets, and Program(s)	- Setting objectives and developing risk and incident prevention, protection, preparedness, mitigation, response, continuity and recovery management strategies - Risk prioritization and treatment	- Prioritize the issues identified as a result of the risk assessment and impact analysis. - Set objectives and targets (including time frames) based on the prioritization of issues within the context of an Organisation's policy and mission. - Develop strategic plans for incident prevention, protection, preparedness, mitigation, response, continuity and recovery. - Identify resources needed and the availability of adequate human, infrastructure, processing and financial resources. - Identify roles, responsibilities, authorities and their interrelationships within the Organisation as far as needed to ensure effective and efficient operations. - Plan the operational processes for actions effecting how the objectives and targets are achieved. - Make internal and external arrangements, agreements, and contingency plans that need to be in place to manage foreseeable emergencies.	- Documented objectives and targets establish internal and external expectations for the Organisation and its stakeholders that are critical to mission accomplishment, product and service delivery, and functional operations			

4.4.1 Resources, Roles, Responsibility, and Authority	- Ensure the availability of resources essential for the implementation and control of the ORMS. - Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective OR management.	- Establish procedures, roles and responsibilities to cover all normal and abnormal operating conditions, including disruptions and emergencies. - Establish management processes and procedures for human resources including employees, contractors, temporary staff, etc. - Identify and assure availability of human, infrastructure and financial resources in the event of a disruption. - Establish and document provisions for adequate finance and administrative resources and procedures to support the management program or system normal and abnormal conditions. - Make arrangements for supply chain obligations, mutual aid and community assistance. - Determine the local, regional and public authorities' roles, relationships and interactions with the Organisation's management system implementation plans.	- Roles, responsibilities, and authorities are defined, documented, and communicated in order to facilitate effective Organisational resilience management within the Organisation, enterprise-wide and within the community consistent with achieving Organisation, stakeholder, supply chain and community resilience objectives, targets and programs			

4.4.2 Competence, Training, and Awareness	Awareness, competence and training strategies, plans, programs and procedures	- Identify and establish skills, competency requirements, and qualifications needed by the Organisation to maintain operations. - Assess, develop and implement training/ and education program for the Organisation's personnel, contractors, and other relevant stakeholders. - Develop Organisational awareness and establish a culture to support resilience management. - Determine Organisational interface protocol, identification and training requirements and assign appropriate internal staff or support representatives. - Develop tools to enhance situational awareness.	- Build, promote, and embed a resilience management culture within the Organisation, enterprise, supply chain and community - Ensure the resilience management culture becomes part of the Organisation's core values and Organisational governance - Stakeholders aware of the Organisational resilience management policy and their role in any plans			

4.4.3 Communication and Warning	Communication and warning strategies, plans, programs and procedures	- Establish procedures and make arrangements for communications both within the Organisation and to/from external sources. - Document procedures and identify tools to manage relationships and communications processes with external stakeholders including supply chain business partners, first responders, governmental agencies, vendors, etc. - Develop, coordinate, evaluate and exercise plans to communicate information and warnings with internal stakeholders, external stakeholders (including the media) for normal and abnormal conditions. - Develop and maintain reliable communications and warning capability in the event of a disruption.	- Identify external communications and warning needs and capacity of stakeholders supply chain and community - Determine reliability of external communications infrastructure and to augment system internally and externally in the event of a disruption			
4.4.4 Documentation	Organisational resilience documentation	- Establish processes and procedures for management of documents which are essential to the successful implementation and operation of the resilience management system and programs. - Document the procedures, processes, work plans and forms to support the management system and its elements, as well as for use before, during and after a disruptive incident.	- Evaluate document and information sharing needs with stakeholders, supply chain and community			

4.4.5 Control of Documents	Documentation control	- Establish processes and procedures for control of documents and records (including back-up) to protect the integrity and access to documentation and essential information.	- Evaluate stakeholder and supply chain information needs			
4.4.6 Operational Control	Developing and implementing operational and risk control strategies, plans, procedures and programs	- Establish operational control measures needed to implement the strategic plans and maintain control of activities and functions against defined targets, as well as the unexpected. - Develop procedures for controlling key activities, functions and operations that are associated with the Organisation. - Establish processes and procedures for operational management and maintenance of infrastructure, plant, facilities, technologies, finance, etc. which have an impact on the Organisation's performance, its supply chain and stakeholders. - Establish operational control measures needed to implement the strategic programs and maintain control of activities and functions. - Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident.	- Address reliability and resiliency, the safety and health of people, and the protection of property, supply chain and other stakeholder needs, and the environment potentially impacted by a disruptive incident - Ensure demand signals are comprehended in capacity planning - Priority is given to adaptive approaches - Ensure processes are in place to validate supplier responses			

4.4.7 Incident Prevention, Preparedness, and Response	- Risk avoidance, mitigation, reduction, sharing and treatment procedures - Reactive, proactive, and adaptive incident management	- Establish and implement risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident. - Establish, document and implement procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event using personnel. - Establish, implement, and maintain procedures to avoid, prevent, protect from and mitigate a disruptive event. - Develop action plans for increased threat levels. - Establish, implement, and maintain procedures to manage a disruptive event and continue its activities based on recovery objectives. - Establish, documented procedures for how the Organisation will manage a disruptive event; and recover or maintain its activities to a predetermined level.	- Identify the Organisations potential role in supporting the capacity of stakeholders, the supply chain and the community to avoid, prevent, protect from mitigate, respond to and recover from a disruptive event - Established detailed procedures for stakeholders, the supply chain and the community support			
4.5.1 Monitoring and Measurement	Performance evaluation	- Establish metrics and mechanisms by which the Organisation assesses its ability to achieve its objectives and targets on an ongoing basis. - Monitor, measure, and assess the Organisation's resilience performance on an ongoing basis.	- Include partnership and supply chain relationships			

4.5.2.1 Evaluation of Compliance	Compliance evaluation	- Monitor, measure, and assess the Organisation's legal and regulatory compliance performance on an ongoing basis.	- Report to relevant stakeholders as appropriate			
4.5.2.2 Exercises and Testing	Testing and system evaluation	- Test and evaluate appropriateness and efficacy of its ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies) - Plan, coordinate, and conduct tests and exercises, and evaluate and document results. - Review exercise results with management to ensure lessons learned and appropriate action is taken.	- Test and evaluate the appropriateness and efficacy of ORMS with stakeholders, supply chain and community			
4.5.3 Non-conformity, Corrective Action, and Preventive Action	- Analysing and handling non-conformities - Improvement	- Determine nonconformities and the manner in which these are dealt with. - Establish and implement mechanism for eliminating the causes of detected nonconformities both in the management system and the operational processes. - Establish and implement mechanism for instigating action to eliminate potential causes of non-conformities in both the management system and the operational processes.				
4.5.4 Control of Records	Control of records	- Establish and maintain records to demonstrate conformity to the requirements of its ORMS and the results achieved.				

4.5.5 Internal Audits	System audits	- Conduct internal audits of system and programs. - Report audits and verification results in management review.	- Audit includes stakeholder and community interactions, as well the supply chain			
4.6 Management Review	Management review	- Management review of the system to determine its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary. - Set priorities, policy, objectives and targets to support continual improvement.	- Review integrated with overall risk management and business review processes - Review includes evaluation of suitability, adequacy, and effectiveness with regard to stakeholders, community and supply chain			
4.6.4 Maintenance	System maintenance	- Make provisions for improvement of programs, systems, and/or operational processes.	- Ensure that any internal or external changes that impact the Organisation, the overall enterprise, stakeholders and the supply chain are reviewed in relation to the ORMS			
4.6.5 Continual Improvement	Continual improvement	- Provisions made for continual improvement of the management system and resilience performance.	- Continually improve the effectiveness of ORMS through the use of the Organisational resilience management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review.			
				TOTAL POSSIBLE SCORE		
				ACTUAL SCORE		
				PERCENTAGE ACHIEVED		