INFORMATION SECURITY RISK MANAGEMENT IN THE SOUTH AFRICAN SMALL, MEDIUM AND MICRO ENTERPRISE ENVIRONMENT:

THE PECULIUM MODEL

By

LIESL VAN NIEKERK

DISSERTATION

Submitted in fulfilment of the requirement for the degree

MASTER OF SCIENCE

in

INFORMATICS

in the

FACULTY OF SCIENCE

at the

UNIVERSITY OF JOHANNESBURG

SUPERVISOR: PROF L LABUSCHAGNE

NOVEMBER 2005

ABSTRACT

The small, medium and micro enterprise (SMME) environment of South Africa contributes 42% to the national gross domestic product. This is a high number for a largely under-regulated environment.

The corporate governance and IT governance standards that apply to South African companies are not feasible for SMMEs, and neither are they enforced, although 80% of failures of SMMEs are attributable to lack of enterprise management skill.

The first objective of this dissertation is to examine the South African SMME, and in so doing determine whether local regulatory standards can be used for this unique enterprise formation.

The second objective of this dissertation is to determine whether international methodologies for information security risk management, as an inclusive of IT governance, may be used in the unique local SMME formation.

The result of these two objectives creates a gap in a typical information security risk management methodology that is suitable for the South African regulatory and economic environment for SMMEs. A model has been created as a possible answer for filling the gap.

The dissertation includes the Peculium Model, which answers the regulatory and economic requirements that resulted from the second objective. The Model allows the small enterprise a simple but effective method for managing risks to its information assets, with the control of corporate governance and IT governance included in its framework. The Model answers the methods for identifying and assessing risk in a tradition-based but feasible new qualitative technique.

OPSOMMING

Die omgewing van klein, medium en mikro-ondernemings (KMMO's) in Suid-Afrika dra 42% tot die nasionale bruto binnelandse produk by. Dit is 'n groot persentasie vir 'n omgewing wat nie veel regulering geniet nie.

Die standaarde vir korporatiewe regering en IT-regering wat op die Suid-Afrikaanse maatskappy van toepassing is, is nie noodwendig gepas vir KMMO's nie en word ook nie afgedwing nie, al faal 80% van KMMO's as gevolg van 'n gebrek aan bestuursvernuf.

Die eerste doelwit van hierdie verhandeling is om die Suid-Afrikaanse KMMO te ondersoek en sodoende uit te vind of plaaslike reguleringstandaarde wel vir hierdie unieke ondernemingstruktuur gebruik kan word.

Die tweede doelwit van die verhandeling is om uit te vind of internasionale metodologieë vir inligtingsekerheid-risikobestuur (ISRB) as deel van IT-regering gebruik kan word in die unieke plaaslike KMMO-struktuur.

Die uitslag van hierdie twee doelwitte skep 'n gaping in 'n tipiese ISRB-metodologie ten opsigte van wat geskik is vir die Suid-Afrikaanse regulerende en ekonomiese omgewing van KMMO's. 'n Model is as moontlike oplossing geskep om hierdie gaping te vul.

Hierdie verhandeling sluit die Peculium-model in wat inpas by die regulerende en ekonomiese vereistes wat uit die tweede doel voortspruit. Die Model verskaf 'n effektiewe dog eenvoudige metode vir die bestuur van risiko's wat inligtingsbates bedreig, terwyl die beheer van korporatiewe regering en IT-regering in die raamwerk ingesluit word. Die metode behels die identifisering en assessering van risiko's met behulp van 'n tradisiegebaseerde, maar bruikbare nuwe kwalitatiewe tegniek.

Acknowledgements

This has been both a stimulating and exciting adventure which can never be reduced in its meaning or importance in my academic career. I have been close to the plight of the SMME and as such, I am satisfied that I have contributed to the body of knowledge for the South African SMME community.

I wish to thank my family and friends for their unwavering support in this journey. Your frowns and raised eyebrows spurred me ever on in trying to simplify my explanations. I have since given up that thankless route. The journey would have been a distinctly lonely path without you all.

Thank you.

The financial assistance of the South African Department of Labour (DoL) in this research is hereby acknowledged.

Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the DoL.

Contents

List of Tables

List of Figures

1 Introduction

1.1 The South African SMME

South Africa has recently celebrated ten years of democracy since the first democratic elections in 1994. The country has undergone many changes, including social, cultural and economic. South Africa has been incorporated into various international associations, unions and societies, including the United Nations, the Commonwealth and the African Union, of which President Thabo Mbeki holds the chairmanship [UN 2005] [CW 2005] [AU 2005]. These relationships with the global village have established South Africa as a preferred tourist destination and investment opportunity [TOUR 2005].

The South African economy has grown considerably, with black empowerment being supported by the state and investors to develop previously disadvantaged communities, and as a result the economy. Government has also targeted small, medium and micro enterprises (SMMEs) for development [NATI 2003].

These enterprises form a sizable portion of the gross domestic product (GDP). The SMME market portion contributes 42% to the GDP, but comprises an estimated 99% of the total enterprises in the economy, as presented in Table 1.1 [SOUT 2002] [NATI 2003].[1]

[1] Survivalist and very small enterprises are included in the SMME grouping although not formally defined as such.

Table 1.1: Estimated distribution of private sector enterprises [NATI 2003]

Sector	Survivalist	Micro	Very Small	Small	Medium	Large	Total
Agriculture	14 700	39 800	17 900	20 900	3 240	1 520	98 100
Percentage of total	15%	41%	18%	21%	3%	2%	100%
Mining	1 100	2 500	500	131	112	137	4 480
Percentage of total	25%	56%	11%	3%	3%	3%	100%
Manufacturing	19 600	45 700	30 600	4 800	3 840	1 479	106 019
Percentage of total	18%	43%	29%	5%	4%	1%	100%
Construction	19 900	51 700	13 300	2 300	996	320	88 516
Percentage of total	22%	58%	15%	3%	1%	0%	100%
Wholesale trade	900	6 500	8 900	3 270	660	577	20 807
Percentage of total	4%	31%	43%	16%	3%	3%	100%
Retail trade	91 700	173 500	43 300	13 100	970	744	323 314
Percentage of total	28%	54%	13%	4%	0%	0%	100%
Catering and accommodation	2 300	9 000	660	3 450	385	124	15 919
Percentage of total	14%	57%	4%	22%	2%	1%	100%
Transport	7 600	43 000	6 200	1 400	293	303	58 796
Percentage of total	13%	73%	11%	2%	0%	1%	100%
Finance and business services	7 700	10 300	24 300	4 600	301	425	47 626
Percentage of total	16%	22%	51%	10%	1%	1%	100%
Community, social and personal services	18 900	53 900	28 400	4 900	525	388	107 013
Percentage of total	18%	50%	27%	5%	0%	0%	100%
Total	**184 400**	**435 900**	**174 060**	**58 851**	**11 322**	**6 017**	**870 590**
Percentage of total	**21%**	**50%**	**20%**	**7%**	**1%**	**1%**	**100%**

Of the 870 590 registered enterprises in South Africa, 864 573 are SMMEs. These are the great majority of enterprises, but contribute less than half of the GDP. This is a clear indication that there are very many SMMEs, but that their economic contribution is much less than when compared to a large enterprise. Figure 1.1 provides a graphical representation of the enterprise distribution.

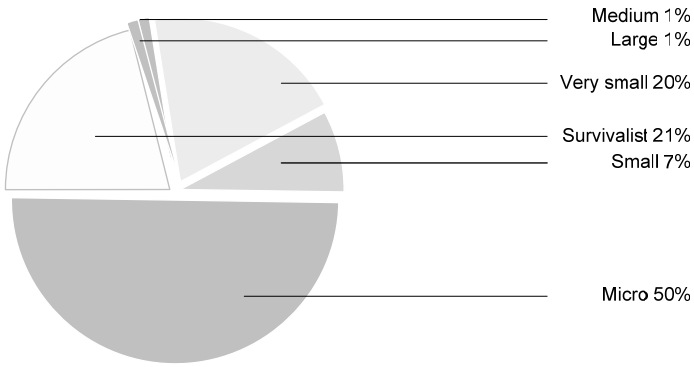


Figure 1.1: Distribution of enterprises

The following calculations reflect the approximated average contribution of 1 000 SMMEs to the GDP, when compared to large enterprises.

Table 1.2: SMME and large enterprise contribution to the national GDP

	Enterprises	Contribution to GDP	Contribution by 1 000
SMME	864 573	42%	0.05
Large	6 017	58%	9.64

Every 1 000 SMMEs of various sizes contribute an approximated 0.05% to the GDP, whereas 1 000 large enterprises contribute almost 10% to the GDP. Five large enterprises contribute approximately the same value (0.048) to the GDP as a thousand SMMEs.

SMMEs also suffer a high failure rate in the economy, especially the micro and very small enterprises. This failure is attributable to AIDS, crime and a lack of management know-how [DISP 2003]. The study discovered that 80% of SMMEs fail, with a large number of SMME owners lacking managerial qualifications. This indicates that entrepreneurs, although innovative, neglect good business practice. These entrepreneurs are also lax in implementing crime-prevention or reduction controls [DISP 2003].

The lack of good business practice and security indicates a lack of corporate governance. Corporate governance, as noted by the King II Report of 2002, should be applied to all public organisations and is not compulsory for SMMEs. Corporate governance, whilst establishing good business practice, also entices the business decision-maker to balance economic, environmental and social aspects of the enterprise [KING 2002]. This includes taking into

consideration financial regulations, social conditions of employed staff and the environment in which the organisation operates.

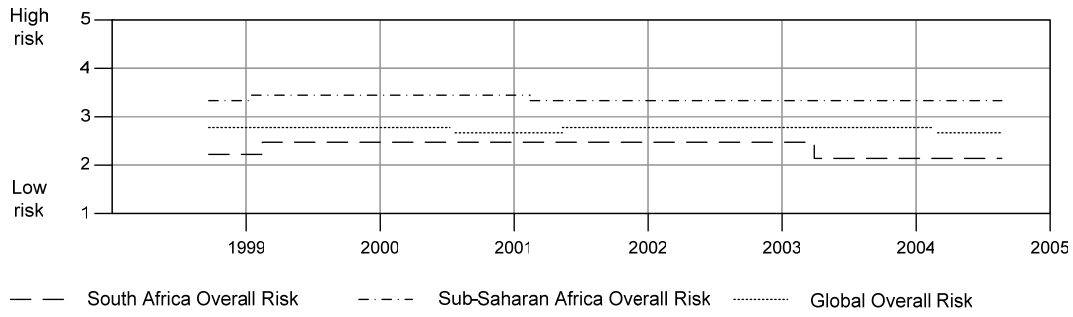


Figure 1.2: Comparative risk of South Africa [WORL 2004]

This environment in South Africa includes a high crime rate, so much so that it affects the overall risk rate for South Africa (refer to Figure 1.2) [WORL 2004].

The security risk rating for South Africa is set at 3.25, which is higher than the average for Sub-Saharan Africa, at 2.6. Global overall risk is lower still, at 2.2. Crime prevention and reaction is a serious consideration when securing an organisation.

A well-managed SMME, for conformance to good business practice, should consider governance to include securing of all company assets, which includes information assets. IT governance is a subset of corporate governance and, when applied with due diligence, will protect the information assets of the organisation [COBI01 2000]. Due diligence requires that the organisation follow a process of identifying the assets and any risks it may face from internal or external threats [COBI02 2000].

1.2 The Problem Statement

The problem, as identified above, is the lack of corporate governance, and as inclusive, IT governance in SMMEs in South Africa. SMMEs lack these as enablers to good business practice.

A further problem is the divide between the developed and developing countries. The developed countries have well-established standards and regulatory measures in place to analyse their governance efficiency, but these differ greatly from South African measures. It has to be determined whether developed countries' measures are usable in South Africa, and whether these

measures can be applied to the South African environment, considering its regulations already in place.

1.3 The Research Project Objectives

The objective of this study is to determine whether corporate governance standards can be applied to SMMEs, and whether they are usable in South Africa. The hypothesis is that the developed countries' methodologies for corporate governance are not suitable due to the unique nature of South African SMMEs. As a result, this study determines whether subsets, specifically the subset of IT governance standards in developed countries, conform to regulations and are applicable to the SMMEs.

IT governance is further drilled down to risk management. Risk management as applied in IT governance includes information security risk management (ISRM).

ISRM methodologies used by developed countries are also evaluated as enablers of IT governance, for conformance to regulations and applicability to the developing countries' SMMEs.

A requirement for a new methodology may arise if the hypotheses are proven.

In the eventuality of such a requirement, the methodology must be created and then tested for the conditions raised. These conditions of conformance and applicability are expanded into tangible scientific measures.

1.4 Structure of this Study

The structure of the study for the formulation of this dissertation is as follows:

1.4.1 Research Methodology

The design of this study is structured according to the following methods [OLIV 1999]:

- Primary method: Model

  The final outcome of the study is the creation of a qualitative model, in response to the hypotheses stated throughout the body of the study. This model is tested in a scientific theoretical environment and the results analysed and reported.

- Secondary method: Literature study, argument

  As noted, the formulation of the hypotheses and model requires a literature study, and as a result, arguments proving or disproving the hypotheses.

  The primary means of obtaining literature used was through published books, online academic libraries and journals. The arguments are based on the comparison of the literature, and in some cases assumptions made from the literature when analysed.

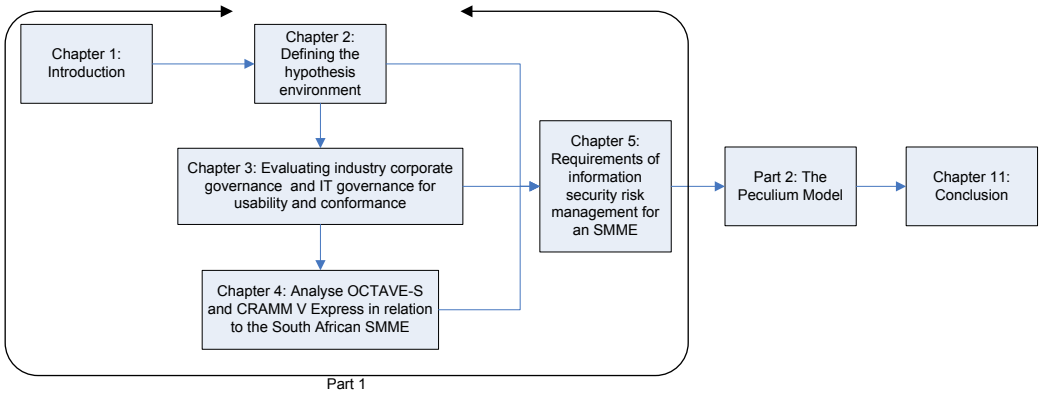


Figure 1.3: Logical flow of the structure

The structure of this study follows a logical flow of the definition of the environment and a literature review of governance and security standards (refer to Figure 1.3). The principles discovered in these standards and the environment are used to analyse existing ISRM approaches. The results of the analysis are used to compile the Peculium Model, an ISRM model for SMMEs, which is then tested in a theoretical, real-world based environment for usability.

1.4.2 Brief Description of the Chapters

Each chapter is succinctly summarised below. The descriptions provide further explanation of the structure presented in Figure 1.4.

Chapter 1 – Introduction

This chapter focuses on the purpose of the research and eventual creation of a methodology. The hypotheses are set and the objectives aligned that demonstrate the logical flow of the continuing document.

The chapter also provides a description of the research methodology and structure of the dissertation.

Chapter 2 – Defining the hypothesis environment

Chapter 2 defines the various aspects of the hypotheses that require further insight. It clarifies the hypothesis environment as well as the terminology used throughout the dissertation. This information sets the foundation for the following chapters.

Chapter 3 – Evaluating industry corporate governance and IT governance for usability and conformance

This chapter explores those standards and regulations that form the foundation of effective ISRM. Implementing ISRM without due diligence to these standards can nullify the efforts of ISRM. This chapter also determines how corporate governance and IT governance empower the ISRM process.

Chapter 4 – Information security risk management for small businesses

This is an extensive chapter analysing existing commercial ISRM methodologies for their advantages and disadvantages in the SMME market. The analysis also forms part of the hypothesis defined in Chapter 1. The methodologies are analysed for:

- Fit to the objectives of ISRM
- Suitability to the SMME market, considering cost, resource requirements, nature of implementation and usable components.

Chapter 5 – Requirements for information security risk management for an SMME

The framework created in Chapter 5 presents the minimum requirements of a methodology that conforms to the requirements as determined by corporate governance, IT governance, information security standards and the advantages of the methodologies analysed in Chapter 4. The chapter provides a framework as preparation for the methodology to be created.

Chapters 6 to 10 – The Peculium Model[2]

These chapters form the created methodology in response to the proven hypotheses. The components as well as the holistic approach of the methodology are presented and discussed in a systematic step-by-step procedural manner. A scenario test of the Model is presented in Appendix 5.

Chapter 11 – Conclusion

This chapter serves as a summary of the preceding chapters, reiterating the hypotheses and the proof thereof. It also concisely describes the Peculium Model.

1.5 Conclusion

This chapter has been used to articulate the problem statement, objectives for the dissertation and research model that is used.

The dissertation is based on the proof of hypotheses and, if done, the creation of a model in support of the hypotheses.

The first hypothesis that is attempted is as follows:

> South African SMMEs cannot be compared to other countries' descriptions of small organisations.

This hypothesis is proven in the following chapter. Chapter 2 offers an explanation of the environment in which this study is conducted, focusing on the difference between SMMEs in developing and developed countries. The chapter also includes definitions of the terminology used for the research environment as applied throughout the dissertation. ISRM is defined from a top-down association with corporate governance and IT governance.

[2] 'Peculium' taken from the Latin word for 'a bit of money'.

Part 1: The Hypotheses

2 Defining the Hypothesis Environment

2.1 Introduction

As with many fields of study and analysis, an awareness of the environment in which the analyst acts is of paramount importance. For example, a pathologist examining a blood sample for toxicity has to understand what represents toxicity in the blood. The same applies to a chemist analysing the reaction of chemicals. Ignorance of the properties of the chemicals may have hazardous consequences. The principle is also applicable in this case. Stating a hypothesis for an SMME environment without understanding what the environment is defeats the value of the findings and statements that result.

One also cannot, in good sense, analyse a field such as information security risk management without fully understanding what it is.

The objective of this chapter is thus the definition of the environment in which the research was conducted, based on the hypothesis defined in Chapter 1. Consequently, it is to define what the research is analysing. This objective consists of the following two goals:

The first goal of this chapter is the definition of the environment and all associated principles that should create a clear understanding of the environment of the hypothesis.

The second goal of the chapter is the definition of the broad discipline of risk management and ISRM as they apply to this study.

Before starting any journey, it is advantageous to have information of both the destination and the first steps. This chapter begins with a comparison of the small enterprises in developed and developing countries.

Upon establishment of the hypothesis environment, the definition of ISRM and all the associated terminology in the field is presented.

The resulting outcome sets the environment for the literature study that follows hereafter.

2.2 Comparison of the Small Enterprise in Developing and Developed Countries

A distinction is made in many levels of society between the “have’s” and “have-nots”. The same applies to countries. There are civilisations that have developed faster and more effectively than others, with efficient infrastructure, low unemployment figures and matured educational systems.

There are countries at the other end of the scale that have not enjoyed such development. These countries have diminished governmental structures, poor economies and lack of infrastructure. Many symptoms can be blamed for this; in most cases it is due to civil warfare, lack of natural resources and fast-developing populations.

There are, however, also countries that cannot distinctly be defined as either. South Africa is such a case. Colonial influence in the 18th and 19th centuries provided South Africa with strong infrastructures, a well-developed educational system and a firm commercial structure [AFRI 2005]. Another facet of history, apartheid specifically, removed the majority of the population from such development. This led to widespread poverty, illiteracy and unemployment [EDUC 2005].

Many parties have debated the question of whether South Africa is a developed or developing country.

The international authority on the definition of developed and developing countries, the International Monetary Fund (IMF), has declared South Africa as a developing country due to the high unemployment and inflation rates and the high level of international debt [IMF 2004].

The American Central Intelligence Agency recognises South Africa as a developed country, based on the high degree of industrialisation [CIA 2004]. South Africa is the only African country listed as developed by the Agency, whereas no African countries are listed as developed by the IMF.

South Africa therefore must be recognised as one of the leading developing countries. The criteria for a developed country do seem apparent in certain

areas of South Africa, but the lack of infrastructure, employment and economic sustainability in the large populous areas of the South African townships has created the focus for development. Development in these areas is highly focused on the construction of housing, roads and schools [JOBU 2005] [ALEX 2005]. This is a clear indication that South Africa, although noted as a developing country, is definitely assigning resources to development, and is firmly en route to having a developed nature.

2.2.1 Economic Data on Developed and Developing Countries

Some of the criteria listed in the previous section for declaring a country as developed include industrialisation, stable inflation, low unemployment figures and firm commercial structures. South Africa has been declared as a leading developing country by the IMF. Such a country must be compared to developed nations to find those areas that are still lacking in stability or maturity.

The governmental and legal systems in South Africa, influenced by British colonial rule, are well established, but, in hindsight, are systems built from the foundations of a world leader onto the unstable soil of a developing country. Many of the still developing countries were once ruled by the great maritime rulers of old, such as England, Spain and Portugal [AFRI 2005].

To accurately evaluate the applicability of ruling systems created by developing countries to developed countries, some data is required to define the distinction between the two divides.

Below follows the comparison of economic data of developed countries and developing countries. Samples have been selected to represent the groups from the IMF List of Advanced Economies and its exclusions.

2.2.1.1 Developed Countries

The following countries have been selected to represent developed countries in a sample for this study:

- United States of America
- United Kingdom
- Australia

These countries have well-developed economies and low poverty rates, and are considered by most to be representative of effective coherence to criteria for a developed country. The economic data follows hereafter [WORL 2004].

Table 2.1: Economic data of the developed countries sample [WORL 2004]

	Developed Countries		
Data as at 2003	**United Kingdom**	**United States**	**Australia**
GDP growth %	2.00	2.90	2.97
Inflation %	3.00	2.27	2.77
Population (m)	59.30	288.00	19.90
Unemployment (m)	5.00	6.08	6.30
Economic risk	1.50	1.50	1.25

The developed countries have an inflation rate of or below 3%, with varying populations. The countries also have negligible economic risk, due to their well-established economic practices and lack of warfare within their borders. The following graphical representation demonstrates the inflation and GDP growth over the last six years:

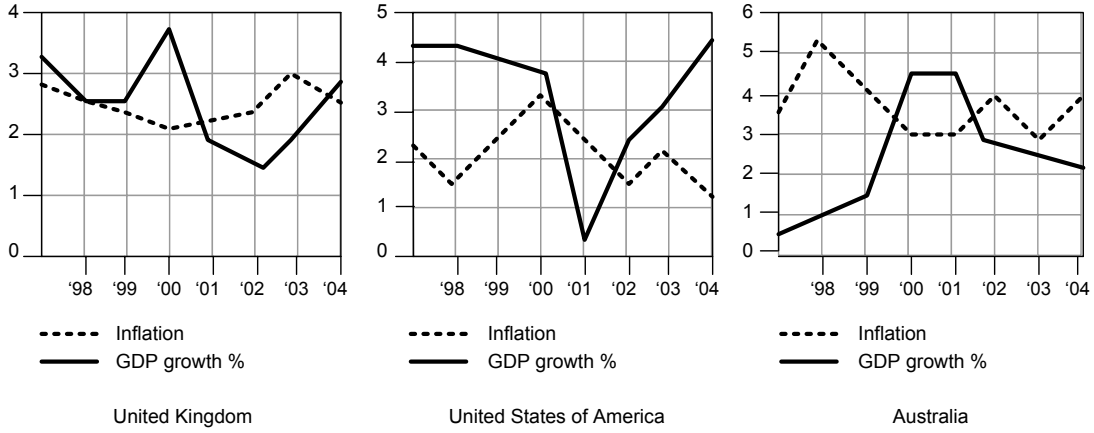


Figure 2.1: Inflation and GDP growth of the developed countries sample [WORL 2004]

The United Kingdom has shown the most stability over the period, with both inflation and GDP below 3% for the last three years. The USA, on the other hand, suffered a significant drop in GDP in 2001. This can be attributed to the lack of consumer confidence after the 9/11 attacks on the Pentagon and

World Trade Center Towers [WORL 2004]. Inflation did, however, maintain its downward trend. The GDP has maintained a steady increase.

Australia has experienced a decreasing inflation from an already low 3% since 2002. The GDP has been fluctuating between a healthy 3 and 4% over three years.

From this information it can be concluded that the well-established systems in place in these countries are managing economic growth effectively, especially in the case of the United States. A disaster shocked the nation into great fear and a war on terror. The economy did recover at a significant pace to establish the high level experienced previously. This is also an indication of effective governmental and commercial rule.

2.2.1.2 Developing Countries

The sample selected to represent developing countries is based on countries that have experienced colonial rule, been subject to economic crises or suffer diminished governmental, educational or infrastructural systems. The representative sample provides a collection of differing cultures, continents and current economic growth.

It has been decided that the sample for developing countries should not portray similar economic data, but should reflect the differing motivation for the 'developing' label assigned to these countries. The sample of developing countries is:

- South Africa
- Botswana
- Argentina

Table 2.2: Economic data of the developing countries sample [WORL 2004]

	Developing Countries		
Data as at 2003	**South Africa**	**Botswana**	**Argentina**
GDP growth %	1.85	5.00	8.41
Inflation %	5.86	8.36	13.44
Population (m)	45.30	1.72	38.40
Unemployment (m)	28.00	..	21.10
Economic risk	2.25	1.75	3.50

The developing countries have unstable inflation rates above those of the developed countries, with varying populations. South Africa and Argentina have moderate to high economic risk due to crime rates and economic instability, respectively. Botswana's economic risk is negligible. The following graphical representation presents the inflation and GDP growth over six years:

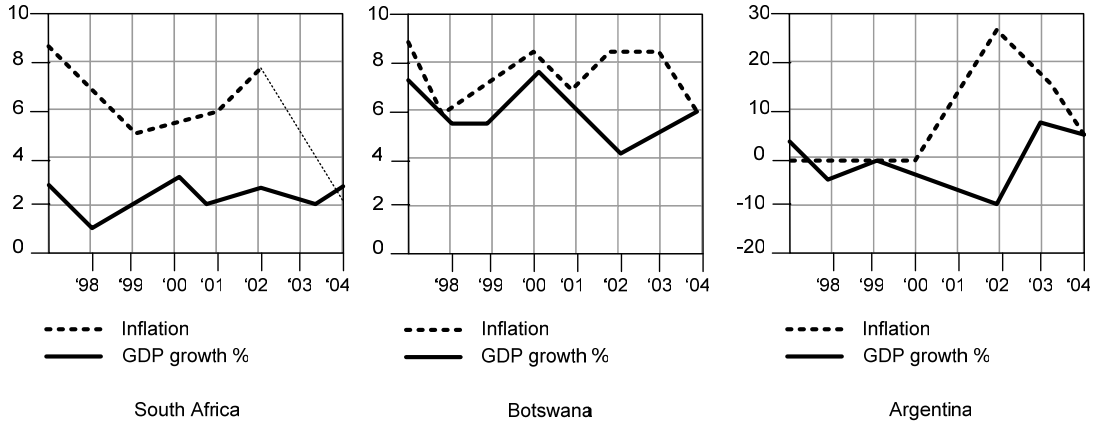


Figure 2.2: Inflation and GDP growth of the developing countries sample [WORL 2004]

South Africa has maintained a stable range of GDP figures over the last three years. Inflation has improved tremendously, dropping from 8% in 2002 to under 3% in 2004. Botswana's inflation has been fluctuating within a high range of 6 to 8%. The GDP has enjoyed consistent growth for the last two years.

Argentina is a high-risk economy, as represented in this graph. The inflation rate has reached levels of 25%, dropping back down to approximately 8% in 2004. This is an indication of volatility, confirmed by the GDP figures growing from a negative figure in 2002 to 8% in 2004.

It is clear from this data that the sample of developing countries reflects instability in various economic measures. None of the three countries have enjoyed stable inflation and GDP growth over the last two to three years, as apparent in developed countries.

This also confirms that they cannot as yet be labelled as developed countries, and are correctly grouped in the developing countries category.

The value of this data to this study becomes apparent in the following section, where the definitions of small, medium and micro enterprises (SMMEs)[3] in the two samples are compared. The differing definitions of SMMEs between developed and developing countries also reflect the economic contribution by SMMEs as being different in the two categories.

2.2.2 The Small Enterprises in the Sample of Developed Countries

The data contained in this section is split first into the categories of developed and developing countries, and thereafter into each country in the samples. The information provides the two measures currently used in the definition of SMMEs, that being employee size and annual turnover. Some countries do, however, rely on either of the two measures.

This data determines whether the definitions of SMMEs in developing countries also differ as the economic data has been proven to differ.

2.2.2.1 United Kingdom

Small enterprises in the United Kingdom fall under legislation of the European Union (EU), and are thus defined according to the EU definition of their SMEs, or small, medium and micro enterprises [COMM 2003]. The shortened acronym includes medium and micro enterprises. The EU defines an SME as follows[4]:

Table 2.3: SMEs in the United Kingdom [COMM 2003]

Enterprise Size	Number of Employees	Annual Turnover	Rand/Euro Exchange at R8,14[5]
Medium enterprise	Fewer than 250	Less than EUR 50m	R407m
Small enterprise	Fewer than 50	Less than EUR 10m	R81.4m
Micro enterprise	Fewer than 10	Less than EUR 2m	R16.2m

[3] SMMEs will be used as the collective descriptive word for the remainder of this chapter. Some countries do, however, define these collections differently, which will be stipulated.
[4] As defined by the EU Commission held on the 6th of May 2003 concerning the definition of micro, small and medium-sized enterprises [COMM 2003].
[5] Exchange rates as at October 2005.

2.2.2.2 United States of America

The Small Business Administration[6], an organisation in the US specialising in offering small businesses financial and strategic assistance, is the national authority on the definition of a small business [SBA 2005].

The American small business definition is very extensive in considering all industries, which are narrowly defined. The definition is structured to represent some 300 industries, not listed here, that either list the annual turnover in million, or number of employees. The American small business is defined as presented in Table 2.4.

Table 2.4: Small business in the United States of America [SBA 2005]

Enterprise Size	Number of Employees	Annual Turnover	Rand/Dollar Exchange at R6,55
Small enterprise	500 to 1 500	$750 000 to $25m	R4.9m to R164m

2.2.2.3 Australia

The Australian Bureau of Statistics defines the Australian SMEs as presented in Table 2.5. Australia does not measure its SMEs in turnover figures, but relies solely on the organisation sizes [KIRI 1999]. As such Table 2.5 only presents the number of employees in the enterprise definitions.

Table 2.5: SMEs in Australia [KIRI 1999]

Enterprise Size	Number of Employees
Medium enterprise	Fewer than 200
Small enterprise	Fewer than 20
Micro enterprise	Fewer than 5

An assumption is made that the annual turnover of Australian SMEs, as a member of the developed country sample, also experiences turnover into multiple millions.

[6] Established as a non-profit organisation in the service of the state. It makes use of a "Table of Small Business Size Standards" based on the North American Industry Classification System (NAICS) industries [SBA 2005].

It can thus be concluded that SMMEs in the developed world are successful in their revenue generation. Parallel information is required of developing countries to compare whether there is a notable difference in the data.

2.2.3 The Small Enterprises in the Sample of Developing Countries

The sample identified previously is used again to represent the developing countries. The definitions of SMMEs are again based on number of employees and annual turnover.

2.2.3.1 South Africa

The South African SMMEs have become key players in the economy of this developing country. The promulgation of the Small Business Development Act in 1996 recognised the need for official recognition of these enterprises by the state, and the accompanying formalising of their significant role in the developing nation [GOV 2004].

The initial use of the European Union's structure allowed the state to use a definition that would be easily applicable in the industry. This definition has since been adapted to more realistic measures in the National Small Business Amendment Act of 2003 [GOV 2004]. A summary of the definition in the Amendment Act is as follows:

Table 2.6: SMMEs in South Africa [GOV 2004]

Enterprise Size	Number of Employees	Annual Turnover
Medium	More than 50 and fewer than 200, excluding agriculture which allows only up to 100	Ranging from R13m to R64m across various industries
Small	Fewer than 50 employees	Ranging from R3m to R32m across various industries
Very small	More than 5 and fewer than 20 employees	Ranging from R500 000 to R5m across various industries
Micro	Up to 5 employees	R200 000 across all industries

The South African definition includes a measure for very small enterprises, although they are not included in the acronym. This is due to the large number

of enterprises with the number of employees ranging between 5 and 50 (refer to Chapter 1, Table 1.1). This grouping is included in the small enterprise grouping for the purposes of this study.

2.2.3.2 Botswana

Botswana, the current economic star of Africa, is experiencing a 30% to 40% contribution to its GDP by SMMEs, employing 190 000 people, just over 9% of the population [DAIL 2004]. The Botswana SMME is defined below [LECH 2004].

Table 2.7: SMMEs in Botswana [LECH 2004]

Enterprise Size	Number of Employees	Annual Turnover	Rand/Pula Exchange at R0,73
Micro enterprise	Up to 2	Up to P60 000	R44 000
Small enterprise	Up to 25	P60 000 to P1.5m	R44 000 to R11m
Medium enterprise	Up to 100	P1.5m to P5m	R11m to R37m

2.2.3.3 Argentina

The Argentinean system of defining SMEs, in contrast to their other South American counterparts, is based upon annual sales [FUND 2004]. A study has, however, been conducted in which world SME definitions are compared. This study suggests that Argentinean SMEs have up to 250 employees [AYYA 2003]. The SME is defined in Table 2.8.

Table 2.8: SMEs in Argentina [FUND 2004] [AYYA 2003]

Enterprise Size	Number of Employees	Annual Turnover	Rand/Peso Exchange at R0,39
Micro enterprise	..	Up to 500 000 pesos	R195 000
Small enterprise	..	Up to 3m pesos	R1.2m
Medium enterprise	Up to 250	Up to 24m pesos	R9.4m

It is clear from Argentina's data that the SMMEs are not economically as successful as those in Botswana, and also offer less individual income by a greater number of employees. This again reflects the economic turmoil noted in the economic data presented earlier.

2.2.4 Small Enterprises in Developed versus Developing Countries

The information provided throughout this chapter has drafted a map of SMMEs spanning five continents across the globe. The countries evaluated differ in geographical size, cultures, economic risk and many other factors. There is, however, one factor which remains the same. All of these countries recognise SMMEs as contributors to their respective economies.

None of the countries define an SMME as an exact copy of that of another country. The various countries use different measures and different currencies when defining these enterprises. Table 2.9 below summarises the information in this section.

Table 2.9: Comparison of economic data

	Developing Countries			**Developed Countries**		
Data as at 2003	**SA**	**BOT**	**ARG**	**UK**	**USA**	**AUS**
GDP growth %	1.85	5.00	4.10	2.00	2.90	2.97
Inflation %	5.86	8.36	6.59	3.00	2.27	2.77
Population (m)	45.30	1.72	38.40	59.30	288.00	19.90
SMME employees	< 50	< 25	< 250	< 50	> 500	< 20

The definition of a small enterprise across the two samples and six countries differs tremendously. For example, Australia and the USA are evenly matched in GDP growth, but have a significant difference in population and small enterprise size.

South Africa and the UK also share similar definitions for number of employees, but differ greatly in economic strength.

It thus follows that the South African SMME is unique when compared to that of any of the other sample countries selected here. The hypothesis thus stands, that corporate governance of an SMME in one of these countries

cannot be directly applied to the South African SMME without some customisation.

A subset of corporate governance, IT governance, can be construed not to directly apply to South African SMMEs either. This is, however, a bold and as yet unproven statement. A further hypothesis is thus stated, that IT governance as created for other countries' SMMEs is not absolutely suited to South African SMMEs either.

Thus having defined the environment in which this study is focused and the accompanying hypothesis, additional preparation is required before proving this second hypothesis.

Proving a hypothesis on the unsuitability of corporate governance, or IT governance, requires once again an understanding of the environment. The following definitions apply to this study as a guide to understanding corporate and IT governance.

2.3 Defining Corporate and IT Governance

Corporate governance is fast becoming a much more important consideration in both developed and developing countries [WORD 2004]. Countries with a well-established and applied corporate governance standard have a more secure presence in the global economy.

2.3.1 Corporate Governance

Corporate governance refers to the manner in which a corporation is directed, and laws and customs affecting that direction. It includes the laws governing the formation of firms, the bylaws established by the firm itself and the structure of the firm. The corporate governance structure specifies the relations and the distribution of rights and responsibilities, among primarily three groups of participants – the board of directors, managers and shareholders. This system spells out the rules and procedures for making decisions on corporate affairs; it also provides the structure through which the company objectives are set, as well as the means of attaining and monitoring the performance of those objectives. The fundamental concern of corporate governance is to ensure the conditions under which a firm's directors and managers act in the interests of the firm and its shareholders, and to ensure

the means by which managers are held accountable to capital providers for the use of assets [CLIF 2004].

This lengthy definition can be interpreted as stating that corporate governance creates a framework by which an organisation is managed. It provides guidelines on responsibilities held by directors, shareholders and managers. The decisions made by these parties should be made with due consideration of the organisation in its entirety, including its assets, business interests and staff.

This interpretation is supported by the World Bank Report on Corporate Governance in 1999, in which Sir Adrian Cadbury stated that:

“Corporate Governance is concerned with holding the balance between economic and social goals and between individual and commercial goals…the aim is to align as nearly as possible the interests of individuals, corporations and society.” [KING 2002]

The King II Report also recognises the alignment of corporate governance with factors outside financial governance such as the “fundamental practices of good financial, social, ethical and environmental practice” as reflected in the diagram in Figure 2.3.

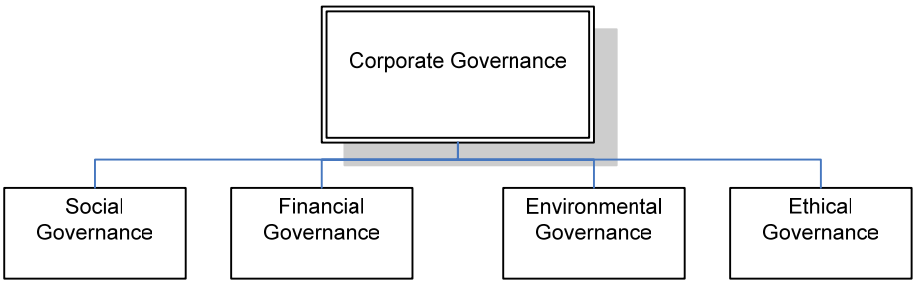


Figure 2.3: Corporate governance practices as noted in King II

Corporate governance is the structure for an organisation to monitor its decision-making and to act upon its objectives and strategies. An organisation comes to understand through good corporate governance that its strategies and objectives will hold an inherent risk. The management of such inherent risk, i.e. risk management, becomes a major practice in corporate governance. The protection of information assets and continuous usability of the information systems that enable achieving organisational goals become important considerations.

IT governance provides the structure that links IT processes, resources and information to organisational strategies and objectives.

2.3.2 IT Governance

IT governance is defined as a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes [COBI01 2000].

IT governance applies risk management, or specifically information security risk management (refer to Figure 2.4).

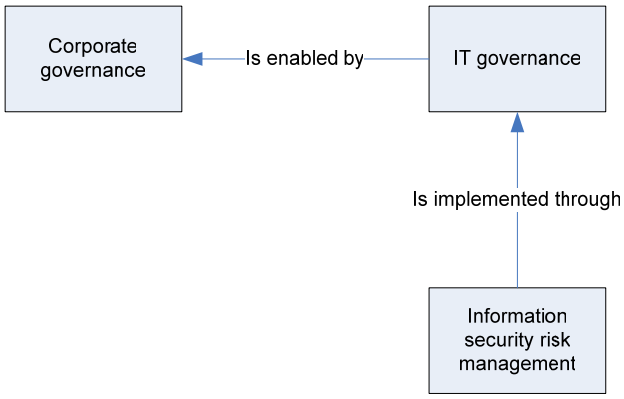


Figure 2.4: The relationship between corporate and IT governance

ISRM is a complex structure of processes and procedures that secures an organisation's IT and information assets against those risks faced when an organisation applies strategies to reach its objectives. These risks are not restricted to strategic objectives, but are in effect present in daily operations.

Corporate governance, a regulated and applied discipline, is defined according the standardised measures. The same applies to IT governance. ISRM is yet to be defined. Lack of such a definition reverses the importance of IT governance, and as a result corporate governance to this study.

The next section defines information security risk management and the various facets involved in the discipline.

2.4 Defining Information Security Risk Management

ISRM is a particular extension of risk management. Risk management is applicable to various facets of an organisation, such as operational risk management, market risk management and financial risk management. Four

major components of risk management have been identified in the literature [BAND 1999]:

1. Risk identification
2. Risk analysis
3. Risk-reducing (mitigating) measures
4. Risk monitoring

These four components are complex centres within their own disciplines. Definition of each of these components is required as each component, although stemming from its previous partner, has its own functionality, success criteria and objectives. The one factor that binds all these components is the generic, yet focus enabling concept of risk. Risk management is thus defined, firstly by evaluating risk, and then broaching each component in the order noted in the bottom-up view of Figure 2.5 below [COBI01 2000].

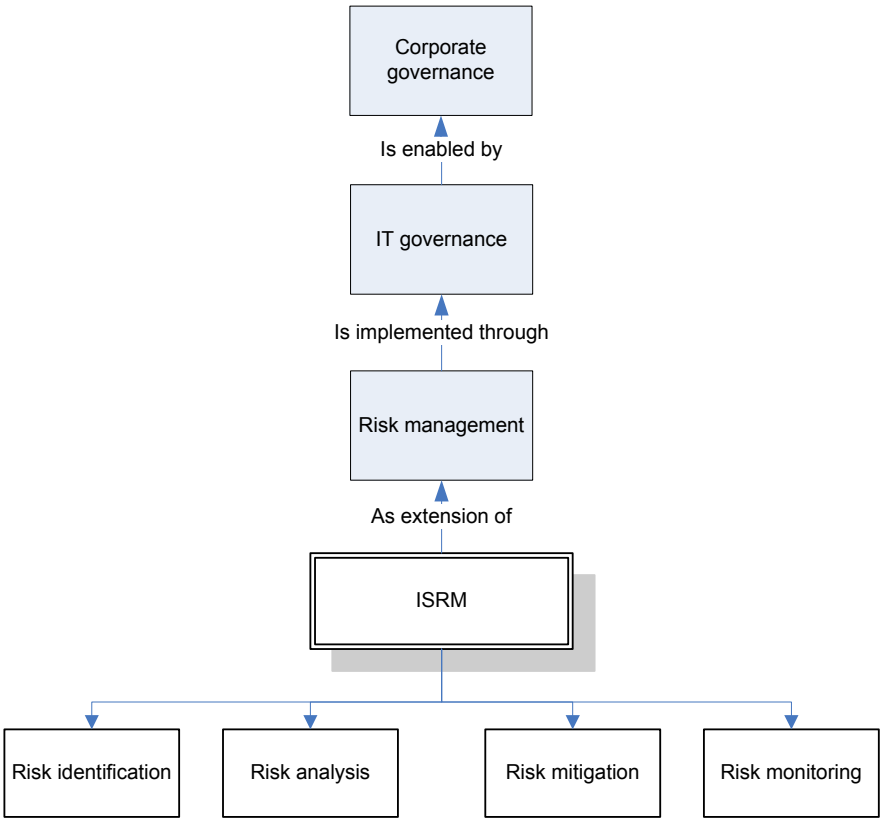


Figure 2.5: Fit of risk management into corporate governance and its components

2.4.1 Risk

This chapter has been structured to create an understanding of the environment in which this study is focused. It is fitting that care be taken when defining risk. Risk, as noted above, is present in every facet of daily life. As such, various definitions for risk exist and are used for many different purposes. These definitions are not, however, similar as would be expected.

a. Risk is the quantifiable likelihood of loss or less-than-expected returns [INVE 2004].

This definition suggests that risk is an uncertainty, but a measurable one. This implies that some analysis would be involved either in measuring the uncertainty or, as stated next, the uncertain loss. This loss could be represented as monetary, asset-related or otherwise. The definition also refers to returns. This represents risk in an investment of some variety. This definition appears to be directed at monetary risk.

The definition holds a contrast in perceived impact, as it states a “likelihood of loss” which provides a negative connotation, and then states “less-than-expected returns” which presents a comparatively positive connotation.

b. Risk is the possibility of suffering harm or loss [OCTA01 2003].

This definition differs greatly from the first, but also shows similarity. It is more negatively representative of the facets of risk. It humanises risk and creates an emotional link to the result of a risk that is realised, in stating the possibility of “suffering harm or loss”. There is no indication of measurement of the risk. It does not link the result of the harm or loss to an asset. This definition is applicable to any risk, in business or private capacity.

c. Risk is a factor, thing, element or cause involving uncertain danger [AMER 2004].

This definition is perceived to create a broad scope of applicability, as risk may have any source. It also presents an uncertainty of the level of danger ‘involved’. The definition carries a definitive negative connotation, but does not declare any certainties.

It is clear that although definitions of risk abound, they are either too non-specific or too focused on an area not applicable to this study. For the purposes of this dissertation, the following definition of risk is used:

Risk is the measured probability of decreased value of an asset or investment as a result of an exposed vulnerability.

2.4.2 Risk Identification

Risk identification, as noted in Figure 2.5, is the first component of the generic risk management model. Risk identification is a necessary component. As stated earlier, some organisations choose to apply selected components, but risk identification is unavoidable. Risks cannot be managed if they are not first identified. There is, however, some confusion as to what risk identification entails. The following definitions illustrate this uncertainty.

a. The method of identifying and classifying risk [MCNA 1999].

This definition suggests a logical and simple process of identification and classification of risks. It states that risk identification is the method of identifying risks, which is nonsensical. It does not provide any information on what the method entails. It also provides no indication of what classification is used.

b. Recognizing that a risk exists and trying to define its characteristics. Risk identification is a deliberate procedure to review, … anticipate possible risks [SOCI 2004].

This definition clearly states that risk identification is a procedure used to gather information on risks, including their characteristics, used to anticipate realisation of the risks. It does not provide guidance on which characteristics are reviewed.

Neither definitions provide a clear map to identify these risks, nor what preparatory processes may be required. The definitions do touch on classification and a procedure, respectively. The risk identification definition that is more suited to this study is thus created as a modified collective representation of the definitions evaluated above. Risk identification is defined as follows:

Risk identification is the process of identifying assets, the vulnerabilities of those assets and any threats facing those assets.

Figure 2.6 illustrates this collective representation.

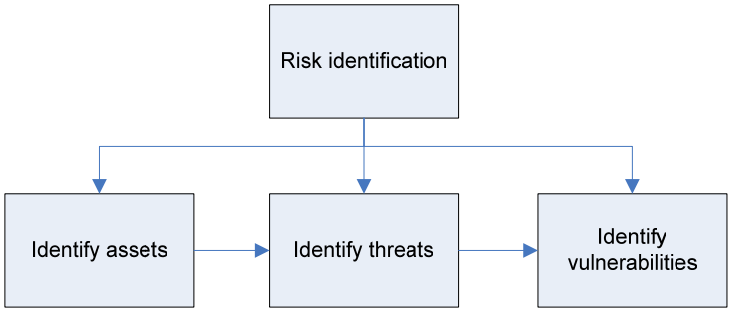


Figure 2.6: Risk identification

The terms ‘assets’, ‘vulnerabilities’ and ‘threats’ are additions to the collective definition. These are defined as follows:

2.4.2.1 Assets

In security, a resource or information that is to be protected [ATIS 2004].

Any item of economic value owned by an individual or corporation, especially that which could be converted to cash [BURE 2004].

2.4.2.2 Vulnerabilities

A weakness in an information system, system security procedures, internal controls or implementation that could be exploited [ATIS 2004].

The degree to which a system is susceptible to, and unable to cope with, injury, damage or harm [EURO 2004].

2.4.2.3 Threats

Capabilities, intentions and attack methods of adversaries to exploit; or any circumstance or event with the potential to cause harm [ATIS 2004].

Something that is a source of danger [WORD 2004].

These definitions suffice for the purposes of this dissertation as the connotations are clear and offer no confusion.

2.4.3 Risk Assessment or Analysis

The next component of risk management is risk analysis. This is a component that causes much confusion, and at times a stalemate in a poorly informed risk management exercise. The risks that the organisation faces

have been identified. The organisation may be faced with insecurity regarding the process going forward. The next component requires a clear route for the risk management executor to take. The terms ‘analysis’ and ‘assessment’ are easily interchangeable.

2.4.3.1 Risk Assessment

a. Risk assessment is measuring two quantities of the risk, the magnitude of potential loss, and the probability that the loss will occur [INVE 2004].

The definition asserts itself as a tool of measurement by considering probability and loss. The information obtained of such an assessment should empower a better decision with regard to control versus asset value.

b. Formal and systematic *analysis* to identify and quantify probabilities and consequences [BURE 2004].

This definition uses the word ‘analysis’ as an explanation of assessment. It also measures probability and loss.

c. Risk assessment is the process of analysing threats to and vulnerabilities of *[assets]* and the potential impact of the loss *[of the asset]*. The resulting analysis is used as a basis for identifying appropriate and cost effective countermeasures [ATIS 2004].

This definition suggests that analysis is a subset of assessment. This analysis implies the gathering of information on risks. This information is then analysed for impact and probability. This creates a more structured view of the measurement step in risk management.

2.4.3.2 Risk Analysis

a. A systematic method of identifying the assets, the threats to those assets, and the vulnerabilities to those threats [ATIS 2004].

This definition, although explanatory, excludes factors mentioned above. It does not measure the impact of the threats realised (exposure) or the probability of exposure. The process explained analyses the assets more than the risk (quantifiable probability of decreased value of an asset or investment) to the asset.

The definitions create confusion. The terms ‘analysis’ and ‘assessment’ are thus defined as follows:

- Risk analysis is the scientific measurement of the threat to an asset, the associated probability of the vulnerability being exploited and the associated impact of the exposure.
- Risk assessment is the judgement made when considering the analysis result. This judgement is used when prioritising mitigating controls.

For this study, risk analysis is used as a subset of risk assessment (refer to Figure 2.7), as the ultimate goal of the step of measurement in the risk management process is to be prepared to control the risk.

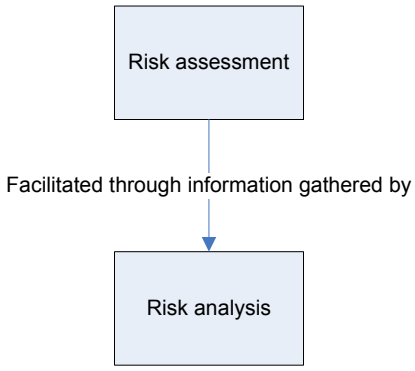


Figure 2.7: Risk analysis as a subset of risk assessment

The term ‘exposure’ has been used in defining risk analysis. Exposure as an individual factor is defined as follows:

2.4.3.3 Exposure

The condition of being subjected to a source of risk [WORD 2004].

The potential compromise associated with an attack exploiting a corresponding vulnerability [ATIS 2004].

These definitions suffice for the purposes of this dissertation as the meaning is clear and easily understood.

2.4.4 Risk Mitigation

Risk mitigation, the third component of risk management, provides the device for reaction to the identified risk. This reaction may be focused on reducing, transferring, terminating or accepting the risk. This component poses great difficulty in application if the step of risk assessment has not been performed.

An organisation may face great difficulty in justifying the expenditure on mitigating measures if no motivational documentation is available, documentation that the risk assessment would have provided. This could potentially offer another stalemate if an organisation has exploited resources for risk identification, but cannot justify assigning more resources to mitigation. Risk mitigation is, however, the crux of the exercise, as awareness of risks alone does not reduce the impact they may have. Risk mitigation is defined as follows:

a. Risk mitigation seeks to reduce the probability and/or impact of a risk to below an acceptable threshold [PMBO 2004].

This definition demonstrates the purpose of risk mitigation being the reduction of the probability of a risk occurring, or impact of the risk if it does occur, to an acceptable level. It does not provide any indication of a procedural process, or how this mitigation is facilitated.

b. Risk mitigation is the steps you take to reduce your security risk to an acceptable level [ATIS 2004].

This definition reflects that risk mitigation is not a single action, but a series of steps taken to reduce risk. It does not give an indication of what these steps are.

These definitions do not provide a clear understanding of the scope of risk mitigation, when considering the amount of input required in the previous two components of risk management. They provide no mention of how mitigation is executed, or which courses of action are recommended to the risk manager. The definition given below applies more effectively to this study, by providing all information required to attempt successful risk mitigation.

Risk mitigation is the implementation of a strategy that either:

- Implements controls that reduce the probability and impact of those risks identified by assessment as the most probable and with the highest impact, or
- Transfers the risk to a third party, or
- Terminates the risk by removing the asset from the environment, or accepting the risks and associated impacts.

A combination of strategies may be implemented for a risk in a very complex situation.

2.4.5 Risk Monitoring

Risk monitoring, the final component of the ongoing process of risk management, is not a result of risk mitigation, but in fact a continuous revolving component that monitors the previous componential results for change. Risk monitoring is formally defined as follows:

a. Process of following up the decisions and actions within risk management in order to ascertain that risk containment or reduction with respect to a particular risk is assured [WORD 2004].

This definition clearly states that decisions and actions during the risk management process to date are monitored and evaluated to ensure that the risks identified are controlled. It does not provide any indication of what actions are taken if the containment of risk is not assured. This definition provides no contingency.

b. Risk monitoring is the ongoing risk management task of monitoring the success and status of the other risk management tasks [FIRE 2004].

This definition, although vague, does plainly state that monitoring is ongoing and that it involves monitoring of all other risk management tasks. These tasks are noted as identification, assessment and mitigation. It does not provide any information as to how this monitoring should occur.

A clearer formal definition is required to continue the componential definitions created thus far.

Risk monitoring is the regulated and ongoing process of evaluating those risks identified, assessed and mitigated for changing characteristics and changing the control of those risks accordingly.

At this stage, it becomes necessary to redefine risk management by combining the definitions of the four components as discussed above.

Risk management, when considering the elements across the various components, can be represented as follows (refer to Figure 2.8):

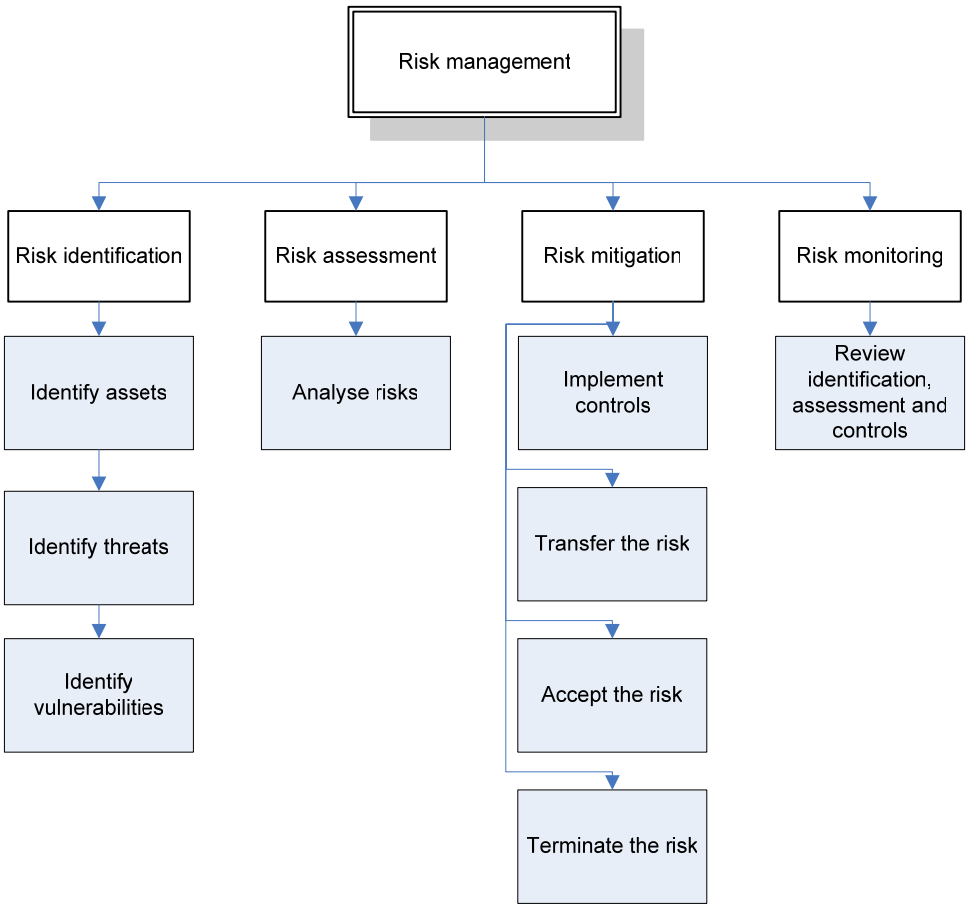


Figure 2.8: Risk management

Risk management, for the purposes of this study, is a collective of the components defined in this chapter and is thus formally defined as follows:

Risk management is the ongoing componential process of risk identification, assessment of the risk identified, mitigation of those risks and monitoring of these components for change.

This definition represents the high-level description of risk management, and should be accompanied by the definitions of the components. The definition from the literature given earlier in this chapter does not denote this fluid structure, or expansion of the components. This definition is thus a much-improved panorama of the environment in which this dissertation is focused.

Risk management is still defined too broadly for this dissertation and, as mentioned previously, needs further drilldown into the particular extension of ISRM.

2.5 Specialising in Information Security Risk Management

A clear understanding of risk management and its components has been reached. This study focuses on information security risk management. This new terminology requires formal definition as suited to this study. It is broken down into individual terms, and then once again collectively defined.

The individual terms that make up information security risk management are defined below.

2.5.1 Security

Security, in general terms, can be defined as follows:

a. Freedom from risk or danger [DICT 2004].

This is a very simple and exact definition. It also includes the word ‘risk’, which serves the purpose of this study.

b. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences [ATIS 2004].

This definition is very comprehensive in that it takes into consideration not only the state of being secure, but those measures that enforce security, as well as, very importantly, the maintenance of those measures.

c. The condition or quality of being secure [WEBS 2004].

This definition is more suited as a definition of the result of applying protective measures, which logically, is security.

These definitions all contain properties suited to this study, but none contain all the properties collectively. A new definition is created that does represent all properties required.

Security is the condition of negligible vulnerability due to the implementation of protective measures.

2.5.2 Information Security

Information security, concerning security as listed above, is a subset. Though applicable to any environment, it does not ensure general security. Information security is formally defined below.

a. The protection of information against unauthorised disclosure, transfer, modification or destruction whether incidental or intentional [GLOS 2004].

This definition is a holistic description of information security, and includes the reference to intentional or unintentional harm. This is important, as securing information should include accidental happenstance that may occur. The definition does not include descriptions of the harm centres.

b. Information security is protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide:

    I. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

    II. Confidentiality, which means preserving authorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information

    III. Availability, which means ensuring timely and reliable access to and use of information [NIST 2002]

This definition is very thorough in expanding on (a). It expands on the threats listed in (a), but also includes reference to information and information systems, which is vital. It does not, however, refer to intentional or unintentional attacks. A collective definition is once again required that reflects all the important elements highlighted above. The following definition applies for the purposes of this study:

Information security is protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction, whether intentional or unintentional, in order to provide:

    I. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

II. Confidentiality, which means preserving authorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information

III. Availability, which means ensuring timely and reliable access to and use of information

This dissertation focuses on information security risk management. Taking into consideration the formal definitions created for risk management, information security and all the components of each creates the requirement for the definition of the holistic information security risk management.

2.5.3 The Definition of ISRM

This definition faces a great challenge. It represents the discipline in which this study evaluates the conformance and usability of developed countries' methodologies for IT governance, as a result of corporate governance in South African SMMEs. It carries great weight through the remainder of this study, and should be carefully considered as the benchmark for evaluating hypotheses going forward. ISRM is thus defined as follows:

Information security risk management is the ongoing componential process of identifying information security risks, assessing the information security risks identified, mitigating those information security risks and monitoring these components for change.

ISRM thus defined is close to the definition of risk management (refer to Figure 2.8), but with the clear distinction of the primary focus on information security risks, and not generalised organisational risk. It should, however, be considered that these information security risks possibly pose great threats to strategic objectives, and should always be held in high regard.

2.6 Conclusion

The environment in which this study is conducted has been investigated and defined. This environment has been identified as the unique South African SMME.

The South African SMME is defined as having no more than 200 employees, generating a turnover up to R64m. The SMME applies across all industries, and is defined in the National Small Business Amendment Act of 2003.

The hypothesis proven in this chapter is this uniqueness of the South African SMME, and this hypothesis was expanded to include a second hypothesis.

This second hypothesis states that due to the uniqueness of South African SMMEs, corporate governance and IT governance principles as applicable to international SMMEs are not applicable to South African SMMEs.

The environment for this study is defined in the second section of the chapter. This study, based on the second hypothesis concerning IT governance, investigates ISRM as its chief implementer. This discipline has been defined as suitable for this study, and is investigated for applicability and usability to South African SMMEs in the coming chapters.

The objective of defining the environment of South African SMMEs and an analysis environment of ISRM has thus been achieved.

The subsequent two goals of defining what makes South African SMMEs unique compared to those of the developed and developing countries have also been reached, as well as the definition of the components of and relating to ISRM.

Chapter 3 investigates the second hypothesis of corporate governance, its accompanying IT governance and its conformance and usability to South African SMMEs.

3 Evaluating Industry Corporate Governance and IT Governance for Usability and Conformance

3.1 Introduction

South Africa as a developing country has a corporate governance standard known as the King II Report [KING 2002]. Corporate governance though, as noted in Chapter 1, is not a compulsory practice for SMMEs. This is one of the recognised shortcomings in SMMEs that leads to their high failure rate in South Africa (refer to Chapter 1).

Corporate governance at international level allows increased investment in organisations that can prove that good corporate governance is practised [INET 2004]. This cannot yet be corroborated for South Africa, but it is assumed that such a future exists.

There is much potential in evidence for investment, should corporate governance be applied accurately and effectively across industries and size-markets. This does, however, beg the question whether the good corporate governance standard is applicable or usable across those industries and size-markets.

The same query arises regarding IT governance. IT governance, as noted in Figure 2.4, enables corporate governance. The lack thereof, or impact if applied carelessly, can hamper corporate governance. This in turn means that corporate governance cannot reach its ideal of enhancing the organisation, but in fact becomes a cumbersome exercise with little return on investment.

With such flags of concern already raised if corporate governance or IT governance is applied without due diligence, the same concern is compounded if the standards in existence have not been created for applicability across size-markets, specifically when considering South African SMMEs.

The objective of this chapter is thus to determine whether the standards of corporate and IT governance in place in South Africa are on a par with international standards, and if so, whether they can be applied to South African SMMEs, as defined in Chapter 2.

The first goal of this chapter is to compare the King II Report with an international corporate governance standard to determine whether King II is at an internationally acceptable level.

The second goal of this chapter is to present the results of the evaluation of the King II Report for suitability to South African SMMEs.

The third goal of this chapter is to establish the fit of the accepted IT governance standard in South Africa to King II.

The final goal is to present the results of the evaluation of the IT governance standards for applicability to South African SMMEs.

This chapter begins with a comparison of the corporate governance standard in South Africa with an international standard.

3.2 Corporate Governance in South Africa compared to the International Standards

South Africa as a developing country is advanced in the sense of having a practised corporate governance standard. This is apparent when evaluating the so-called deliverable of corporate governance, namely sustainability reporting.

3.2.1 Corporate Governance in Africa

Sustainability reporting, stemming from the term ‘sustainable development’, reflects the organisation’s commitment to continuous growth and development. The Association of Chartered Certified Accountants (ACCA) is an international body that evaluates the contribution of these reports by organisations worldwide [ACCA 2004].

These evaluations have found that South Africa produces over two-thirds of all sustainability reports in the Africa and Middle East region (refer to Figure 3.1) [ACCA 2004]. This commitment by South African organisations has surged since the inception of the King II Report in 2002. The creation of these reports is thus directly attributable to King II [ACCA 2004].

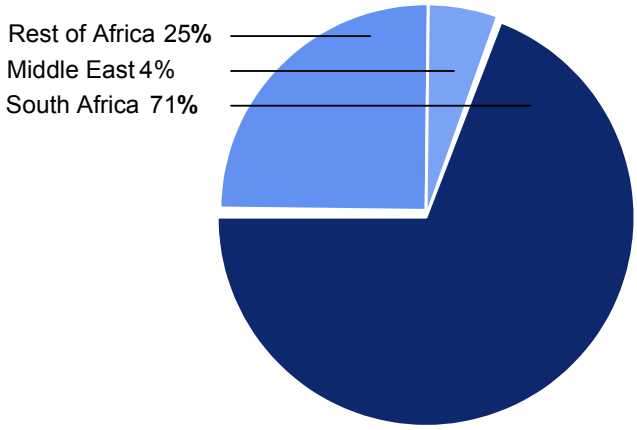


Figure 3.1: Sustainability reports produced in Africa and the Middle East

The rest of Africa reflects a poor representation of reporting, only contributing 25% of the total. In the sample of developing countries used in Chapter 2, Botswana, an African country, showed the most economic growth over the last three years. The same cannot, however, be said of corporate governance.

The highest producer of sustainability reports in Africa after South Africa is Nigeria at 7% (refer to Figure 3.2). The number of reports contributed by Botswana does not feature as representative of Africa's tally. It can thus be deducted that corporate governance in this example of a well-developing country is negligible.

The King II Report has had an obvious influence on sustainability reporting in South Africa. It demonstrates the importance of the reports through a section devoted solely to integrated sustainability reporting [KING 2002].

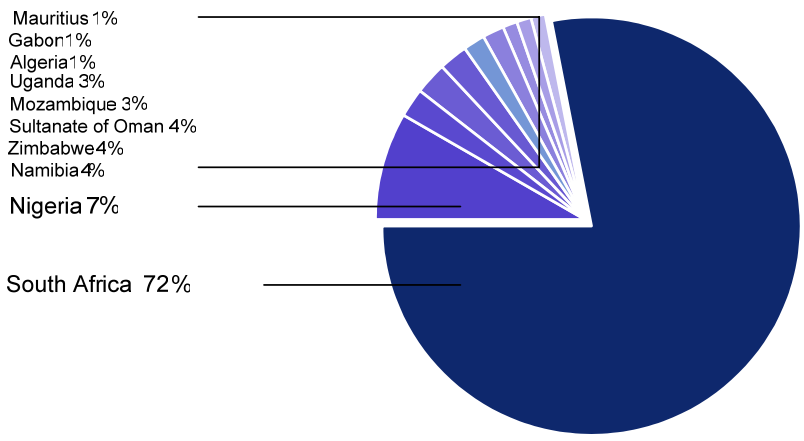


Figure 3.2: Sustainability reports produced throughout Africa

More evidence of the influence of King II in Africa is the acceptance of King II as the corporate governance standard by NEPAD (New Partnership for Africa's Development) [ACCA 2004]. This decision reflects that NEPAD recognises the King II Report as the foremost corporate governance standard in Africa.

The comparison of developing and developed countries continues by also evaluating the sustainability reports produced by the sample of developed countries.

3.2.2 Corporate Governance in the Americas, Australasia and Europe

3.2.2.1 The Americas

The other partner in the developing countries sample, Argentina, paints a similar picture to Botswana when considering corporate governance. South America, as a whole, represents only 6% of all sustainability reports produced in the Americas, with Argentina producing a mere 0.4% of South American reports. The only country showing a sizable contribution is Brazil, having produced 23 reports (refer to Figure 3.3).

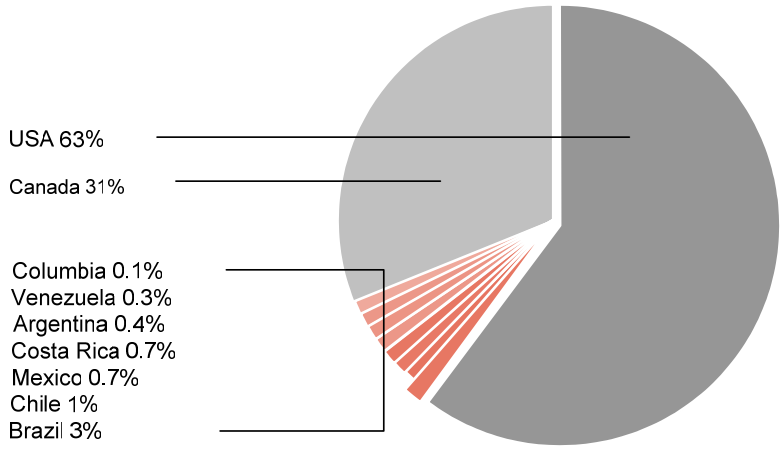


Figure 3.3: Sustainability reports produced in the Americas

Brazil recognises the need for reporting and has created an Institute of Business and Social Responsibility devoted to this cause [ACCA 2004]. No other South American country has taken such steps.

The USA, a developed country sample representative, as reflected in Figure 3.3, produces 63% of the total for the Americas. This amounts to 446 reports.

It is clear that the Americans are committed to creating these reports, and as such a well-established corporate governance presence.

Canada, although not in the sample, also clearly has a strong corporate governance commitment.

3.2.2.2 Australasia

The largest contributor of sustainability reports in Australasia is Japan at 49%, followed by Australia at 38% (refer to Figure 3.4).

Australia, as representative of the developed countries sample, proves to have a substantial reporting drive, producing 339 reports. This number is high when compared to the USA, which produces 446. The two populations of these countries, as noted in Chapter 2, differ greatly. Australia appears to be extremely committed to corporate governance.

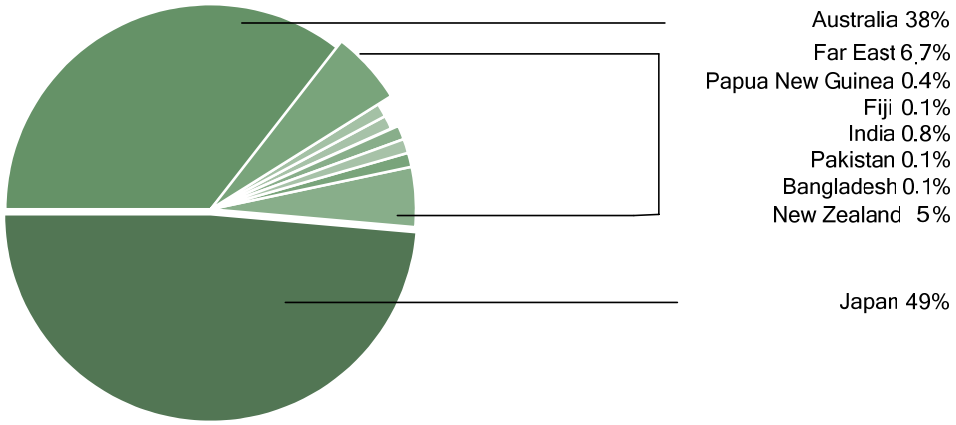


Figure 3.4: Sustainability reports produced in Australasia

3.2.2.3 Europe

Europe is at the forefront of compliance. It is the largest producer of sustainability reports, producing 1 964 reports.

The UK is the largest producing country with 28% (549 reports), with the Scandinavian region following closely behind with 20% (392 reports), despite being a sparsely populated region (refer to Figure 3.5).

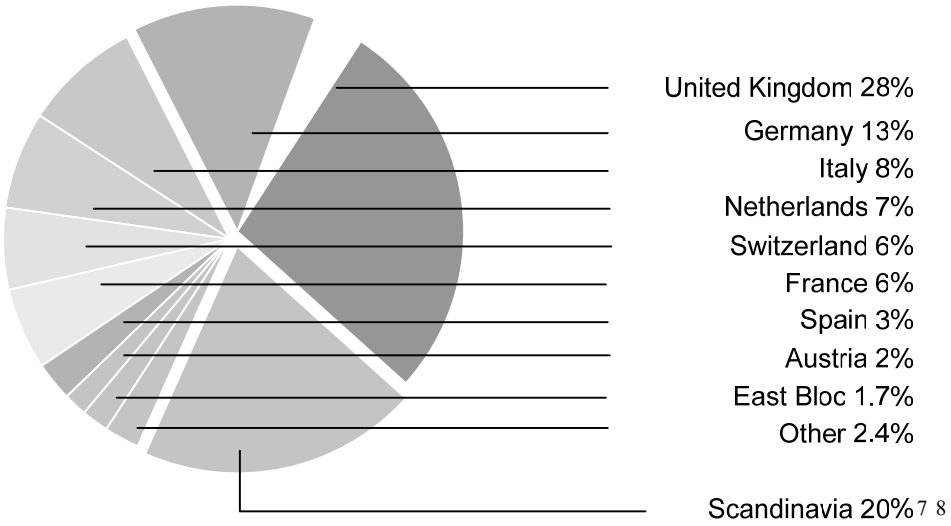


Figure 3.5: Sustainability reports produced in Europe

The conclusion can be made from the figures in Figure 3.5 that corporate governance is practised widely in Europe, the only continent that can boast such an achievement.

A further conclusion can be made that developed countries have embraced the concept of corporate governance and apply it significantly. This is further supported by the heightened investment in organisations that can prove good corporate governance.

The number of reports produced by South Africa, although rising every year, is still very low when compared to the developed countries. King II thus needs to be examined against the corporate governance of a developed country to ensure that it is a standard at a level conducive to international scrutiny.

3.2.3 King II vs. Australian Stock Exchange Corporate Governance Council[9]

From the above, the King II Report seems to be the only admirable corporate governance standard in the sample of developing countries. King II is thus compared to one country's corporate governance standard selected from the sample of developed countries to ensure that it is a standard on a par with that of an economically viable country before attempting to apply it to South

[7] The East Bloc in Figure 3.5 represents the following countries: Croatia, Slovakia, The Russian Federation, Czech Republic, Estonia and Hungary.
[8] 'Other' in Figure 3.5 represents the following countries: Luxembourg, Ireland, Greece and Portugal.
[9] The Australian Stock Exchange Corporate Governance Council is a body created for the formulation of Australian corporate governance and its control.

African SMMEs. As all three countries have proven commendable standards, cross-evaluation of each would prove redundant.

The standard selected for comparison is thus the Australian Stock Exchange Corporate Governance Council standard (hereafter referred to as ASX) [ASX 2003]. No previous comparison of King II and ASX has been found in literature. The research findings listed here are unique to this study.

Each of these standards must be compared by content, compliance and usability to examine both the quality of the standard and its applicability. The standards should be usable, but not lightweight in content.

3.2.3.1 Major Sections covered by King II

The major sections into which the King II Report is divided are listed as follows [KING 2002] [CLIF 2004]:

- Roles and responsibilities of the boards and directors
- Responsibility and method of risk management
- Role and scope of internal audit
- Integrated sustainability reporting
- Accounting and auditing
- Compliance and enforcement

3.2.3.2 Major Sections covered by ASX

The ASX agrees that the fundamental foundation of corporate governance lies in establishing the roles of management and the board [ASX 2003]. The essential sections of corporate governance are listed as:

- Recognise and publish the respective roles and responsibilities of the board and management
- Have a board of effective size and commitment
- Actively promote ethical and responsible decision-making
- Safeguard the integrity of the company's financial reporting
- Promote timely and balanced disclosure
- Respect the rights of shareholders

- Recognise and manage risk
- Encourage enhanced performance
- Remunerate fairly and responsibly
- Recognise legal and other obligations of all legitimate stakeholders

The sections of the two standards can be compared using the guide in Table 3.1.

Table 3.1: Sections of the corporate governance standards

King II	ASX
Roles and responsibilities of the boards and directors	Recognise and publish the respective roles and responsibilities of the board and management Have a board of effective size and commitment Actively promote ethical and responsible decision-making Respect the rights of shareholders Encourage enhanced performance Recognise legal and other obligations of all legitimate stakeholders
Responsibility and method of risk management	Recognise and manage risk
Role and scope of internal audit	Safeguard the integrity of the company's financial reporting
Integrated sustainability reporting	Promote timely and balanced disclosure
Accounting and auditing	Remunerate fairly and responsibly
Compliance and enforcement	None

Seven accentuated factors have been extracted from the content of both King II and ASX to evaluate the similarities and differences of the two standards. The evaluation is represented in Table 3.2.

Table 3.2: The similarities and differences of King II and ASX

Factor	King II	ASX	Comment
Importance of the board	Denoted early in the standard.	Denoted early in the standard.	The implementers of the standard should be identified before providing additional information.
Information related to the board	All information related to the board is in one large section.	The information is separated into various categories.	All information related to the board should be communicated as a collective.
Risk management	Risk management is noted as an internal control function.	Risk management is noted as a duty at board level, but no further guidance is noted.	Risk management should be controlled by the board and as such afforded the sense of importance it warrants.
Clear description of internal audit function	A section is devoted to the roles of an audit committee.	The creation of an audit committee is promoted.	The requirement of an audit committee is made apparent; the role of said committee should also be thus.
Annual reporting	A section is devoted to describing reporting.	The strength of the reports section is reduced by ambiguous guidelines.	Annual reporting should be a guided, fixed requirement. It creates a standard of performance measurement and community awareness.
Clearly defined code of conduct	A code of conduct is a preface to the sections of the report.	A section is devoted to the code.	The two standards evaluated offer fair representation of a corporate code of conduct.
Compliance	Clearly defined non-compliance and enforcement.	Reporting is voluntary and not enforced.	Quality of reporting is not guaranteed if not enforced.

The question of compliance with corporate governance regulations could lead to a heated debate. The fact that the Australian standard is not enforced but yields such large numbers raises the paradox of enforce and receive some reports, or not enforce and perhaps receive no reports.

The Australian achievement is deflated though by the Horwath Corporate Governance Report, which examined the quality of the many reports submitted [PSAR 2002]. Of the 250 reports analysed, only nine were created at the appropriate level of quality. 13 reports were at the lowest level of quality, and the majority in the lower tiers of quality. The Horwath Report suggested the instigation of non-compliance measures [PSAR 2002].

The next evaluation compares the sections of the two standards by considering the weight they carry in the standard, the clarity with which they are presented and their technical requirements. This evaluation is represented in Table 3.3.

From the criteria listed in Table 3.3, King II compares well against a developed country's corporate governance standard. It is thus concluded that King II is a quality standard, and is successfully compared to an international level of standard.

Table 3.3: Cross-sections of corporate governance

Cross-section	ASX	King II
Solid foundation for management	ASX promotes the publishing of roles and responsibility of the board. This is presented in a board charter.	King II also requires the creation of a charter, adding that it should be included in the annual report.
Structure the board to add value	ASX recommends that the board have a proper understanding of current business, and an effective review system to manage the competency and performance of the board. The board is required to host independent board members and an independent chair.	King II contains the same almost to the letter, except for including disciplinary measures against board members that do not add the required value (as a result of annual evaluations), as well as requiring social transformation.
Promote ethical and responsible decision-making	ASX requires the establishment of a code of conduct for board members, as well as confidentiality policies relating to securities.	King II has devoted an entire section to the code of conduct of a board, which includes a summary of board composition, key focus areas and prohibition of securities trade.
Safeguard integrity in financial reporting	ASX requires a formal statement by either the chairperson or chief financial officer (CFO) that the financial reporting is accurate, and represents a fair view of the organisation's financial standing. An audit committee should be established with a majority of independent directors and a formal charter.	King II requires that each board have at a minimum an audit and remuneration committee. These committees should be chaired by a non-executive, independent director. Committee composition, meetings held and a brief description of its responsibility have to be included in the annual report.

Make timely and balanced disclosure	ASX requires establishment of written policies to ensure accountability at senior management level for compliance. There are no legal ramifications of non-compliance.	King II has devoted an entire section to compliancy regulations, although adds that the recommendations are not too burdensome. “The legal principles imposed are subject to criminal remedies.” Disclosure is enforced by King II threatening legal action.
Respect the rights of shareholders	ASX requires the design of a strategy for effective communication with shareholders. Attendance of the annual general meeting by the external auditor to present testimony of the audit is encouraged.	The board is requested to encourage shareowner attendance at general meetings. Repricing of share options is subject to prior shareowner approval. Non-executive directors are encouraged to receive shares rather than share options.
Recognise and manage risk	ASX requires a policy on risk management to be established by the board or a committee of the board. The chief executive officer (CEO) or CFO is accountable for the adherence of financial reporting to the risk management policy.	King II has expanded on the mention of risk management and controls to include technology risk to the financial risks. It requires documented proof that risks were identified and managed, to be included in the annual report.
Remunerate fairly and responsibly	ASX requires that the board motivate the link between remuneration paid to directors and corporate performance. This is done in a disclosure document in the annual report. The establishment of a remuneration committee is required.	Membership of the remuneration committee should be published in the annual report. Full disclosure of director remuneration on an individual basis is required. The annual report should contain a “Statement of Remuneration Philosophy”.

3.3 The Usability of King II in South African SMMEs

The King II Report was created for public companies to ensure that corporate South African business is well governed. The fact that no allowances or additions regarding SMMEs were made is concerning, considering the contribution of SMMEs to the GDP, and their subsequent importance relating to employment, empowerment and development as discussed in Chapter 2.

The ACCA[10] report [ACCA 2004] recognises this shortfall on a global scale by stating that:

> *"…for small and medium sized enterprises the resource costs of collating data and publishing a report remains an inhibiting factor, the development of common standards and efficient guidance will help make it more realistic for smaller organisations to produce reports."*

The cost of applying corporate governance controls and the subsequent reporting on the triple bottom-line is a costly exercise [KING 2002], and can be even more so for an SMME.

There are definite factors in the King II Report that, if applied to the SMME, could have a dramatic impact on the diligence of management and the subsequent sustainability of the SMME.

The following assumption is taken into consideration:

> It is not feasible to order an SMME with a staff complement of ten individuals to remunerate a board of directors, with the majority being independent non-executive directors.

Below follows an analysis of the sections of the report from the perspective of an SMME, and how the guidelines may be applied.

Boards and Directors

The functions of the board described in King II include the appointment of an audit committee, a nomination committee and a remuneration committee. These duties can be combined in the SMME by forming a board of decision-makers. This board should include those members of staff who own shares, hold a senior management position, have the required skills and have a vested interest in the success of the business, and an independent chairperson, or if this is not possible, a non-shareholding executive.

[10] The Association of Chartered Certified Accountants is the largest international accounting body. The ACCA participates in reporting awards in over 20 countries, and the Global Reporting Initiative (GRI).

Senior management officials may be nominated to the board by either opting for a board decision, or a staff selection, depending on the size of the SMME and the role required by the nominee.

The chairperson of the board should by rights be independent to ensure impartial decisions and proper use of meeting times. If the organisation cannot financially support such an individual, an executive member of staff should be elected.

Duties of the board:

- Financial control of the organisation
- Sustainability investigations
- Risk management
- Transparency and communication

Accounting and Auditing

The member of the board managing auditing and accounting is held responsible for the internal control of the organisation, including systems, and is to report to the board on the financial state of the organisation.

Sustainability Reporting

Accepting the benefit of sustainability investigations as an SMME, even at a simplified level, prepares the organisation for possible future growth where such an exercise becomes compulsory.

The purpose of sustainability reporting is to create awareness of the community surrounding an enterprise, including opportunities, threats, the environment and the ethics of the community that empowers the organisation to improved decision-making regarding future strategies.

Risk Management

SMMEs are by nature entrepreneurial enterprises that face risks on a daily basis.

An exercise in determining the risk tolerance or profile of an SMME should be considered in the sense of sustainability. The SMME should evaluate those risks that threaten its survival, and mitigate or terminate the risk.

A major consideration for risk management is evaluating those risks that face the everyday survival of systems on which the organisation depends.

King II proposes the use of recognised models for risk management. Whether these models exist for SMMEs is yet to be identified. The areas listed for risk management are:

- Physical and operational risk
- Human resource risk
- Technology risk
- Business continuity and disaster recovery
- Credit and market risk
- Compliance risk

Technology and business continuity risk controls are not volunteered by King II. IT governance fulfils these requirements, and as such becomes an enabler of corporate governance.

Transparency and Communication

The concept of transparency is that of transferring knowledge to parties that have a vested interest in that knowledge, may benefit from the knowledge and may add value to the organisation once owning that knowledge. Staff members of an organisation are stakeholders in the enterprise. This is vital to an SMME, as a strike by staff may cripple the enterprise, or in some cases ruin it. It is, though, not entirely likely, due to the fear of unemployment.

Staff buy-in is recognising improved productivity and efficiency.

The responsibility of reporting the success of transparency should reside with the chairperson. The same applies for the implementation of transparency.

IT governance, as noted, enables corporate governance. The usability of an accepted IT governance standard as a component of corporate governance is determined next.

3.4 IT Governance in South Africa

IT governance in South Africa is corporately practised through the only internationally accepted standard CobiT (Control Objectives for IT). The third

version of CobiT was released in 2000 and is endorsed by the International IT Governance Institute, the ITGI [ITGI 2005].

The CobiT standard consists of five manuals:

- The CobiT Framework. The Framework presents an overview of the CobiT methodology, including definitions of the terminology used throughout the manuals [COBI01 2000].
- The CobiT Control Objectives. The CobiT Framework consists of 34 control objectives. Each control objective is thoroughly discussed in this manual [COBI02 2000].
- The CobiT Implementation Tool Set. This manual provides guidelines on the implementation of the control objectives, considering the resources required and outcomes expected [COBI03 2000].
- CobiT Management Guidelines. The management guidelines form a dashboard with which management can monitor progress made in the Framework, as well as the impact on the enterprise. This includes a maturity model used to examine the advancement of the enterprise [COBI04 2000].
- CobiT Audit Guidelines. These guidelines are offered to audit the effectiveness of the control objectives applied. They are also used to assess compliance with CobiT [COBI05 2000].

CobiT can be related to the King II definition of risk management [KING 2002], defined as the:

"identification and evaluation of actual and potential risk areas…followed by a process of either termination, transfer, acceptance or mitigation of each risk."

The risk management process is defined as [KING 2002]:

"planning, arranging and controlling of activities and resources to minimise the impacts of all risks to levels that can be tolerated..."

CobiT is structured around four domains that follow a cycle for IT governance. These domains form steps in the IT governance process. Below is a comparison of the steps in the CobiT process and the process of risk management defined in King II.

Table 3.4: King II risk management process compared to the CobiT process

<table>
<tr><th>King II</th><th>CobiT</th></tr>
<tr><td>Planning</td><td>Planning and organisation</td></tr>
<tr><td colspan="2">The control objectives listed in the planning and organisation step in the CobiT process allow the organisation to define its IT strategies, assess risks, manage compliance and communicate back to the organisation.</td></tr>
<tr><td rowspan="2">Arranging</td><td>Acquisition and implementation</td></tr>
<tr><td>Delivery and support</td></tr>
<tr><td colspan="2">Acquisition and implementation allow the organisation to act upon the planning done in the previous step of the process, arranging solutions, so to speak.

Delivery of the solutions and support for them create the opportunity for the organisation to ensure continuous management of the resources involved in IT governance and mitigation of risks.</td></tr>
<tr><td>Controlling</td><td>Monitoring</td></tr>
<tr><td colspan="2">Monitoring of controls implemented allows the organisation to be aware of its IT governance in practice and the progress made in managing any problems identified. This offers control of the risks and their mitigation.</td></tr>
</table>

The CobiT steps fit with the requirements of King II, even more comprehensively so. There is considerable detail in the CobiT manuals and as such, the ITGI does not expect all 34 control objectives of the steps to be implemented, but does require that each of the steps be implemented. Using the steps of CobiT allows an organisation to create an IT strategy for a cycle of determined duration. CobiT also allows the implementation of risk management in the same cycle.

Refer to Appendix 2 for a summary of CobiT, spanning the steps (domains) and the control objectives.

3.5 Usability of CobiT in South African SMMEs

There is no question whether CobiT should be applied in any organisation. There are benefits for each conceivable IT-empowered organisation to apply some, if not all, of the control objectives. It is, however, recognised that application of the control objectives as they stand is an expensive, time-intensive exercise requiring commitment from various parties [COBI01 2000].

An SMME, as has been established, is not an organisation with much time or resources to spare. Application of some of the control objectives may, however, open up time pockets to allow other activities to occur. Once again, application of IT governance with commitment prepares the SMME for entrance into the corporate arena.

Selection of the applicable or most effective control objectives is no simple task. An erroneous selection may cause the allocation of resources to a low-return effort. The benefit of any control objective is not questioned, but rather the selection of the highest level of benefit versus resource allocation. Appendix 3 details the selection criteria that have been identified as guidelines to the selection process. The guidelines are used in the following example to demonstrate the selection process.

An Example of CobiT Control Objective Selection for an SMME

A stereotypical SMME is used in the example to demonstrate the application of the selection guidelines. The selection process makes use of four maturity model based criteria, each attributing a maximum score of 5 points. The selection process is as follows:

1. Identify the organisation's IT resource management maturity

   By identifying the organisation's maturity, an understanding can be reached of the scope of control objectives required. The IT resource management maturity is rated as *Repeatable* due to the organisation's interest in applying control measures. A score of 2 is attributed.

2. Identify the level of authority by organisation owners or managers

   The level of authority of business owners or managers would determine the amount of staff buy-in that may be obtained. The maturity is rated as

Initial as the organisation has not established formal management structures. A score of 1 is attributed.

3. Level of technological sophistication in the organisation

   The level of technology used in the organisation affects the control required of the systems in place. The maturity is rated as *Defined* due to the conformance of machines and systems available to the existing IT need. A score of 3 is attributed.

4. Technology/information risk profile

   The awareness of a risk profile may increase the consideration of decisions made and steps taken concerning the risk area. The maturity is rated as *Defined* due to the recognition of risks and the understanding that mitigation is required. A score of 3 is attributed.

The model used above is now used to calculate the control objective application range used to identify those control objectives most suited to the organisation. The range is reached by adding the model values selected in the four criteria above. The determining score is presented in Table 3.5.

Table 3.5: The score determining the application of control objectives

Criteria	**Score**
IT resource management maturity	2
Level of management authority	1
Technological sophistication	3
Risk profile	3
Final score	**9**

The example organisation has been rated into the third level of maturity out of 4 (score of 9 – 12). The growth of the organisation from one maturity level to another should follow the “define process, implement sophistication, monitor process” route as explained in Appendix 3.

The organisation is assumed to have made progress in its IT governance and needs a formalisation of the outcomes of its efforts. The table defining all four ranges is available in Appendix 3.

The control objectives suggested for application are listed in tabular form. The extent to which the SMME chooses to apply the control objectives should be at the discretion of the board.

The control objectives identified as applicable were selected considering the following assumption:

- Any control objective attempted should be done in a workshop environment allowing staff participation. As control objectives do require resources, buy-in becomes paramount.
- The maturity levels of “define process, implement sophistication, monitor process” can be expanded as follows:
    - **Define process** selects the initial control objectives required for formalising the organisation’s intended use of IT, assessing the risks the organisation faces, managing those resources required, developing service levels, formalising change and incident response structures and monitoring these initial steps during the process.
    - **Implement sophistication** creates room for the organisation to improve the policies and procedures already in place. This includes the acquisition of improved systems, higher levels of service delivery, more control over IT resources and improved monitoring of IT. This step involves the largest requirement of resources, as it lifts the organisation from acceptable control to sophisticated control.
    - **Monitor process** is the maintenance of the sophistication reached in the previous level. An organisation rated at this level already may require some backtracking if some of the sophistication markers are not in place. This level is the least resource intensive, but may require increased resources if the required input for maintenance is not upheld.

Table 3.6: Recommended use of CobiT by the example SMME

Control Objective	Range
Planning and organisation	**9 – 12**
Define a strategic IT plan	●
Define the information architecture	●
Determine technological direction	●
Define the IT organisation and relationships	●
Manage the IT investment	●
Communicate management aims and direction	●
Manage human resources	●
Ensure compliance with external requirements	●
Assess risks	●
Manage projects	●
Manage quality	●
Acquisition and implementation	
Identify automated solutions	●
Acquire and maintain application software	●
Acquire and maintain technology infrastructure	●
Develop and maintain procedures	
Install and accredit systems	●
Manage changes	●
Delivery and support	
Define and manage service levels	●
Manage third-party services	●
Manage performance capacity	●
Ensure continuous service	●
Ensure system security	●
Identify and allocate costs	●
Educate and train users	●
Assist and advise customers	●
Manage the configuration	
Manage problems and incidents	●
Manage data	●
Manage facilities	●
Manage operations	●
Monitoring	
Monitor the processes	●
Assess internal control adequacy	●
Obtain independent assurance	●
Provide for independent audit	●

The application of the control objectives marked above is debatable by the organisation. This list is a guide only, with due consideration of assumed maturity.

3.6 Conclusion

This chapter has delved deeply in the structured governance practices in business and IT. It has been found in this chapter that the King II Report is satisfactorily inclusive of the major governance practices supported by developed countries. The goal of the chapter has thus been achieved.

The chapter also uncovered grounds for the encouragement of compliance enforcement in sustainability reporting as a deliverable of corporate governance.

The second goal has been achieved as the King II Report has been evaluated for usability by an SMME, and tangible uses have been discovered, achieving the goal, even though simplicity is motivated.

The internationally accepted standard for IT governance, CobiT, has been evaluated in its entirety for usability by a South African SMME, fit into the King II standard and recommended prioritised use of the 34 control objectives. Fit has been achieved, as well as a model proposing use of CobiT by an SMME. This is the achievement of the third and final goal.

It has been found in this chapter in total that South African corporate governance and IT governance standards can be applied to SMMEs, even if in a simplified format. It has also been found that although King II prescribes technology and business continuity risk management, it does not volunteer how the organisation should approach such a monolith. CobiT does represent the means to control the technology and business continuity risk, specifically relating to ownership of responsibility, and the inclusion of risk management in the organisation's IT strategy (refer to Appendix 2).

The operational evaluation of risk and its subsequent management is not yet clear. CobiT, although creating control opportunities, does not provide risk analysis/evaluation and management methodologies, nor does it endorse the use of any recognised methodologies. This is a significant gap in the information security management of the organisation, as the resolution of possibly crippling risks is not guided, nor emphasised enough.

The use of risk management, or specifically information security risk management methodologies for this IT governance, and subsequently corporate governance, is evaluated in Chapter 4.

4 Information Security Risk Management for Small Businesses

4.1 Introduction

ISRM has been mentioned several times thus far in this dissertation. It was defined in Chapter 2, and referred to in the context of IT governance in Chapter 3. The actual methodologies in practice, however, have not yet been vetted.

This chapter's primary objective is the examination of ISRM methodologies, specifically those for use by small businesses.[11]

The examination of the said methodologies is split into two goals. The first goal is to present the results of the evaluation of the methodology against a predetermined set of criteria based on discoveries in the previous chapters.

The second goal is the categorisation of the advantages and disadvantages of the methodology based on the performance against the criteria.

The secondary objective of the chapter is to determine whether the advantages of the evaluated methodologies motivate their use by South African SMMEs to manage information security risk.

The methodologies that are evaluated for this dissertation have been selected due to their free availability to the public, and thus an SMME, and their endorsement by internationally recognised institutions or associations. The search for freely available methodologies did not provide further, internationally endorsed candidate methodologies. The methodologies are:

- OCTAVE-S, developed by the Software Engineering Institute (SEI) residing in the US.
- CRAMM V Express, developed by Insight Consulting, the foremost implementer of CRAMM, a British developed methodology.

[11] The term 'small business' represents SMMEs in this chapter as used by the methodologies examined.

The evaluation is based upon a set of criteria defined hereafter.

4.2 Framework for the Evaluation of ISRM Methodologies

The research findings presented thus far have ranged from defining a South African SMME as a unique small business compared to developed and other developing countries' small businesses, to the use of corporate and IT governance by SMMEs.

Elements of these findings have created a panorama of characteristics of an SMME. It has been discovered that SMMEs in South Africa fail due to the lack of business knowledge and governance. It has also been found that SMMEs lack due diligence owing to the constraints of time, human resources and cost, as related to the attainment of tools for diligence.

The use of corporate and IT governance as suggested in this dissertation also creates a benchmark of procedural order to be followed.

These characteristics and benchmark create a framework of requirements for the evaluation of an undertaking by an SMME. Such an undertaking may be any project approached by the SMME for development, improvement and auditing. In this case, this framework is used to evaluate the fit of recognised ISRM methodologies to a South African SMME. The framework is explained below.

4.2.1 The Framework Explained

The framework that has been created for the evaluation of SMME undertakings has four main elements. These elements are subdivided into factors.

The framework is three-dimensional, and includes a weighted system for quantifiable measurement of the undertaking.

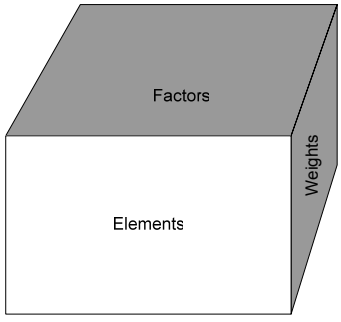


Figure 4.1: The three-dimensional framework

4.2.2 Elements of the Framework

The elements as derived from the research findings above are:

1. Visibility
2. Cost
3. Regulatory fit
4. Fit to South African SMMEs

Each element is discussed in detail below.

4.2.2.1 Visibility

Visibility pertains to the ease with which the ISRM approach may be obtained, specifically by an SMME. This includes whether the full methodology is obtainable with ease, or whether promotional material only is available. The objective of visibility is to measure whether the interested party within the SMME can reasonably gain an understanding of the methodology and thus make an informed decision of whether to proceed with the ISRM methodology.

4.2.2.2 Cost

The cost of implementing the undertaking is an estimated measure, as the true cost of any exercise can only be determined after the fact. Cost is, however, a relative term, as there are many facets to an undertaking that may be added as a cost, even though no direct spending was involved. Cost is therefore split into these factors:

- Purchase cost is the requirements of cash spent on the undertaking, whether it is an upfront cost, or expenditure throughout the undertaking for obtaining the methodology.
- Organisational involvement is attributable to the human resources involved in the undertaking, through various channels. These channels, known as subfactors, are:
    - Knowledge requirement. All training required by the organisation, or elected individuals.

- Senior management buy-in. The involvement of senior management in an undertaking is an expensive factor, as senior management time is at a higher value than that of an operational employee.
- Self-directed or consulted. The nature of the undertaking also affects the cost of the implementation. A self-directed approach may be higher in organisational involvement cost, but lower in purchase cost. The inverse applies to a consulted approach. The purchase cost may be higher, but organisational involvement is less. The duration of the undertaking, as prescribed by the nature of the undertaking, must also be considered.
- The duration of a consulted approach may be shorter, as the schedule is managed by a third party. The duration of a self-directed approach is self-led, and thus may be prone to operational delays.

4.2.2.3 Regulatory Fit

The regulatory models that have been evaluated thus far have been the King II corporate governance standard and CobiT. Table 3.4 refers to the fit between these two standards, and the requirements of risk management in King II. The evaluated methodology is required to conform to the steps of Table 3.4.

The steps require the undertaking to have a planning, execution and management course, ensuring that a cyclical reviewing process is followed.

4.2.2.4 Fit to South African SMMEs

South African SMMEs have been determined as unique when compared to five other nations' definitions, and this should be considered before implementing an undertaking created for the SMME of a different nation.

The fit to South African SMMEs is evaluated contrariwise against the following factors:

- Horizontal or vertical industry. The undertaking should not promote or be aligned with a horizontal or vertical industry. There should be no restriction on the industry of the SMME.
- The size of organisation. The South African SMME has been defined as ranging from 1 staff member to 200. The undertaking should not be focused on a number excluding parameters of this range.
- The type of organisation. Any structure of small businesses should be allowed, especially when considering the existing lack of business skills. There should be no restriction on structure.

To summarise, the only restriction that is endorsed is the maximum allowance of 200 employees.

The framework is summarised in Figure 4.2. The undertaking is evaluated against the four elements.

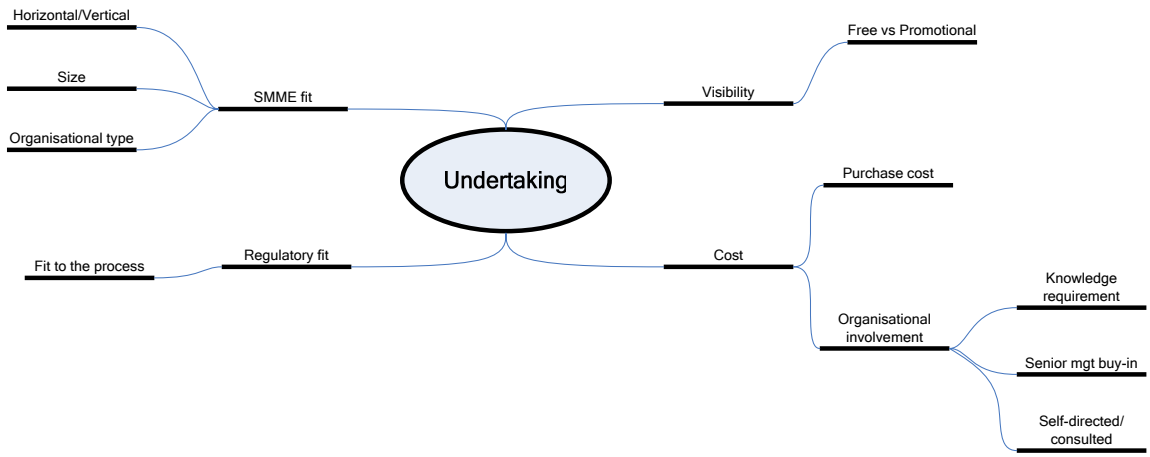


Figure 4.2: The framework, its elements and factors

The framework has thus far been explained in two dimensions. The third dimension, the weighting, is assigned as follows:

4.2.2.5 The Weighted Dimension

Weights have been assigned to each element, factor and subfactor. The weights have been assigned based on estimated importance of the element.

The most important element, cost, has been assigned the highest weight due to the cost focus of SMMEs. A high purchase cost alone could dissuade the SMME owner or decision-maker from implementing an undertaking, and thus

it carries the most weight. However, cost is not the only consideration. Lack of SMME or regulatory fit may result in a very low return on investment, even though the cost is low. This is thus the motivation for a weighted framework.

Visibility also carries a fairly high weight, even though it does not directly impact the implementation of the undertaking. It does, however, impact the undertaking itself. The remaining weights become of no consequence if the decision-maker cannot obtain an initial understanding of the undertaking. Avoidance of visibility would create a blind implementation of the undertaking, as the decision-maker is attempting to improve the organisation, but has no assurances that the implementation is the right one.

The remaining weights are also go/no-go weights. If the undertaking scores low on SMME and regulatory fit, the organisation can be assured that, for its enterprise, it is not the optimum solution. A score of 0 in both requires immediate dismissal.

The total of the weights provides a score out of 100. This is then easily compared to other evaluations for decision-making. Should two options score equally, the elements themselves should be compared, using the go/no-go decision blocks. The organisation should review the weights for adequacy in the environment before implementation.

Table 4.1 below outlines the elements, factors and subfactors with their assigned weights. A description of the assigning of weights for each factor is provided, creating guidance for quantification. All decision points are also highlighted, providing the evaluator with the option to dismiss an undertaking. The final decision is based on a score higher than a reasonably conservative 30.

Table 4.1: The weights of the framework

Elements, Factors and Subfactors		**Assigned Weight**
Visibility		**20**
The undertaking's methodology is freely available and user-friendly	*20*	
Promotional information is freely available with details for further information	*10*	
No information is freely available	*0*	
GO/NO-GO DECISION – HIGH RISK OF FUTILE IMPLEMENTATION		

Cost		**40**
Purchase cost		20
The undertaking's methodology is free	*15*	
The undertaking's methodology is free but has a tool that reduces organisational involvement available at a cost	*5*	
The undertaking's methodology has a cost attributed	*0*	
The undertaking's methodology has a cost attributed that includes a tool that reduces organisational involvement	*5*	
Organisational involvement		20
Knowledge requirement		5
The organisation is expected to already have all knowledge required for the undertaking	*0*	
There is training available for the organisation at a cost	*5*	
No previous knowledge is required	*5*	
Senior management buy-in		5
The undertaking's methodology promotes senior management buy-in or sponsorship	*5*	
The undertaking's methodology requires senior management execution	*0*	
The undertaking's methodology does not promote or require senior management buy-in	*0*	
Self-directed or consulted		10
The undertaking is self-directed	*5*	
The undertaking is self-directed with consulting available	*10*	
The undertaking is consulting based with no operational involvement from the organisation	*5*	
GO/NO-GO DECISION: IS THE COST TOO HIGH?		

Regulatory Fit		**20**
The undertaking's methodology conforms to the steps in Table 3.4	*10*	
The undertaking's methodology does not conform to the steps in the process in Table 3.4, but does include at least planning and arranging	*5*	
The undertaking's methodology does not conform to the steps in the process in Table 3.4 at all	*0*	
The undertaking's methodology is cyclical and promotes reviewing	*10*	
The undertaking's methodology is not cyclical and does not promote reviewing	*0*	
GO/NO-GO DECISION: HIGH RISK OF ANTI-REGULATORY SOLUTION		
Elements, Factors and Subfactors		**Assigned Weight**
SMME Fit		**20**
Horizontal/vertical		5
The undertaking's methodology is restricted to a horizontal or vertical industry	*0*	
The undertaking's methodology is not restricted to any industry	*5*	
Size		10
The undertaking's methodology restricts the size of the organisation to a range within the parameters of South African SMMEs	*0*	
The undertaking's methodology is restricted to the parameters of South African SMMEs	*10*	
Organisational type		5
The undertaking's methodology is restricted to a specific type of organisation, e.g. hierarchical structure	*0*	
The undertaking's methodology is not restricted to a specific type of organisation	*5*	
GO/NO-GO DECISION: HIGH RISK OF INAPPROPRIATE SOLUTION		
TOTAL		**100**
GO/NO-GO DECISION: IS THE SCORE HIGHER THAN 30?		

The framework has been established in all three dimensions. The following section uses the framework to evaluate the OCTAVE-S information security risk management methodology as an undertaking methodology. The section begins with a discussion of OCTAVE-S, followed by the evaluation outcomes.

4.3 OCTAVE-S Evaluated

OCTAVE-S is based on the OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) approach designed specifically for the unique constraints experienced by small organisations [OCTA01 2003]. OCTAVE-S was developed by the Technology Insertion, Demonstration and Evaluation program of the Software Engineering Institute (SEI).

The OCTAVE approach was launched in 1999 by Christopher Alberts and Audrey Dorofee and was created for use by large organisations [ALBE 2003]. The SEI developed the OCTAVE-S approach in 2003.

The framework of OCTAVE was retained, with simplified implementation of the detail. Below is a brief summary of the OCTAVE-S approach. OCTAVE-S v0.9 is summarised and subsequently evaluated.

4.3.1 OCTAVE-S Summarised

OCTAVE-S is a self-directed information security risk evaluation. It requires a three- to five-member interdisciplinary team to lead the undertaking, and also requires that these staff members have broad insight into the organisation's business and security processes [OCTA02 2003]. The ultimate outcome of the undertaking is an organisation-wide protection strategy and risk mitigation plans.

The OCTAVE-S approach is divided into three phases [OCTA01 2003]. These phases are:

1. Build asset-based threat profiles
2. Identify infrastructure vulnerabilities
3. Develop security strategy and plans

4.3.1.1 Build Asset-based Threat Profiles

The team uses this phase to create a set of criteria against which risks are later evaluated. All organisational assets are identified and the existing

security practice is defined. No external consulting is offered in this phase and all operational tasks are completed by the team itself [OCTA03 2003].

A selection process is used to select three to five critical assets, on which the remainder of the evaluation is conducted.

Finally, security requirements are defined and threat profiles created for each critical asset. The threat profile is based on three levels: the asset, followed by all connected aspects that may expose a threat and the outcomes if the threat is realised. The outcomes are closely related to the characteristics of information security, as defined in Chapter 2. These are disclosure, modification, destruction and interruption of the function of the asset.

The phase is divided into the following processes and activities:

S1. Identify organisational information
- S1.1 Establish impact evaluation criteria
- S1.2 Identify organisational assets
- S1.3 Evaluate organisational security practices

S2. Create threat profiles
- S2.1 Select critical assets
- S2.2 Identify security requirements for critical assets
- S2.3 Identify threats to critical assets
- S2.4 Analyse technology related processes

4.3.1.2 Identify Infrastructure Vulnerabilities

The team analyses the computing infrastructure in this phase, focusing on the access means to the critical assets, albeit systems and data. The team also analyses which parties are responsible for the maintenance of these assets; in many cases with small businesses, this is an outsourced party [OCTA03 2003].

The phase is divided into the following processes and activities:

S3. Examine computing infrastructure in relation to critical assets
- S3.1 Examine access paths
- S3.2 Analyse technology related processes

4.3.1.3 Develop Security Strategy and Plans

This phase requires the team to identify risks to the critical assets and what may be done to mitigate these risks. Risks are measured on a qualitative scale of high, medium or low. All this information is collated into a protection strategy for the organisation's critical assets and mitigation plans to reduce the risks. The worksheets provided are a structured benchmark for creating these plans [OCTA03 2003]. No expectation of when these plans are executed is provided.

The phase is divided into the following processes and activities:

S4. Identify and analyse risks
- S4.1 Evaluate impact of threats
- S4.2 Establish probability evaluation criteria
- S4.3 Evaluate probabilities of threats

S5. Develop protection strategy and mitigation plans
- S5.1 Describe current protection strategy
- S5.2 Select mitigation approaches
- S5.3 Identify changes to protection strategy
- S5.4 Identify next steps

4.3.2 Scope of Application

OCTAVE-S is aimed at organisations ranging from 20 to 80 staff members. The organisational structure is flat, with people from different departments being accustomed to interdepartmental projects [OCTA01 2003].

An organisation such as this is expected to be able to assign three to five people that have broad knowledge of the organisation and its security practices.

OCTAVE-S is not recommended for an organisation that cannot create a team of knowledgeable staff members, for example an organisation that consists of independent business units, or dispersed groups of staff that do not interact much.

The team members are expected to have problem-solving abilities, analytical skills, a teamwork ethic and time, described as a few days. It is not indicated whether the few days are full days, or the total of various short sessions.

4.3.3 Preparation Guidelines

OCTAVE-S provides a module containing all preparation activities that are suggested before kicking off the undertaking [OCTA02 2003].

- The first notable preparation is senior management sponsorship. OCTAVE-S makes it very clear that senior management sponsorship is vital, but cannot clearly define how to obtain it, which is reasonable.

  Senior management sponsorship is required to encourage staff participation, allocation of resources and support of implementation of the outcomes.

- The next preparation activity is selection and training of the team. As has been mentioned, the team should be made up of individuals with the skills listed above, containing at least one leader in the group, and a staff member with close links to IT, either through working closely with IT, or the third-party provider.

  The use of managers on the team is encouraged, but they should not make up the majority of the team as this may restrict open communication.

- Training of the team is addressed by promoting the training of at least one team member on OCTAVE-S. The number of team members to be trained is guided by financial resources available. Training may be received either by formal education, or self-study of the implementation guide. This creates a circular reference, as the creation of the team would already have required some study of the implementation guide.

- Setting the scope of the evaluation allows the team to identify which areas of the organisation are evaluated. A subset of the organisation's business units may be selected, as opposed to the whole. In some cases a single business unit may be selected to provide stimuli for authorisation for a full analysis by senior management. OCTAVE-S recommends at least four business units, one of which must be the IT department or IT management department. This restriction is questionable, as many small businesses may consist of only one or two business units.

- The schedule for the undertaking is created next. Worksheets are provided to offer guidelines of workshop duration, depending on the experience of the team. The duration of the undertaking is demonstrated in Table 4.2.

Table 4.2: Duration of OCTAVE-S

Phase	From	To
Preparation	4 days	8 days, 4 hours
Build asset-based threat profiles	1 day	2 days, 6 hours
Identify infrastructure vulnerabilities	3 hours	1 day
Develop security strategy and plan	1 day	5 days, 1 hour
Total	**6 days, 3 hours**	**17 days, 3 hours**

The worksheets provide a checklist at each process to ensure that all steps have been completed. Guidance is also provided on managing logistics for all workshops.

4.3.4 Implementation Guidelines

OCTAVE-S provides a set of guidelines for each process in each phase with step-by-step instructions of what information is to be gathered and which worksheet is to be completed, as well as definitions of any terminology used [OCTA03 2003].

The guidelines are structured in the order of the phases and their processes. The remaining modules of the implementation guide provide the worksheets for the phases. The evaluation of OCTAVE-S is discussed next.

4.3.5 OCTAVE-S Evaluation Outcomes

The evaluation of OCTAVE-S based on the implementation guide is presented in tabular format in Table 4.3, allowing presentation of scores attributed to the elements and factors provided in the framework, as well as the motivation for the scores.

OCTAVE-S has achieved an average score in total, but ranks very low in the regulatory and SMME fit elements. It is a high-risk methodology for an undertaking for ISRM.

Table 4.3: OCTAVE-S framework evaluation

Elements, Factors and Subfactors	Score Achieved
Visibility	**20**
OCTAVE-S is freely available online and is easy to understand	20
SCORE	**20**
Cost	**40**
Purchase cost	
OCTAVE-S is available at no cost	15
Vulnerability tools may be obtained at a cost but are not required	5
Organisational involvement	
Knowledge requirement	
There is training available for the organisation at a cost	5
Senior management buy-in	
OCTAVE-S requires senior management buy-in or sponsorship	5
Self-directed or consulted	
OCTAVE-S is self-directed	5
SCORE	**35**
Regulatory Fit	**20**
OCTAVE-S does not conform to the steps in Table 3.4, but does include at least planning and arranging	5
OCTAVE-S is not cyclical and does not promote reviewing	
SCORE	**5**
GO/NO-GO DECISION: HIGH RISK OF ANTI-REGULATORY SOLUTION	
SMME Fit	**20**
Horizontal/vertical	
OCTAVE-S is not restricted to any industry	5
Size	
OCTAVE-S restricts the size of the organisation to 20 to 80 staff members	
Organisational type	
The organisation is expected to have more than 4 business units	
SCORE	**5**
GO/NO-GO DECISION: HIGH RISK OF INAPPROPRIATE SOLUTION	
TOTAL	**65**

The following section presents a similar summary of the CRAMM V Express system, with subsequent evaluation outcomes.

4.4 CRAMM V EXPRESS Evaluated

CRAMM V Express, similar to OCTAVE-S, is based on the large organisation version CRAMM V Expert. The software was developed by Insight Consulting based on the CCTA Risk Analysis and Management Method (CRAMM) methodology, created by the United Kingdom Central Computer and Telecommunication Agency (CCTA) in 1987 [SPIN 1999] [CRAM 2005].

CRAMM V Express is a tool for rapid yet effective risk assessments that require limited time and human resources [INSI 2005].

4.4.1 The CRAMM V Express Tool

The tool available from Insight Consulting follows a very simple process for identifying the assets, assessing the risks facing an organisation's assets and proposing mitigating controls, or as CRAMM describes them, countermeasures to reduce the risk.

The tool presents user-friendly screens that allow input from a single user, with reporting available for review. The process followed by the tool is presented in Figure 4.3.

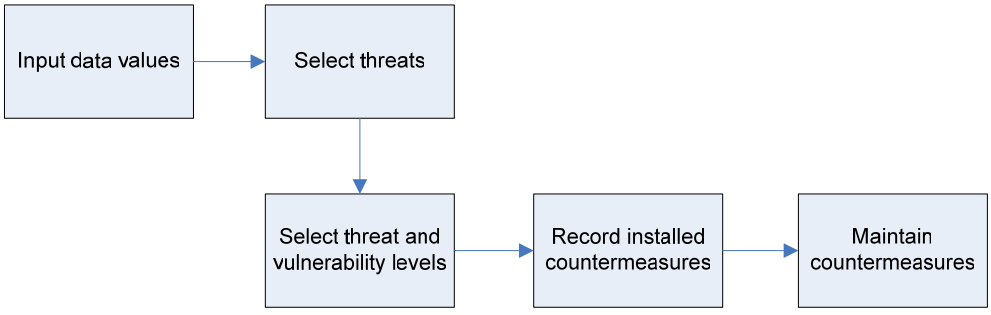


Figure 4.3: The CRAMM V Express Process

4.4.2 Scope of Application

The tool may be used for any system; there is no distinction of which systems should be assessed. There is also no promotion of an organisation-wide assessment or assessment of departments or business units only.

No guidance is offered on who is responsible for managing the assessment, for example who is required to enter the information, and who is responsible for ensuring that the mitigating controls are applied.

The tool does not offer any training on identifying threats or vulnerabilities, or assessing the level of vulnerability once the risk has been identified. The tool assumes that the user is knowledgeable of this specialist information, but still requires a tool to present the countermeasures.

4.4.3 Preparation

The tool itself does not require any preparation, but does assume the user is aware of all systems that should be entered into the tool. The onus lies on the user to nominate which systems are to be assessed and gain the assessment skill beforehand as well.

4.4.4 Implementation

Implementation of CRAMM V Express does not take place per se, as the use of the tool takes very little time, but no guidance is offered on when or how the proposed mitigating controls are to be implemented. The onus again lies on the user to make those decisions. The use of the tool is also dependent on the single user, as it does not push the user to use it; instead it remains on a shelf.

4.4.5 Cost

The CRAMM V Express tool is available at a cost of £1 500,00 excluding tax, with an additional annual licensing fee of £250,00. In rands, this translates to a purchase cost of R17 205,00[12] excluding tax, and R2 867,50 per year for licensing.

This is not an extremely large sum of money, but may be contested if the tool is not used to its full potential. The risk of investing the purchase cost with no return on the investment is high [KARA 2005]. It is, however, fast to use and does not have a high cost in organisational involvement.

CRAMM V Express has scored below average and has failed in the cost element. This is surprising as very little organisational involvement is required, although a purchase cost is attributed. The downfall is the lack of the requirement of senior management involvement. This has been stipulated by King II as well as CobiT as vital, which also supports the low regulatory score.

[12] Calculated at the rate of R11,47 per pound as at October 2005.

The high score in SMME fit is inconclusive, as CRAMM V Express is not specifically tailor-made for small businesses, but neither does it exclude them.

4.4.6 CRAMM V Express Evaluation Outcomes

Table 4.4: CRAMM V Express framework evaluation

Elements, Factors and Subfactors	Score Achieved
Visibility	**20**
Promotional information is freely available with details for further information	10
SCORE	**10**
Cost	**40**
Purchase cost	
CRAMM V Express has a cost attributed to a tool	5
Organisational involvement	
Knowledge requirement	
The organisation is expected to already have all knowledge required for the undertaking	
Senior management buy-in	
The undertaking's methodology does not require senior management buy-in	
Self-directed or consulted	
The undertaking is self-directed	5
SCORE	**10**
GO/NO-GO DECISION: IS THE COST TOO HIGH?	
Regulatory Fit	**20**
CRAMM V Express does not conform to the steps in Table 3.4 at all	
CRAMM V Express promotes reviewing by offering a record of countermeasures used and still to be implemented	10
SCORE	**10**
SMME Fit	**20**
Horizontal/vertical	
The CRAMM V Express is not restricted to any industry	5
Size	
CRAMM V Express has no restrictions on organisational size at all	10
Organisational type	
CRAMM V Express is not restrictive	5

	SCORE	**20**
	TOTAL	**50**

4.5 Advantages and Disadvantages of OCTAVE-S and CRAMM V Express

This section is used to highlight those features of both OCTAVE-S and CRAMM V Express that are advantageous for use by South African SMMEs, and those that are not.

The advantages and disadvantages are categorised according to those discoveries while evaluating the approaches for the framework outcomes. Advantages or disadvantages not covered by the framework, but that still have value, are also highlighted.

Table 4.5 presents the various advantages of both approaches, categorised by the framework elements and factors.

The advantages of the two approaches provide a structure that may form the ideal approach for an SMME, had the approach existed.

The conclusion may be made that although the above approaches may offer some benefits to South African SMMEs, there are risks that they become difficult to apply and are abandoned before completion. There is no support available for either of these approaches should the organisation grow weary of self-direction.

The portal has now been opened to create an approach that holds all the advantages listed in Table 4.5, but none of the disadvantages; such an approach that scores higher on the framework, if not the ultimate score of 100.

Table 4.5: Advantages and disadvantages of OCTAVE-S and CRAMM V Express

Framework	**OCTAVE-S**	**CRAMM V Express**
Visibility		
Advantages	The full implementation guide is available online, containing introductory information, preparation guidelines, worksheets and other documents.	A flash presentation presenting the uses of the CRAMM V Express tool is available to anyone that requests it.
Disadvantages		The presentation provides information on the function of the tool only, with no background of CRAMM. The user has no means to test the tool before making a purchase decision.
Cost		
Purchase cost		
Advantages	OCTAVE-S is completely free.	The cost of the tool has been greatly reduced from the full CRAMM V Expert version.
Disadvantages		The tool must be purchased for use and has no demo version available for testing beforehand.
Organisational involvement		
Advantages	OCTAVE-S is self-directed, and may be applied using the organisation's own discretion for schedules. OVTAVE-S insists on senior management involvement.	No human resources except the tool user are required to obtain results. The tool provides a dashboard against which the countermeasures may be listed that requires implementation.

Disadvantages	No external assistance is available for conducting OCTAVE-S successfully. Training is said to be available, although no institutions are recommended. Self-training is also recommended, assuming the organisation has the human resources at its disposal for this. The approach requires the creation of a mitigation plan, but does not include assigning resources to execution of this plan, only to the steps of the plan.	No senior management involvement is required or endorsed by CRAMM V Express. The tool may never be used effectively, and has no measure to control this. Knowledge of risk analysis is assumed by the tool and offers no training provision for those non-skilled users. The countermeasures dashboard is static unless the organisation applies the countermeasures and self-manages their management. This, again, requires training.
Regulatory Fit		
Advantages	OCTAVE-S has a well-structured preparatory process that encourages detailed planning before launching the undertaking. The 'arranging' phase of OCTAVE-S is split into three phases, which concludes in deliverables of next steps and plans, which have assigned resources.	CRAMM V Express offers the dashboard of implemented countermeasures that can be maintained with updates of implementations at any time.
Disadvantages	OCTAVE-S does not offer detail on monitoring the execution of the plans created, and does not create scope for reviews of the planned executions. There is thus no 'controlling' phase of the plans.	CRAMM V Express does not follow any procedural structure, nor does it allow the assigning of tasks to individuals or groups. The reviewing of implementation of countermeasures is self-driven, and appears easy to lapse.

SMME fit		
Horizontal/vertical		
Advantages	OCTAVE-S offers no restrictions.	CRAMM V Express offers no restrictions. It was created for reduced cost and time requirements.
Disadvantages		CRAMM V Express offers no restrictions, and is thus not tailor-made for SMMEs.
Size		
Advantages	OCTAVE-S was specifically created for the small business and is much simplified from the original OCTAVE approach.	CRAMM V Express offers no restrictions. It was created for reduced cost and time requirements.
Disadvantages	OCTAVE-S restricts implementation to a specific size range which excludes 91% of South African SMMEs.	CRAMM V Express offers no restrictions, and is thus not tailor-made for SMMEs.
Organisational type		
Advantages	OCTAVE-S was created for an enterprise with multitasking, interdisciplinary staff, which is characteristic of many SMMEs.	CRAMM V Express offers no restrictions. It was created for reduced cost and time requirements.
Disadvantages	OCTAVE-S was designed with a flat hierarchical, interdisciplinary structure in mind. It excludes those enterprises with independent business units, or non-interdisciplinary staff members.	CRAMM V Express offers no restrictions, and is thus not tailor-made for SMMEs.

4.6 Conclusion

This chapter has presented a framework that may be used to evaluate any undertaking by an SMME concerned with developing, protecting or auditing the business. The framework is three-dimensional, providing a quantitative scoring system for evaluating an undertaking. The three dimensions are element, factor and weight. The factor dimension is in some cases split into subfactors.

The first objective was achieved by applying this framework to the arena of ISRM, specifically evaluating OCTAVE-S and CRAMM V Express.

The framework evaluated each approach in terms of availability, cost, regulatory fit and SMME fit. The framework has found that neither of these approaches is ideal for South African SMMEs, with mediocre scores of 65% and 50%, respectively.

It was also found that the advantages and disadvantages of each are not in favour of South African SMMEs, which led to the conclusion, and achievement of the second objective, that application of the approaches is not recommended.

An outcome of these evaluations was the realisation that a new, South African SMME aimed approach needs to be developed that encompasses the advantages of both, but not the disadvantages of either, and that scores high on the evaluation framework.

The requirements of such an approach, considering the framework requirements as well as international security standards, are presented in Chapter 5.

5 Requirements of Information Security Risk Management for an SMME

5.1 Introduction

The previous chapter revealed that ISRM methodology created for small businesses is not necessarily congruent with the requirements of South African SMMEs.

A South African SMME, with its unique structure and economic placement in South Africa, requires a methodology created to suit its unique structures and requirements for low resource and cost, as well as the requirements of corporate governance and subsequently IT governance. A fourth requirement is that of the international information security standard. Compliance with corporate and IT governance cannot ignore compliance with security standards.

This chapter's primary objective is the identification of the requirements of all of the abovementioned. The goals for this objective are:

1. The requirements of an SMME
2. The requirements of corporate governance
3. The requirements of IT governance
4. The requirements of the information security standard

The second objective is to amalgamate the above and include the advantages of the ISRM methodologies evaluated in Chapter 4. The goals of this objective are:

1. A list of requirements
2. The advantages identified in Chapter 4 added to the list of requirements
3. A structure including both the requirements and advantages

The structure including requirements and advantages is used for the creation of an ISRM methodology that may be used by an SMME in South Africa.

The third objective is the identification of measures and weights for the requirements.

The requirements of the SMME as identified in Chapter 4 are summarised first, following by listings of further requirements.

5.2 SMME Requirements

The requirements of an SMME centre on the structure of the SMME. The requirements are as follows:

S1 Horizontal or vertical industry. The SMME may be from any industry.

S2 The size of organisation. The SMME's size may range from 1 staff member to 200.

S3 The type of organisation. Any structure or hierarchy is acceptable.

The next goal is the identification of the requirements of corporate governance.

5.3 Corporate Governance Requirements

The corporate governance standard applicable to South Africa is the King II standard. This standard has been evaluated for use by SMMEs, and a proposed simplified structure was presented in Chapter 3.

King II is now presented in further detail, specifically relating to the risk management of corporate governance included in the standard. The corporate governance of risk management in the standard was created for all principles of risk faced by the organisation, including those of business continuity and technology.

The corporate governance requirements of risk management are thus presented in the context of business continuity and technology, as information security is included in this grouping.

The requirements of corporate governance are divided into the following:

- Global requirements. These requirements do not apply to any specific step in the risk management process, but are applicable to the management of the process and the selection of the methodology.

- Process requirements. These requirements apply to specific elements of the steps of the risk management process.

The requirements are expressed in relation to SMMEs based on the contents of the King II Report.

5.3.1 Global Requirements

Global requirements are divided into requirements of stakeholders that hold responsibility or accountability for the requirements, as well as the required environment for risk management. The distinction of accountability and responsibility is explained in Appendix 1.

The responsibility and accountability of stakeholders in the risk management process are divided between the board and senior management. The board is ultimately responsible for the entire process, but may hold senior management accountable.

5.3.1.1 Requirements of the Board

The required responsibilities of the board of an SMME are [KING 2002] [CLIF 2004]:

K1.1 Deciding on the organisation's appetite for risk. The level of acceptable or unacceptable risk is identified.

K1.2 Implementation of risk identification, risk impact measurement and proactive management of risk.

K1.3 Inclusion of day-to-day activities of risk management in the organisation.

K1.4 Use of recognised models for risk management. This responsibility may be interpreted as a model compliant with the requirements of this standard for this study, as it has been found that existing models are not necessarily applicable to SMMEs.

K1.5 Maintaining an up-to-date register of key risks, including their estimated financial impacts if realised.

5.3.1.2 Requirements of Senior Management

The required accountability of senior management of an SMME is [KING 2002] [CLIF 2004]:

K2.1 Design, implementation and monitoring of risk management. Although senior management is accountable for implementing risk management, the board is ultimately responsible for it.

K2.2 Ensuring the implementation of risk management is a team-based approach. No single person may be tasked with risk management. A group of members of senior management must implement risk management.

K2.3 A board-appointed committee of directors and senior managers evaluates risk. The operational execution of the evaluation is led by directors and managers, but must not exclude other staff.

K2.4 Effective and continuous monitoring of risks. Senior management are expected to generate reviewed reports of risk monitoring on an annual basis.

5.3.1.3 Requirements of the Environment

King II requires that the following be considered for the environment (organisation) in which risk management is conducted [KING 2002] [CLIF 2004]:

K3.1 Identify the control environment. The environment in which risks are managed must be identified before the process is started. This is the organisational culture, objectives, values and competency of staff.

K3.2 Assess risk related to organisational objectives. The risk assessment process should also consider risks that are significant to the achievement of the organisation's objectives. The risk assessment must be undertaken annually, but management of risks must be undertaken continually.

K3.3 Design control activities to respond to risks throughout the organisation and outside of it. They should enhance the environment.

K3.4 Information and communication. Information gathered by risk identification and assessment should be communicated to the organisation in a method suitable to the culture. It should also be communicated in a time frame that enables staff to continue with their responsibilities. Management's intent for managing risks must be understood by all staff.

K3.5 Evaluate the monitoring of risks against a set of key performance indicators extracted from the organisation's objectives.

K3.6 An effective system of continuity of critical business systems must disclose responses to significant risks should they occur.

5.3.2 Process Requirements

The process requirements of King II are listed next.

Risk Assessment Requirements of King II

King II prescribes risk assessment as a step in the process of risk management, and is required to include [KING 2002] [CLIF 2004]:

K4.1 A demonstrable system of risk identification.

K4.2 Estimated likelihood of the occurrence of a risk.

K4.3 Quantification of the impact of the risk. This includes estimated costs of significant losses, which may be material losses, loss in earnings or cash flows.

K4.4 Comparison to available benchmarks. No guidance is provided on which benchmarks may be used, or what is compared. This requirement therefore assumes that the final value of the risk is calculated using established methods.

K4.5 Recommendations should be made of how each risk should be managed.

Figure 5.1 presents these requirements in a process flow.

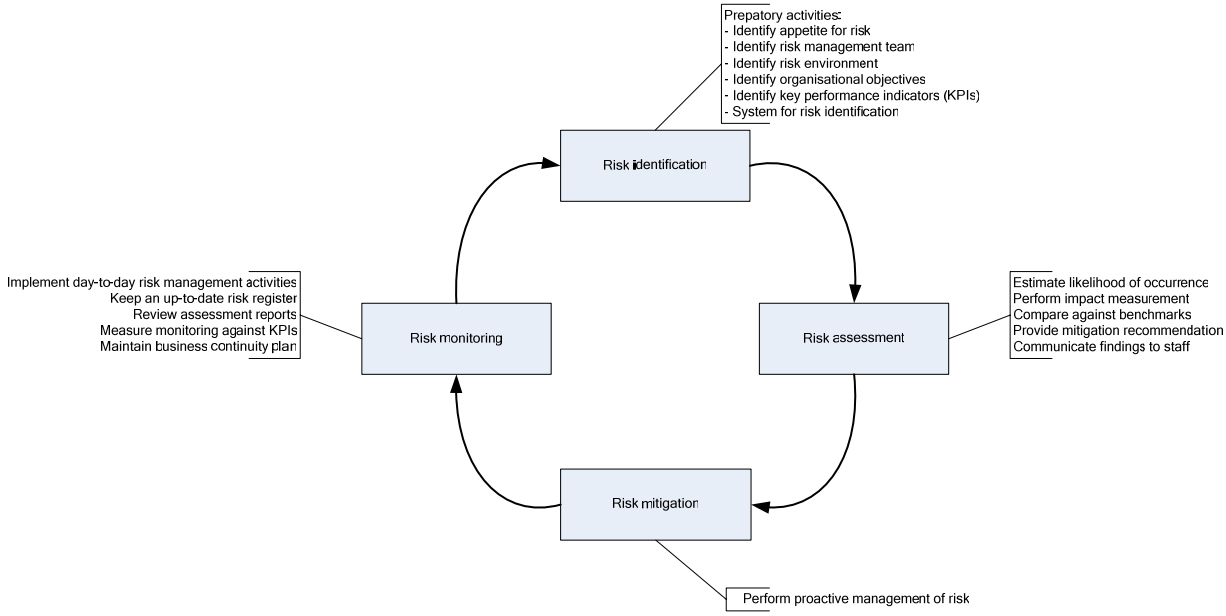


Figure 5.1: Corporate governance requirements for risk management [KING 2002] [CLIF 2004]

The requirements of King II may be expanded by the requirements of IT governance, as a subset of corporate governance. The requirements of CobiT are presented next.

5.4 IT Governance Requirements

IT governance is a continuous, cyclical process as was presented in Chapter 3, when the process of risk management required by King II was mapped to the domains of CobiT.

A control objective of CobiT, assess risks, is included in the planning and organisation domain, or step of IT governance. This control objective provides the following requirements of IT governance for risk assessment, as a step of risk management:

Risk Assessment Requirements of CobiT for an SMME

C1 Business risk assessment. Management is required to establish an assessment framework that is applied to all aspects and systems of the business or organisation, that is applied at regular intervals, and that is regularly updated with information from audits.

C2 Risk assessment approach. The approach adopted by management should allow scope of boundaries and assigning of responsibilities and required skills. Management should lead the decision of the mitigation solution identified after assessment and be involved in identification of risks.

C3 Risk identification. The essential elements of risk include:

a. Tangible and intangible assets

b. Asset value

c. Threats

d. Vulnerabilities

e. Safeguards or controls

f. Likelihood and consequences of threats

g. Qualitative and quantitative rating of risk

h. Business, regulatory, legal, technology, trading and human resources

C4 Risk measurement. The analysis of risk identification information should include quantitative and qualitative measures. Risk analysis forms part of risk assessment. The measurement of the risks thus falls into the risk assessment step in the risk management process.

C5 Risk action plan. A cost-effective risk action plan should be defined that ensures cost-effective controls and measures to mitigate exposure to risk on a continuing basis. The action plan should identify risk mitigation solutions as avoidance, termination, mitigation and transfer. The final option is acceptance, in which case the board is aware of the risk but cannot mitigate it. This applies especially to residual risk.

C6 Risk acceptance. Formal acceptance of residual risk should be documented and offset by adequate insurance.

C7 Safeguard selection. Controls that offer the highest return on investment and quick wins should be prioritised. Management is

required to communicate the purpose of the control and monitor the continued effectiveness.

C8 Risk assessment commitment. Management should encourage risk assessment as an important tool in the implementation of internal control, and include it in the strategic IT plan and monitoring mechanisms.

Figure 5.2 offers a summary of the requirements of CobiT.

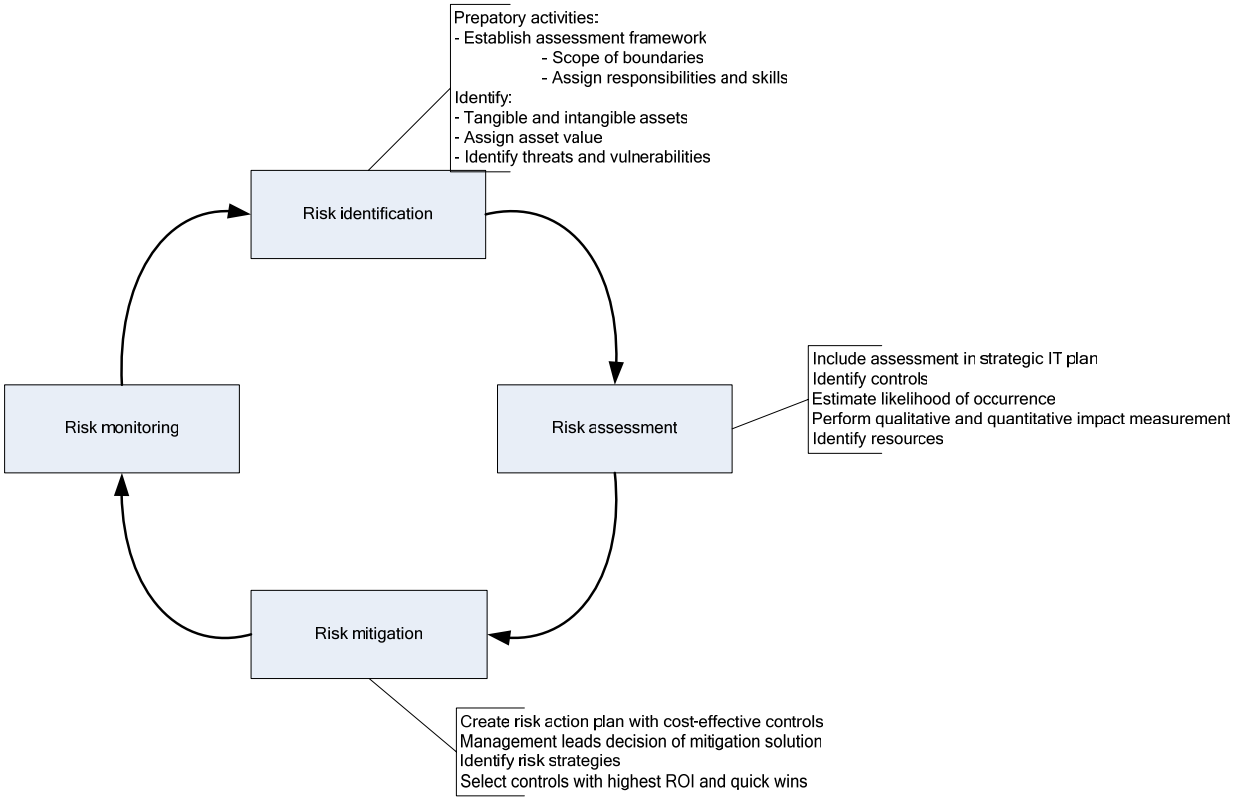


Figure 5.2: IT governance requirements of risk management [COBI01 2000]

The information security standard requirements are identified next to complete the requirements listing.

5.5 Information Security Standard Requirements

The internationally endorsed standard for information security management is the ISO 17799 standard [SABS 2000]. This standard was originally created by the British Standards Institute and was known as the BS 7799 [SABS 2000]. The International Organisation for Standards adopted it and distributed it as ISO 17799. The South African Bureau of Standards subsequently adopted it and dubbed it SABS ISO 17799 [SABS 2000]. Although the standard was

created for no specific size of organisation, it does hold value for the South African SMME. As the standard is also locally endorsed, it should be considered for its generic security content [SABS 2000]. The standard has a specific requirement for risk assessment as is presented in the next section.

Risk Assessment Requirements of ISO 17799

The following requirements are stated by ISO 17799 as the tasks required of risk assessment and management [BSI 2002]:

I1 Asset identification and valuation. All assets associated with the business environment are identified and evaluated against a value scale. This value scale is concerned with confidentiality, integrity and availability (CIA) and any other values deemed necessary.

I2 Security requirements identification. Identification of all threats and vulnerabilities of the assets listed.

I3 Security requirements assessment. Identification of a value scale for each of the security requirements identified. Assigning of the values.

I4 Calculation of risks based on the assets and security requirements.

I5 Identification and evaluation of options for treatment of risks. Identification of a suitable risk treatment action for each of the risks, that is both realistic and in line with business requirements. Document all results for the risk treatment plan.

I6 Selection of security controls, reducing the risk and risk acceptance. Determine the acceptable level of risk and ensure that the level is appropriate for the organisation. For those risks for which the option of risk reduction was selected, select suitable controls that reduce the risk to an acceptable level. A list of controls is provided by the standard.

Figure 5.3 summarises these requirements.

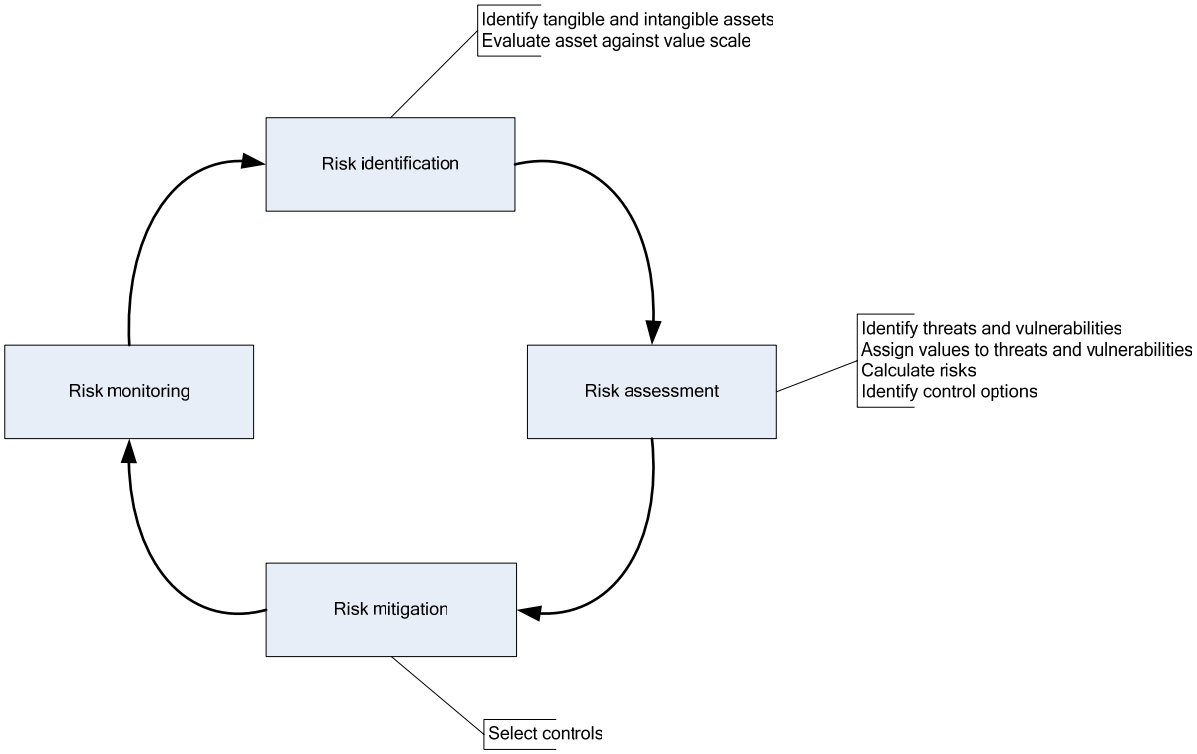


Figure 5.3: Information security standard requirements [BSI 2002]

All the requirements have been gathered and presented in separate groupings. The next section presents the full list of requirements and investigates any overlapping in the list.

5.6 Full List of Requirements and Requirements Matrix

The four sections listing requirements are now compounded into a single list of requirements, and mapped in a matrix (refer to Table 5.1) to determine whether there are any requirements that are duplicated.

The full list of requirements is as follows:

S1 Any industry

S2 1 to 200 staff size of organisation

S3 Any type of organisation

K1.1 Deciding on the organisation's appetite for risk

K1.2 Implementation of risk identification, risk impact measurement and proactive management of risk

K1.3	Inclusion of day-to-day activities of risk management in the organisation
K1.4	Use of recognised models for risk management
K1.5	Maintaining an up-to-date register of key risks
K2.1	Design, implementation and monitoring of risk management
K2.2	Ensuring the implementation of risk management is a team-based approach
K2.3	A board-appointed committee of directors and senior managers evaluates risk
K2.4	The operational execution of the evaluation must not exclude other staff
K2.5	Effective and continuous monitoring of risks
K3.1	Identify the control environment
K3.2	Assess risk related to organisational objectives
K3.3	Respond to risks throughout the organisation and outside of it
K3.4	Information and communication
K3.5	Evaluate monitoring of risks against a set of key performance indicators
K3.6	Disclose responses to significant risks should they occur
K4.1	System for risk identification
K4.2	Estimated likelihood of the occurrence of a risk
K4.3	Quantification of the impact of the risk
K4.4	Comparison to available benchmarks
K4.5	Make recommendations of how each risk should be managed and communicated

C1 Business risk assessment

C2 Scope of boundaries, assigning of responsibilities

C3 Risk identification

C4 Risk measurement

C5 Risk action plan

C6 Risk acceptance

C7 Safeguard selection

C8 Risk assessment commitment

I1 Asset identification and valuation

I2 Security requirements identification

I3 Security requirements assessment

I4 Calculation of risks

I5 Identification and evaluation of options for treatment of risks

I6 Selection of security controls, reducing the risk and risk acceptance

There are requirements that are very similar in nature, specifically between CobiT and ISO 17799. The matrix maps the requirements to the risk management process.

The matrix demonstrates that although corporate governance provides requirements throughout the entire process of risk management, IT governance and the security standard do not. The gap analysis is discussed next.

Table 5.1: The requirements matrix

	SMME	King	CobiT	ISO 17799
Preparation	Size Industry Structure	Appetite for risk Risk management team Objectives KPIs		
Identification		Environment System of risk identification	Scope of boundaries Responsibilities Tangible assets Intangible assets Assign asset value	Tangible assets Intangible assets Evaluate asset against value scale
Assessment		Likelihood of occurrence Impact measurement Communication to staff	Threats Vulnerabilities Assessment in IT plan Likelihood of occurrence Impact measurement Identify resources	Threats Vulnerabilities Calculate risks Identify controls

Mitigation		Proactive management	Action plan Mitigation solution Risk strategies Select controls	Select controls
Monitoring		Day-to-day activities Risk register Performance measurement Assessment reports Monitoring measurement Business continuity plan (BCP)		

5.7 Gap Analysis

The listing of requirements created by standards in place in information security in South Africa has created a gap when mapped to the ISRM process.

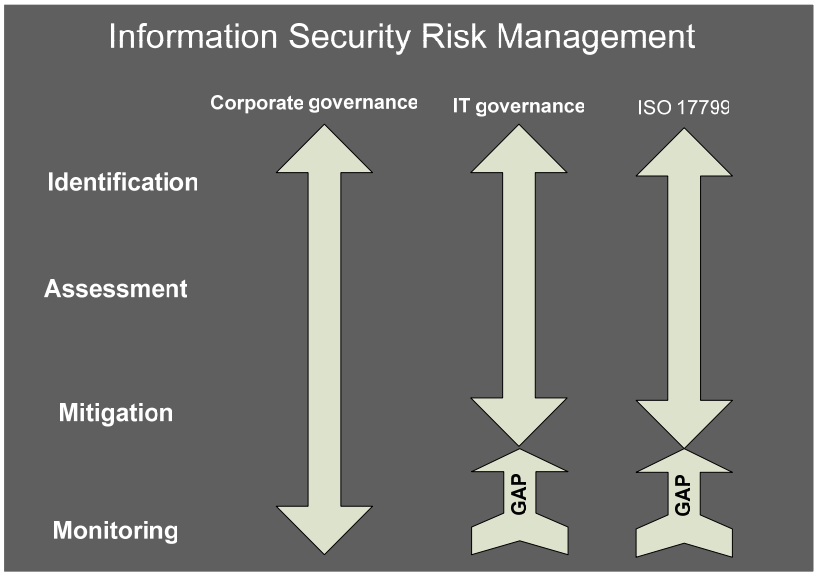


Figure 5.4: Gap analysis of standards requirements

Both IT governance and the security standard provide guidance on the selection of mitigating controls for risk, but offer no guidance on the implementation of the controls, or the subsequent continuity of the process, including monitoring of the risk profile for change.

The requirements of continuity and monitoring rely solely on corporate governance that is at a high level of generic requirements for any business risk. They do, however, offer good guidance and are accepted for the framework of requirements.

The last piece of the requirements puzzle is the inclusion of the advantages of OCTAVE-S and CRAMM V Express identified in Chapter 4. The required inclusions are listed below.

5.8 Required Inclusions in the Framework

The advantages and disadvantages of the two methodologies evaluated in Chapter 4 are amalgamated into a list of required inclusions in the requirements framework.

IF1 Implementation with organisation-approved schedules

IF2 Senior management involvement

IF3 Restriction of human resource involvement beyond minimum requirement

IF4 Dashboard for measurement of control implementation success (The dashboard may be updated at any time as the risk profile changes.)

IF5 Availability of training

IF6 Creation of mitigation plan with proposed use of resources required for execution

IF7 Detailed planning process before commencement of risk identification

IF8 Milestones achieved at the end of each step of the process that are required for the start of the next step

IF9 Review sessions during mitigation and monitoring phases to ensure control of schedules and mitigation

IF10 No restrictions on organisation structures or sizes within the SMME definition

The matrix is repeated to include these requirements (refer to Table 5.2):

Table 5.2: The requirements matrix with inclusions

	Previous Matrix List	**Inclusions**
Preparation	Size Industry Type Appetite for risk Risk management team Objectives KPIs	Type Size Senior management involvement Training Planning process
Identification	Environment/scope Responsibilities Tangible assets Intangible assets Evaluate assets against value scale	
Assessment	Threats Vulnerabilities Likelihood of occurrence Impact measurement Calculate risks Include in IT plan Identify resources	
Mitigation	Action plan Mitigation solution Risk strategies Select controls	Mitigation plan
Monitoring	Day-to-day activities Risk register Performance measurement Assessment reports Monitoring measurement BCP	Performance measurement

These inclusions and the requirements listed in previous sections are combined into a requirements framework.

5.9 The Requirements Framework for Information Security Risk Management of an SMME

The compounding of all the information presented in this chapter is presented first in the final list of requirements, and then in a diagram depicting the procedural steps with the requirements listed. Figure 5.5 presents the diagram. Measures and weights are assigned to the requirements in the section following thereafter.

1. Preparation

1.1 Confirm organisation is an SMME (size, industry, type) (S1, S2, S3)
1.2 Identify appetite for risk ((K1.1)
1.3 Risk management team (K2.2)
1.4 Objectives (K3.2)
1.5 KPIs (K3.5)
1.6 Senior management involvement (IF2)
1.7 Training (IF5)

2. Identification

2.1 Environment/scope (C2)
2.2 Responsibilities (C2)
2.3 Tangible and intangible assets (C3)
2.4 Evaluate assets against value scale (I1)

3. Assessment

3.1 Threats (I2)
3.2 Vulnerabilities (I2)
3.3 Likelihood of occurrence (C3)
3.4 Impact measurement (C3)
3.5 Calculate risks (I4)
3.6 Include in IT plan (distributed to staff) (C8)
3.7 Identify resources (C3)

3.8 Communicate findings to staff (C8)

4. Mitigation

4.1 Proactive management/action plan (K1.2)

4.2 Mitigation solution (C5)

4.3 Risk strategies (C5)

4.4 Select controls (C7)

5. Monitoring

5.1 Day-to-day activities (K1.3)

5.2 Risk register (K1.5)

5.3 Performance measurement (K3.4)

5.4 Assessment reports (K3.4)

5.5 Monitoring measurement (K3.5)

5.6 Business continuity plan (K3.6)

5.10 Measurement of Requirements

The list comprises 29 requirements. These requirements cannot carry equal weight in the creation of an ISRM approach for SMMEs as some steps are more important than others, e.g. identifying risks is more important than identifying key performance indicators. Each requirement is important though, and is thus included.

The measurement of each requirement and the subsequent weights are presented in Table 5.3. Each step in the risk management process is assigned a weight for achieving the milestone that is the completion of all requirements within the step. The final step, risk monitoring, presents the highest weight as it is most often neglected, as shown in the gap analysis.

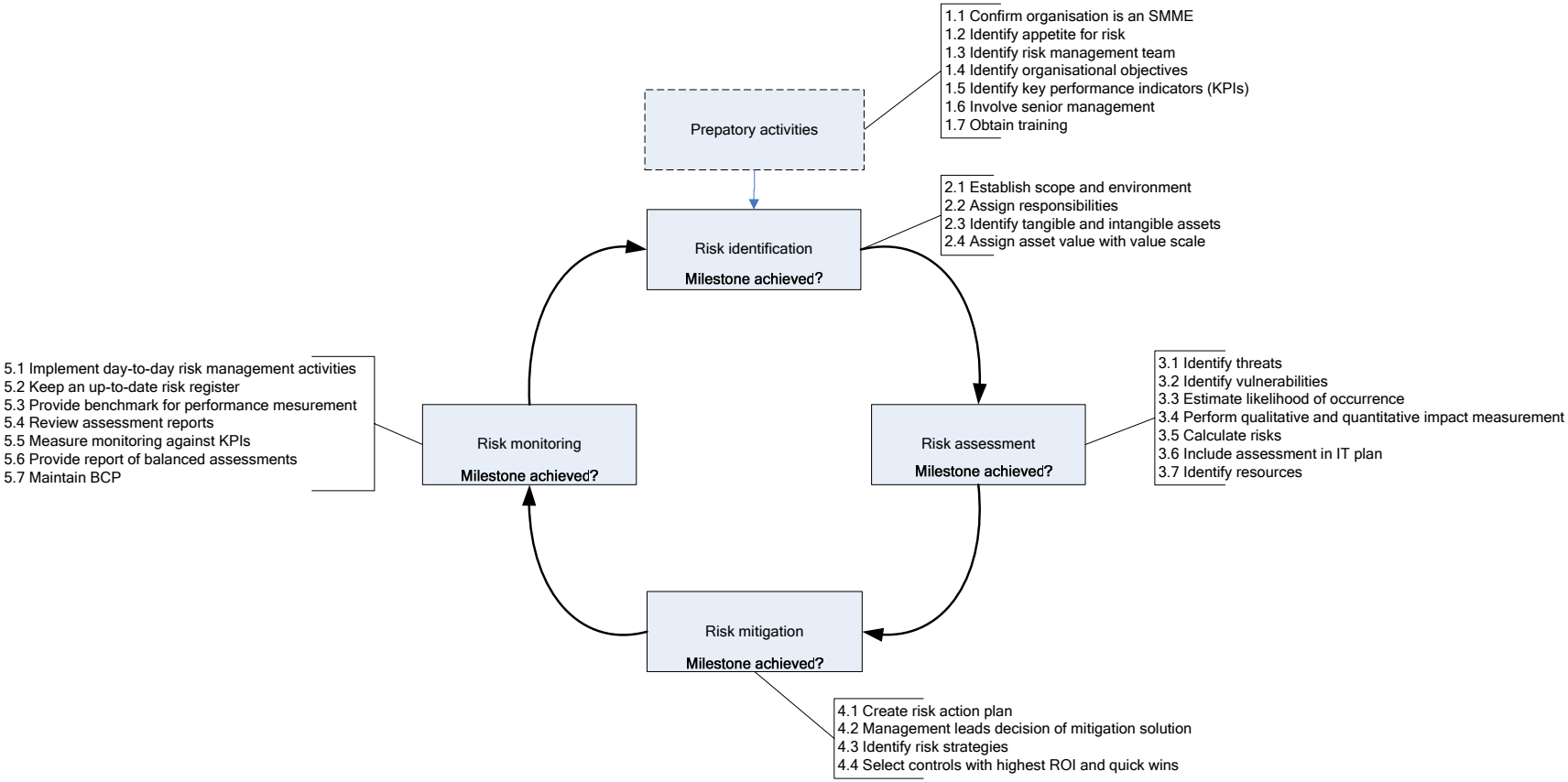


Figure 5.5: The requirements framework

Table 5.3: Requirements, measures and weights

Requirement	Measure	Weight
Preparatory Activities	**Milestone Achieved**	**20**
SMME	The methodology is fit for an organisation between 1 and 200 staff in size[13]	2
Identify appetite for risk	Formal statement from the board of the risk value that is acceptable	3
Identify risk management team	Team comprising senior management and staff	3
Identify objectives	List of primary organisational objectives	1
Identify key performance indicators	List of key performance indicators	2
Involve senior management	Responsibility of process assigned to high authority (either board member or senior member of staff)	5
Obtain training	Trained team	4
Risk Identification	**Milestone Achieved**	**15**
Identify risk environment	Statement of organisation/part of organisation for which methodology is applied	3
Assign responsibilities and skills	Documented list of responsibilities	2
Identify assets	Asset register	5
Evaluate assets against value scale	Documented value scale Register completed with values	5
Risk Assessment	**Milestone Achieved**	**20**
Identify threats and vulnerabilities	Threats and vulnerabilities register	2

[13] This is the ultimate measure of the requirements list, although with a low weight. Non-compliance with this requirement is contrary to information security risk management for an SMME.

Estimate likelihood of occurrence	Register completed with qualitative likelihoods	4
Impact measurement	Register completed with qualitative measures	4
Calculate risks	Register completed with risk values	5
Requirement	**Measure**	**Weight**
Include in IT plan	Dates captured at each update Communication to staff	2
Identify resources	Resources list, controls list	3
Risk Mitigation	**Milestone Achieved**	**20**
Risk action plan	Action plan	5
Mitigation solution	Statement of solution selection	3
Risk strategies	Documented risk strategies	5
Select and apply controls	Controls mapped against register with dates for implementation	7
Risk Monitoring	**Milestone Achieved**	**25**
Day-to-day activities	Inclusion in employment policies	5
Up-to-date risk register	Dates captured at each update	5
Performance measurement	Review sessions	5
Report of assessments	Documentation	3
Measure monitoring	Score achieved on KPIs	4
Maintain BCP	Dates captured at each update	3

5.11 Conclusion

This chapter has completed the preparation for the creation of an ISRM methodology for South African SMMEs by creating a framework of requirements for the methodology.

The following objectives and goals have been achieved:

The first objective of identifying the requirements was achieved by identifying the requirements of:

- The SMME
- Corporate governance
- IT governance
- The information security standard

In the identification of these requirements, a gap was discovered in the governance of risk management. The only standard presenting requirements for the final step in the risk management process, risk monitoring, is King II, which is at a high level. This is a shortcoming of CobiT and ISO 17799.

The second objective was achieved by combining the requirements with the advantages of the methodologies evaluated in Chapter 4. Some overlapping requirements were combined into a framework of 29 requirements and presented in a process flow diagram allowing a global perspective of the requirements framework.

The third objective was achieved by listing the 29 requirements, and assigning measures and weights to them. This enhances the governance of the process in the methodology yet to be created, and is congruent with the requirement of performance measurement already included in the framework.

The framework creates a benchmark that is used to create a methodology compliant with the standards and the SMME. This methodology is called the Peculium Model and is described in Part 2.

Part 2: The Peculium Model

6 Preparation for Information Security Risk Management

6.1 Introduction

ISRM, as defined in Chapter 2, is a procedural process used to identify, assess, mitigate and monitor risks of the information assets of an organisation.

Many methodologies for ISRM exist across the world with recurring themes used in various aspects, such as risk identification methods and methods for analysing risks, both quantitatively and qualitatively.

It has been established in this dissertation that ISRM methodologies created for the small business market are not necessarily fit for South African SMMEs, which make up a major portion of the South African economy.

A framework of requirements is now in place that guides the creation of the Peculium Model. This Model conforms not only to international standards of risk management, but also to the requirements of the SMME.

The objective of this chapter is to introduce the first step of the Peculium Model based on the requirements framework, namely preparation for risk management. The subsequent chapters each introduce the next step in the Model, as listed below:

- Risk identification
- Risk assessment
- Risk mitigation
- Risk monitoring

The goals of the chapter that collectively achieve the methodology of the first step are as follows:

1. The method for confirming that the organisation is an SMME
2. The method of obtaining senior management involvement
3. The method for identifying the organisational objectives
4. The method for identifying the appetite for risk
5. The method for identifying the key performance indicators of the process
6. The method for selecting the risk management team
7. The method for training the risk management team
8. Checklists that ensure that all deliverables in the step are completed before proceeding to the next step, namely identification

The chapter is structured around the goals, except for the checklists, which are presented with each method as listed above. The chapter begins with a brief overview of preparation for risk management, after which the methods for each of the above are provided.

6.2 Overview of Preparation for Risk Management

Preparation for risk management has been moved from the standard risk management process of identification, assessment, mitigation and monitoring, as the tasks involved require emphasis as well as completion before the process may continue (refer to Figure 6.1). Preparation is thus the catalyst for the risk management process, but vital for completion before commencement of the process.

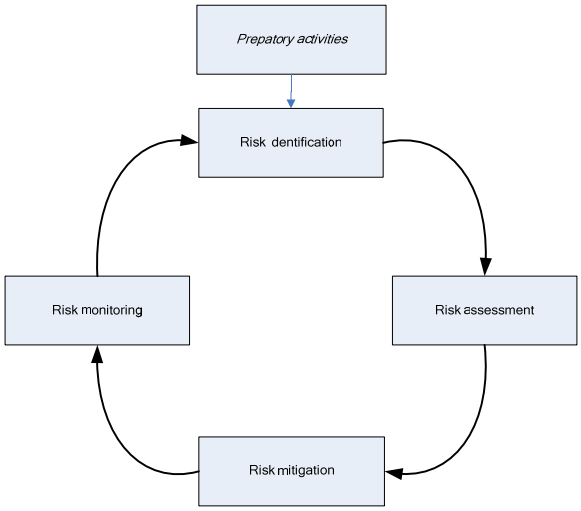


Figure 6.1: The risk management process with preparatory activities emphasised

The preparatory activities, as discovered in Chapter 5, stem mostly from corporate and IT governance. The establishment of the deliverables in preparation is used throughout the risk management process to finally complete the monitoring step and again prepare for the cycle's repetition.

The deliverables, previously noted as requirements for the preparatory activities, are as follows:

- Confirm the organisation is an SMME
- Obtain senior management involvement
- Identify organisational objectives
- Identify the appetite for risk
- Identify the key performance indicators
- Assemble the risk management team
- Conduct training

The deliverables have dependencies associated but do allow some concurrent activities to occur. The first activity, namely confirming the organisation is an SMME, has to be completed first. Thereafter, before any continuation of the process, the risk management sponsor as a senior member of management has to be identified.

This individual facilitates the remaining activities in this step. The sponsor leads the identification of objectives, the risk appetite and the key performance indicators. Finally the sponsor leads the selection of the risk management team and their training. The identification of the KPIs and the team are not dependent on previous activities and may occur concurrently. The training of the team is, however, dependent on their selection as denoted in Figure 6.2. The completion of all the deliverables constitutes the completion of the preparation milestone, as required by the requirements framework.

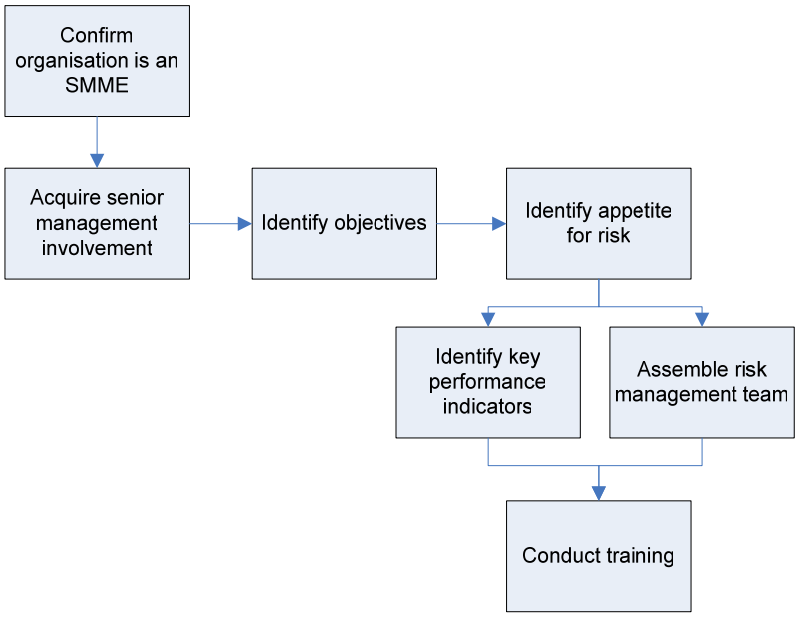


Figure 6.2: Completion of preparatory activities

6.3 Confirm the Organisation is an SMME

The most important deliverable of preparatory activities is the identification of whether the organisation in is fact an SMME. The methods and processes employed in this methodology for ISRM are based on a framework of requirements, again based on the environment of the SMME.

As defined in Chapter 2, SMMEs have staff numbers within the boundaries of 1 to 200. This includes all industries of organisations.

The organisation that applies the following steps and deliverables must be within the boundaries of staff supplied. An organisation that does not conform should reconsider the use of this methodology.

Checklist

The checklist for this deliverable asks only if the organisation does in fact have staff between the boundaries as specified (refer to Table 6.1). The checkbox must be checked before continuing to step two.

Table 6.1: Preparatory checklist 1

Preparatory Activities			
Step One		**Confirm organisation is an SMME**	
	1	Is the staff complement between 1 and 200?	☐

6.4 Obtain Senior Management Involvement

The involvement of senior management cannot only rely on the awareness and budgetary approval of the board or senior management forum. A senior management or board member should be elected as a sponsor for the risk management process.

In the case of corporate governance, this role is usually fulfilled through the financial manager or director, as the head of internal auditing [KING 2002]. This role, if available, should be used as the financial manager has reasonable understanding of budgetary constraints, and the skill of presenting financial data to the board or management forum.

6.4.1 Roles and Responsibilities of the Sponsor and the Board

The role of the sponsor in this process is as follows:

- Progress reporting to the board or senior management forum. Presentation of the KPI scorecard, assessment reports, asset register and risk register lies with the sponsor.

- Obtaining budget approval for the process. The sponsor is expected to present the requirements for budget and consequences of no budget to the board.
- Obtaining resource allocation for the process. The sponsor is also responsible for ensuring that the risk management team or any external resources required are available as and when stipulated.
- Management of schedule adherence. The sponsor is accountable to the board for completion of the risk management process within the period provided. As resources at an SMME are restricted, the scheduling of tasks and maintenance of the schedule become of utmost importance.
- Performance measurement. The sponsor is expected to maintain performance measurement during the process and to ensure that the presentation of performance to the board is favourable.
- Monitoring measurement. The sponsor is expected to measure whether risk monitoring is taking place and with due diligence.
- Communication to staff. The risk register, mitigating strategies and other available communication mechanisms should be communicated to staff to ensure risk awareness within the staff complement, as well as demonstration of risk mitigation.
- Selection of environment or scope for risk management. As dictated within the risk identification step, an environment for risk management must be identified. The sponsor is expected to motivate the selection to the board and staff.

The role of the board in this process is as follows:

- Receipt of progress reports from the sponsor as the process runs. The board is expected to evaluate the progress reports critically for approval or rejection.

- Decisions in support of mitigation strategies. Although the sponsor should have financial evaluation skills for determining the cost benefit of mitigating strategies, the board is finally responsible for the budget allocation.
- Call for completion of the process iteration and beginning of the next iteration of the risk management process. Risk management is a repetitive cyclical process that sees no end once started. There must, however, be a decision of when a new cycle of preparation will begin.

The sponsor should be made aware of his/her responsibilities in the risk management process and should provide a signature as proof of this.

6.4.2 Checklist

The checklist for this deliverable asks that the sponsor be identified, the roles and responsibilities explained and accepted (refer to Table 6.2). All checkboxes must be checked before continuing to step three.

Table 6.2: Preparatory checklist 2

Preparatory Activities			
Step Two		**Obtain senior management involvement**	
	1	Sponsor appointed by the board or management forum	☐
	2	Explain the sponsor roles and responsibilities to the sponsor	☐
	3	Sign off sponsor roles and responsibilities	☐

6.5 Identify Organisational Objectives

The objectives of the organisation determine the focus of the risk management process, as required by corporate governance. The objectives may, for example, focus on revenue generating business units, as opposed to overhead business units, such as an administration department. The objectives furthermore align the system, information and infrastructure assets with the environment determined for risk management.

The organisation may already have a list of objectives compiled. These objectives must, however, be reviewed and communicated to the risk

management team to empower their decisions later in the process. The team cannot be expected to have decisions supported without consulting the objectives.

If no list of objectives exists, one must be compiled by the board or senior management and communicated to the risk management team. This list of objectives articulates the driving factors for the business, such as increased revenue, improved customer service and development of staff. It is not the responsibility of the team or the sponsor to determine these objectives. The board should determine these objectives outside of the risk management process. Risk management is not the organisation's fix-all process for business processes that are lacking.

The SMME may use the following method in standardising the organisational objectives:

6.5.1 Standardising the Objectives

The King Report supports the use of the balanced scorecard for measurement of performance against objectives [KING 2002]. The balanced scorecard stems from the realignment of organisational objectives which in the past were mostly financial, to include perspectives of the customer, internal processes and learning and growth of the organisation [BALA 2002]. This scorecard, when used in its entirety, provides the organisation with a one-page status report of its financial performance, internal process successes, customer relationship strength, and knowledge and other development of its staff. The balanced scorecard in this dissertation is used in a simplified format as it is only used for standardising objectives, and not the full use of performance management.

The objectives should be structured into the balanced scorecard for ease of use in this process.

An example of standardising objectives for the balanced scorecard is as follows:

1. The risk management sponsor convenes the board.

2. The risk management sponsor explains the benefit of the balanced scorecard.
3. The risk management sponsor asks the board to elect at least one objective per perspective of the scorecard.

The balanced scorecard, when completed, should be similar to the example presented in Figure 6.3.

Balanced Scorecard	
Financial	Increase gross profit by 20%
Internal processes	Reduce order turnaround time to 5 days
Customer	Increase customer satisfaction survey score to 90%
Learning & growth	Encourage tertiary study among management staff

Figure 6.3: An example of the balanced scorecard

6.5.2 Checklist

The checklist for this deliverable asks that the balanced scorecard concept be explained to the board and the template completed (refer to Table 6.3). All checkboxes must be checked before continuing to step four.

Table 6.3: Preparatory checklist 3

Preparatory Activities		
Step Three	**Identify objectives**	
	1 Explain use of balanced scorecard for standardising objectives	☐
	2 Complete balanced scorecard	☐

6.6 Identify the appetite for risk

As corporate governance requires, an organisation must identify its appetite for risk before entering the risk management process. This applies to all types of risk management.

The appetite for risk is defined in monetary values. Appetite is the amount the organisation is willing to risk in a venture. In simpler terms, appetite is the worst case scenario loss that the organisation can endure. The appetite for risk is based on the organisation as a whole and is a business-driven decision.

The risk appetite amount is used later on in the process as a benchmark for decisions ranging from the risk valuation to mitigation and subsequently monitoring. The amount therefore requires careful consideration at the highest level of the organisation, preferably the board, or if not in place, senior management.

6.6.1 Determining the Appetite for Risk

The appetite for risk should be discussed at a senior management or board level forum. In the case of a micro enterprise with fewer than five staff members, the owner or senior manager may make the decision on his/her own.

The board or management forum should have the decision on appetite for risk included in the agenda to ensure that it receives recognition as an important item for the forum.

The board or management members must be made aware of the use of the appetite in later stages of the risk management process, and also assure the members that the risk management process is required by corporate and IT

governance, and may benefit the organisation with both improved information security and possibly a return on investment.

6.6.2 Selection of the Appetite Amount

The amount must be based on the worst case scenario loss that the organisation can endure. The organisation may base the amount on a percentage of net profit, percentage of assets owned or revenue for a period.

The amount is used later in the risk management process to measure impacts of a threat on the business, by comparing the projected monetary and productivity loss against this appetite identified.

The amount must be realistic and not purposefully low as this skews the risk assessment.

6.6.3 Checklist

The checklist for this deliverable asks that the appetite for risk be identified (refer to Table 6.4). All checkboxes must be checked to continue to step five.

Table 6.4: Preparatory checklist 4

Preparatory Activities		
Step Four	**Identify appetite for risk**	
1	Include risk appetite as an agenda item at the next meeting of the board	☐
2	Decide on appetite amount	☐

6.7 Identify Key Performance Indicators

The KPIs for any process or project determine the performance measurement for the process or project, and the support or rejection of the continuation of the process, or repetition of the project.

The KPIs are created before the process begins, and are determined by the board or senior management forum. They may be based on the milestones and deliverables of the process, the monetary resource requirement of the process, the completion of the process, or all of the above.

6.7.1 Minimum Required KPIs

The minimum required KPIs for this methodology are the completion of the deliverables required, as created through the requirements framework, and the subsequent achievement of the milestone at each step of the process as the deliverables are completed.

The minimum required list of KPIs is as follows:

- Achieve milestone at each step of the risk management process. Non-performance in this KPI should result in serious action by the board against the risk management team, as their assigned duties have not been completed.
- Complete each deliverable within the milestone at each step of the process. Each deliverable should carry documented proof of this, e.g. the balanced scorecard of objectives. Each deliverable should therefore be proven before the milestone may be marked as completed.
- Present milestone summary to the board or senior management forum at the end of each step. The risk management sponsor should present the progress of the risk management process to the board to ensure its continued support of the process and associated costs.
- Present the completed asset register at the end of risk identification. The asset register should be included in the annual report, if such a report is created, and at least presented to the board to ensure that it is aware of the assets owned by the organisation.
- Maintain the completed risk register at the end of each step. The risk register grows and develops through the process and has to be maintained. Each updated register must be communicated to the board.
- Communicate the completed risk strategies at the end of risk mitigation. The board must be made aware of the strategies employed for coping with the risks discovered and the motivations for them.

- Maintain the completed action plan. The highest valued risks must have an associated action plan that describes how the risk is mitigated. This action plan must be updated regularly with up-to-date progress of mitigation.
- Communicate the completed assessment report at the end of the risk monitoring step. The final assessment report articulates the cost and benefit of the entire risk management process.
- Maintain the updated business continuity plan at the end of each risk management cycle. Business continuity in the face of an exposed risk must be planned for and updated regularly.

This list is the minimum requirement of KPIs. The organisation may, however, add to the list if deemed necessary.

Performance against the KPIs must be updated at the end of each step of the process to ensure that information on the progress of the process is readily available. A scorecard system is presented in Chapter 10 to demonstrate the presentation of progress.

6.7.2 Checklist

The checklist for this deliverable asks that additional KPIs be added to the list if so desired, and the final list entered for the process (refer to Table 6.5). Number 1 is mandatory. Number 2 must be checked to continue to step six.

Table 6.5: Preparatory checklist 5

Preparatory Activities			
Step Five		**Identify KPIs**	
	1	Include additional KPIs to minimum required KPI list provided	☐
	2	Enter final KPI list	☐

6.8 Assemble the Risk Management Team

The risk management team may be assembled at the same sitting of the board or senior management as when the appetite for risk and KPIs are determined.

The team assembly should preferably be conducted with the consent of the individuals. If they are selected as a grudge responsibility, this may reduce commitment and loyalty to the risk management process and its completion.

The composition of the team should be representative of the organisation, including team members from most, if not all, business units. The first deliverable of risk identification, identify the environment, may exclude some business units. The team may be slightly adjusted at that stage.

6.8.1 Risk Management Team Size

The size of the team will differ in each organisation, as the number of business units and their size over a range of 1 to 200 staff members can vary greatly.

OCTAVE-S proposes using the methodology for organisations of staff of 20 and more, and having the team size at three to five members [OCTA02 2003]. This translates to an average of 15% of the staff complement.

OCTAVE-S also proposes up to three team members from any business unit involved in the process. This number may, however, become excessive in smaller organisations. As such, a minimum of one team member from every business unit involved in the process is recommended.

Using the 15% of staff scale, the team size for any SMME may be created using the following guide:

- Staff size fewer than 10: 2 team members
- Staff size between 11 and 30: 3 - 5 team members
- Staff size between 31 and 50: 6 – 8 team members
- Staff size between 51 and 100: 9 – 15 team members
- Staff size over 101: 11 – 20 team members

The size of the team is subject to decisions by the board or senior management forum.

The individuals selected to represent the business units should not be selected for availability, as most staff members will claim that they are not available, but rather knowledge of the business unit's functions, use of information, systems and infrastructure. Again, consent for participation should be obtained, if possible. Difficulties may arise from refusals to participate. The board must use its discretion in selecting team members that have the knowledge and the enthusiasm for participation.

The team members should be encouraged to participate and an incentive offered in return for their participation. The incentive should be performance-based to ensure that the required responsibilities are fulfilled to a high standard. A disciplinary process should be in place if a very low standard of performance is achieved.

6.8.2 Risk Management Team Roles and Responsibilities

The roles and responsibilities of the team members should be assigned at the discretion of the team sponsor. The sponsor should be able to determine which of the following roles are more suited to which team members:

- Asset identification. The team members are expected to identify the information assets in use in the environment for risk management.
- Evaluation of assets. The application of the identified assets to the value scale and subsequent prioritisation needs to be conducted.
- Identification of threats and vulnerabilities. Asset weaknesses and possible areas from which a threat may originate must be identified.
- Likelihood and impact measurement. The effect an exposure of a vulnerability or realisation of a threat may have on the asset needs to be calculated.
- Risk calculation. Threat, vulnerability, likelihood and impact information must be combined into a risk value that may be prioritised for mitigation.

- Proposal of mitigation solution. Best fit of mitigation solution to the risk considering the cost of mitigation and change management needs to be determined.
- Formulation of action plan. Steps that have to be taken to mitigate the risk must be determined.
- Implementation of controls. Installation or processing of controls or other mitigation solutions assigned must be handled.
- Maintenance of risk register and BCP. Regular updates to the risk register and BCP must be made as and when changes are required through the acquisition of new assets or implementation of controls.

6.8.3 Checklist

The checklist for this deliverable asks that the team be identified, the roles and responsibilities explained and accepted (refer to Table 6.6). All checkboxes must be checked before continuing to step seven.

Table 6.6: Preparatory checklist 6

Preparatory Activities		
Step Six	**Assemble risk management team**	
	1 Include team assembly as an agenda item at the next meeting of the board	☐
	2 Explain role of the risk management team and size	☐
	3 Elect risk management team	☐
	4 Obtain elected members' buy-in	☐

6.9 Conduct Training

The risk management team, although selected for their knowledge of their business units and the associated assets, cannot be expected to have knowledge of risks, risk management or any of the associated skill areas. It is therefore vital to prepare the team for the risk management process, and all the assessments and decision-making involved.

The risk management team should, after training, have full comprehension of the following:

- The risk management process, steps and substeps. The team must understand how each step leads to the next and what information in each step is required to complete the next. The team must understand the concepts of information security, identification, assessment, mitigation and monitoring.
- As is required for the board, the team must be aware of the schedule imposed on the process, and all the deliverables and milestones associated with the process.
- Analysis methods required for the substeps where applicable. The analysis methods used in the methodology are simplified for the SMME. The team is, however, still expected to comprehend the analysis required and complete the assessments.

An assessment should be performed on the team before training is provided to determine the level of knowledge. As SMMEs face restrictions of time resources, time should not be wasted on training team members that do not require the training.

The risk management sponsor may also decide to opt for Just-In-Time (JIT) training at the inception of each step. There are advantages and disadvantages to both training methods (refer to Table 6.7).

Table 6.7: Advantages and disadvantages of training methods

	Advantage	Disadvantage
Full training in preparatory activities	The team has full awareness of the extent of the process, and understands the quality required of each step before continuing to the next.	The knowledge gained in training may fade after the first few steps, causing insecurity in the remaining steps of the process.
JIT training	The knowledge required for each step is fresh in the mind of the team member when the step begins, thus ensuring that the correct methods are applied.	The team member is not in a forward-thinking process, but in a compartmentalised method that may reduce the quality of the output of the steps.

Both training methods provide challenges that may be resolved in a combination of the two. The suggested training method is a full course in the preparatory activities, with a refresher course before each step commences to ensure that the team members have full recollection of the methods employed in the step. This ensures that the team members have an understanding of what is required in the next step, but with full cognisance of the current step's requirements.

It is recognised that SMMEs are resource restricted and may not agree with the commitment of resources to this much training. It should, however, be emphasised that the training is not wasted, but that the added benefit of risk awareness and buy-in of staff into risk management may present greater benefits to the organisation outside of the actual process. The training of the team is not a nice-to-have, but a necessity.

An assessment should be performed after the full training course to ensure that the team members are prepared to commence the next step in the process.

These steps are to be completed before risk identification commences. Risk identification should start immediately after completion of preparation whilst the training is still recent.

Checklist

The checklist for this deliverable asks that the team be trained and assessed to ensure that all members are at the same level of knowledge as required for the process (refer to Table 6.8). All checkboxes must be checked before continuing to risk identification.

Table 6.8: Preparatory checklist 7

Preparatory Activities			
Step Seven		**Conduct training**	
	1	Provide the required training to the risk management team	☐
	2	Assess the team to ensure that it is prepared for the process	☐

6.10 Conclusion

This chapter has demonstrated the deliverables required of the preparatory activities for risk management. The chapter has shown that the board enjoys great involvement in the preparation for risk management, as is required by corporate governance.

The goals of the chapter required the methods of the steps in the process to be provided. These are summarised below.

The chapter has provided the necessary guidance in determining the organisation as an SMME, and selecting the sponsor for leadership in the process. The roles of the sponsor and the board were also provided.

The balanced scorecard has been proposed as a tool for standardising organisational objectives in a simple format for use by the risk management team.

The organisation's risk character has been defined, which may act as a catalyst for a higher quality selection of appetite for risk. The use of key performance indicators has also been introduced to the risk management process as the performance management system.

The role of the team has been defined, as well as the selection of the team size for the organisation. Finally, a training strategy has been presented, using both full training and refresher training for best results.

The goals of presenting the deliverables and achievement of them, as well as the checklists to be used as proof of completion have thus been achieved. Completion of the preparatory activities should empower the risk management team to conduct the risk management process, and allow the risk management sponsor to communicate the achievements of the process to the board.

The next chapter demonstrates the deliverables required for risk identification.

7 Risk Identification

7.1 Introduction

The identification step in the risk management process is concerned with the identification of assets and valuing of these assets in order to prioritise them for risk assessment.

This chapter shows the procedure involved in identifying the information assets, and their subsequent valuation.

In the previous chapter, the requirement of identification of the environment for risk management was pointed out. This environment, when identified in this chapter, also determines the duration of the risk management process and the resources required.

The objective of the chapter is to gather enough information about the assets to perform the assessments in the next step of the Peculium Model.

The goals of this chapter are thus:

1. The method for identifying the environment in which risks are identified, assessed, mitigated and monitored
2. The method for distributing responsibilities for the process to the risk management team in the identified environment
3. The method for identifying the information assets in the environment
4. The method for prioritising assets based on their information security weakness value

The goals are based on the deliverables of the identification step in risk management, as defined in the requirements framework of Chapter 5.

The final goal for the chapter is to present the checklists for ensuring completion of all deliverables before advancing to the assessment step in the process. The collective achievement of the goals achieves the objective.

7.2 Overview of Risk Identification

The King Report states that each execution of a risk management process must have a system for risk identification [KING 2002]. The IT governance standard, CobiT, allows for guidance in this instance by requiring the identification of both tangible and intangible assets and then assigning each a value [COBI02 2000]. The difference between tangible and intangible, in the case of information security, is the separation between system and infrastructure as tangible, and information, or data, as intangible.

The reason for this distinction is that the data contained within the system and infrastructure, although processed, stored and accessed through the tangible assets, has value within itself, which is not as readily replaceable as a system or hardware item.

Therefore, in this system for risk identification, tangible information assets, or tangible assets in shorter form, are system and infrastructure, representing hardware and networks. Intangible information assets (or intangible assets) represent that data stored on the hardware, processed by the system and accessed through the infrastructure.

However, before identifying these assets, the risk management team must determine the environment in which the assets require identification, and confirm the responsibilities of the members of the team for identifying the assets.

The chapter now continues with the presentation of the deliverables of risk identification. As with preparation, all deliverables for identification must be completed before continuing with the assessment of the identified assets (refer to Figure 6.1).

The deliverables of risk identification are:

- The identified environment
- Distributed responsibilities of the risk management team
- Identified tangible and intangible assets
- Asset weakness values

These deliverables are in a distinct order and may not be completed concurrently, or out of sequence. Each deliverable must be completed before commencing the next, as displayed in Figure 7.1.

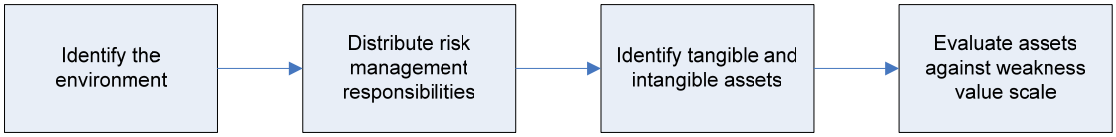


Figure 7.1: Order of completion of deliverables

7.3 Identify the Environment

Identification of the environment is very important to the SMME owner due to the constraints of time and resources present in the small business environment. The risk management sponsor must be aware of the implications of a full-scale risk management process applied to the whole organisation, as well as the benefits the organisation may reap from the process.

In the case of a micro enterprise, it is recommended that the whole organisation be risk managed. However, in the case of an upper level small or medium enterprise, the business units facing the greater risks or holding the higher value assets should be targeted for a first iteration, and other business units scheduled for a later iteration.

The challenge of identifying the environment before knowing the risk or asset values does, however, face the sponsor. The sponsor is expected to make a justified decision on the environment for board approval without the justifying information.

In the case of a repetition of the risk management process, this challenge is removed, as a previously unassessed environment is selected, or the same environment is assessed again to determine a reduction or increase in risk.

7.3.1 Information to make Decisions

In a new environment for risk management, it is not that simple. In this case, the sponsor must use information already available to make an informed decision on the selection of the environment. This information may come in many forms:

- The environment is requested by the board for the risk management process. This is the easier option as the sponsor is handed the environment. This request may stem from an adoption of corporate governance and the requirement for risk management.
- The organisation has suffered an exposure and subsequent loss in business units, or as a whole. In this case, the organisation has experienced the cost of an exposed risk, and this has catalysed the requirement of analysing all risk and having improved protection should another attack occur. An example of such an attack is a virus attack causing a lack of productivity in the sales department.
- The organisation has been made aware of a similar enterprise suffering a loss and is willing to make the investment in risk management in order to be better prepared in the same situation.
- A business unit or the whole of the organisation suspects untoward action by staff and wishes to reduce the risks facing their assets from internal attacks.

There may be various other sources of information in determining the environment. What is, however, important is that the selection of a poor environment does not bring the process of risk management into disfavour with the board as a high-cost waste of time. In other words, selecting a business unit with no assets of great value and no identifiable threats as a “test run” is not recommended.

7.3.2 Checklist

The checklist for this deliverable asks that the environment be identified, approved and documented (refer to Table 7.1).

Table 7.1: Identification checklist 1

Identification Activities			
Step One		**Identify the environment/scope of risk management**	
	1	Identify business units	☐
	2	Identify environment	☐
	3	Approve identified environment	☐
	4	Document environment	☐

Risk Management Environment
Business units/departments/divisions included in environment:

7.4 Distribute Risk Management Responsibilities

Some risk management responsibilities were listed in Chapter 6. Not all team members are expected to perform the same tasks. For example, a team member very familiar with technology or systems may be more suited to identifying assets, whereas a more analytical team member may be more suited to assessing the risks identified.

The same applies in the case of the environment; not all team members originally identified may have knowledge of the environment that is planned for assessment. The discretion lies with the sponsor whether all team members should remain in the team based on their qualities or skills, or whether only staff in the affected business units need remain. The appropriateness of identifying the environment after the team is questionable. This is, however, required as in the requirements framework. For the purposes of this dissertation it remains in this step of the process.

It is important that the temptation of too few team members not lead the sponsor into overloading the team members. The temptation may arise from the uncomfortable restriction on resources of the staff members to assist in the process. The focus must remain on the importance of conducting the process with due diligence.

The requirement of external resources may also be faced by the sponsor. These external resources are not necessarily external to the enterprise, but may be staff members not included in the team. The use of hired external resources is, however, a cost to the enterprise and should be considered carefully before decisions are made.

Checklist

The checklist for this deliverable asks that the originally selected team members be verified for the environment and responsibilities determined, distributed and documented (refer to Table 7.2). All checkboxes must be checked before continuing to step three.

Table 7.2: Identification checklist 2

Identification Activities		
Step Two	**Distribute responsibilities**	
	1 Verify team members	☐
	2 Determine responsibilities	☐
	3 Assign responsibilities to the team members	☐
	4 Document assigned responsibilities	☐
Team Responsibilities		
Team member	**Responsibilities**	

7.5 Identify Tangible and Intangible Assets

In this deliverable of the identification step, the first document that is presented to the board at regular intervals is created. The information asset register provides the board or senior management forum with a list of the systems, infrastructure and information in the possession of the organisation, or if the environment is restricted, in the environment targeted.

The organisation does have the opportunity to identify all assets used across all business units; in fact, it should be aware of all assets in place. The risk management team is, however, restricted by set schedules and budgets, and should not be used as a 'nice-to-have' team to gather information it does not require to complete its function.

7.5.1 Creating the List of Assets

The asset list is created by listing the assets as systems, information or infrastructure.

- Systems are products or applications that process the information for the user, such as presenting financial figures in a structured report. Systems are either off-the-shelf products or custom developed. Systems may also be integration groups of systems that offer a synergistic benefit. Such a system group must also be seen as a separate asset. Such integrated systems usually require the intervention of a developer to return to full functionality.
- Information is the data that is generated, accessed or stored by the system. The data is unique in any enterprise and cannot be replaced by an off-the-shelf purchase.
- Infrastructure includes the hardware, networks, input and output devices used to access or process information through a system. Infrastructure is usually replaceable at a cost, but requires installation by a skilled IT technician.

7.5.2 Creating the Asset Register

The asset register is not a simple list of assets, but in fact provides a more detailed image of the asset for the board. The asset register does contain the asset list, but also stores properties of the asset.

- An asset may be used across an enterprise and by various business units. However, a primary business unit must take ownership of the asset.
- The access route to the asset must also be determined, for example a specific pocket of data is facilitated by a server and a system. The asset register must list both the server that stores the information and the system through which it is viewed.
- The users of the asset must be listed. Most attacks on assets are by the hand of staff. As such, the users that access the asset must be listed.
- The security requirements of the asset may be any or all of the following:
    - Confidentiality of the asset is a security requirement if the asset is a proprietary system of great value, or sensitive data.
    - Integrity of the asset is a security requirement if the accuracy of the asset is of great value, e.g. the accuracy of salaries.
    - Availability of the asset is a security requirement as the lack thereof may cause a damaging loss to productivity.

With the asset register completed for the environment, the board is presented with the first valuable information because of the risk management process. The board now has access to the list of assets with confidentiality requirements, those assets that require integrity and lastly those assets that offer productivity.

The asset register is used further in the next step where weakness values are assigned to the assets based on their security requirements.

7.5.3 Checklist

The checklist for this deliverable asks that the assets be identified and added to the asset register with the associated properties (refer to Table 7.3).

Table 7.3: Identification checklist 3

Identification Activities			
Step Three		**Identify assets**	
	1	Create list of all systems, information, hardware and infrastructure	☐
	2	Complete asset register with properties	☐

7.5.4 Asset Register

The asset register as shown below provides an at-a-glance list of the assets in the environment with their properties identified (refer to Table 6.2). This is the first version of the asset register, which develops throughout this step in the process.

Table 7.4: Asset register 1

Asset Register					
		Properties			
Asset		**Business Unit**	**Access Route**	**Users**	**CIA**

7.6 Evaluate Assets against Weakness Value Scale

The assets identified in the previous deliverable may become a lengthy list of assets of indeterminate value. For this reason assets are valued for weakness to assist the selection of assets for which the risk assessment is performed.

This is a vital step for SMMEs as the cost of assessing all assets for risk may be too expensive an exercise for their resources to conduct.

The weakness valuation of the assets is based on the security requirements determined for the assets and captured in the asset register. The monetary replacement or purchase cost of asset is not considered, as its weakness value goes beyond its price tag.

7.6.1 Asset Valuation System

The system for valuing the assets is as follows:

- Each of the security requirements has equal weight in the system. In other words, if two security requirements apply, each carries a weight of 50%. If all three apply, each carries a weight of 33.3%.
- Each security requirement poses challenges to the asset to determine its strength against the security requirements.
- Values are awarded based on the lack of strength, or presence of weakness. As such, the higher the weakness value of the asset, the more crucial its risk assessment and subsequent mitigation of the risk.

The asset register must be updated with the weakness values assigned to the assets, and reordered according to highest weakness value. Those assets rated with the highest weakness value are then presented to the board for selection for risk assessment. The board makes the decision on the number of assets to select. In the case of low weakness valued assets, a smaller amount may be selected for assessment. A low weakness valued asset is valued lower than 30%.

7.6.2 Checklist

The checklist for this deliverable asks that the weakness values be calculated and stored in the register. The register is then ordered according to highest weakness value and the selected assets for risk assessment identified by the board (refer to Table 7.5). All checkboxes must be checked before continuing to step five.

Table 7.5: Identification checklist 4

Identification Activities			
Step Four		**Evaluate assets against weakness value scale**	
	1	Calculate weakness values	☐
	2	Capture weakness values to asset register	☐
	3	Reorder register according to weakness value	☐
	4	Identify highest weakness value assets	☐

7.6.3 Asset Register

The asset register is updated to include the weakness value and is reordered according to highest weakness value. The categories identified earlier now become properties (refer to Table 7.6).

Table 7.6: Asset register 2

Asset Register					
		Properties			
Asset	**Business Unit**	**Interacts with**	**Users**	**CIA**	**Weakness Value**

7.6.4 Weakness Value Calculation

The calculation of the weakness value is dependent on the security requirements that apply. Each security requirement offers challenges to the asset, with a score of 5 assigned to a “Yes” or “No” answer, depending on the resulting weakness or strength of the asset (refer to Table 7.7).

Table 7.7: Asset value calculation

Weakness Value Scale	Yes/No	CIA Value	Weakness Value
Availability			
Can operations continue when * is unavailable?	No	5	
Can unavailability create a loss of revenue?	Yes	5	
Can * be restored within reasonable period?	Yes	0	3.33
Confidentiality			
Is * confidential?	Yes	5	5.00
Integrity			
Is * encrypted or protected by secure access?	No	5	5.00
			13.33
			88.89%

7.7 Conclusion

This chapter has presented the methodology for the identification of assets for the risk management process. The goals of the chapter have been achieved and are summarised below.

The first requirement of this chapter, the identification of the risk management environment, may occur in many forms, whether by board decision, proposition or response to an exposure.

The chapter has also provided the sponsor with the opportunity of electing certain members of the risk management team to certain tasks, as befits their strengths.

This chapter has provided the first important register of information to the board as proof of deliverable completion, the asset register. The chapter has also demonstrated how an enterprise may value its assets based on confidentiality, integrity and availability requirements.

The chapter has presented checklists that enforce the completion of each deliverable before continuing to the next.

The next chapter on risk assessment makes use of the asset register information to determine the threats, vulnerabilities and risk values for the highest valued assets.

8 Risk Assessment

8.1 Introduction

The assessment of risks empowers an organisation to combat its vulnerabilities, recognise threats and prepare for solutions. Risk assessment may also expose areas in what the organisation thought was a well-protected system to expose its weaknesses in protecting sensitive information.

Assessment is thus a double-edged sword. While it is in the best interest of any organisation to be aware of the risks facing its information security, it is also an unavoidable increase in the potential expenses that result in the discovery of its systems, infrastructure and information protective requirements.

For the owner of the SMME, any unplanned expense is unwanted. The new risk of spending on reducing risks with no guarantee of return faces the SMME. The owner cannot be assured that an attacker, albeit an external hacker or disgruntled employee, will not attempt to corrupt the organisation's data, or steal sensitive information. Neither can the owner be guaranteed that this attacker *will* attack the organisation. This issue becomes the age-old mantra of "rather safe than sorry". It is the same reason why the organisation is insured against physical theft, has a security gate at the front door and a strong box for petty cash.

In this digital age, the SMME owner should be just as concerned with the protection of the organisation's information assets as the physical assets also housed within the organisation's premises. More often than not, the information assets will exceed the physical assets in replacement value.

The objective of this chapter is thus the Peculium methodology for assessment.

The goals of the chapter are as follows:

1. The method for identifying threats
2. The method for identifying vulnerabilities
3. The method for determining the likelihood of occurrence of the threat
4. The method for determining the impact of the threat
5. The method for calculating the risks facing the highest weakness valued assets as identified in Chapter 7
6. The method for including the risk values in the organisation's IT plan
7. The checklists for ensuring the completion of each deliverable

The goals are based on the requirements for assessment listed in Chapter 5. The collective achievement of the goals facilitates the achievement of the objective.

The chapter is structured around the achievement of goals 1 to 6, with the checklists for each goal distributed throughout.

8.2 Overview of Risk Assessment

Risk assessment, as defined in Chapter 2, includes risk analysis. Analysis is the gathering of the information used to assess the risk, in this case the identification of threats and vulnerabilities, measurement of the likelihood of occurrence and impact measurement. All of this data is then used to create the risk value and prioritise the risks from highest to lowest for finding the highest impact mitigation strategies in the next step of risk management.

The methods employed in risk analysis and assessments vary across different industries and methodologies [OCTA01 2003] [CRAM 2005]. There are advocates for both qualitative and quantitative risk analysis methods, and various techniques for calculating the risks [KARA 2005].

In this dissertation the qualitative method for risk assessment is used as it offers a simpler, shorter and more affordable option to the SMME owner. Quantitative methods are often mathematical or financial in nature and usually require a software tool at a purchase cost [KARA 2005]. An example of such a tool is the CRAMM V Express tool examined in Chapter 4.

The SMME owner and the risk management team in this methodology are under the constraints of a limited time frame and budget, and are also only provided with the training for conducting this methodology. The qualitative methods for risk assessment are a better fit to the SMME due to the simplified calculation methods used [KARA 2005].

This chapter presents the methods used to analyse risks and then perform the required assessment. The composite information should provide the risk management team with enough information to enter the next step of risk management, being risk mitigation (refer to Figure 6.1).

The deliverables of risk assessment are:

- The identified threats
- The identified vulnerabilities
- The calculated likelihood of occurrence
- The measured impact
- The calculated risks
- The inclusion of the assessment in the IT plan

The deliverables are in a semi-sequential order, as a pair of deliverables may be completed concurrently (refer to Figure 8.1). The risk management team may distribute these assessments to reduce the time of the assessment step.

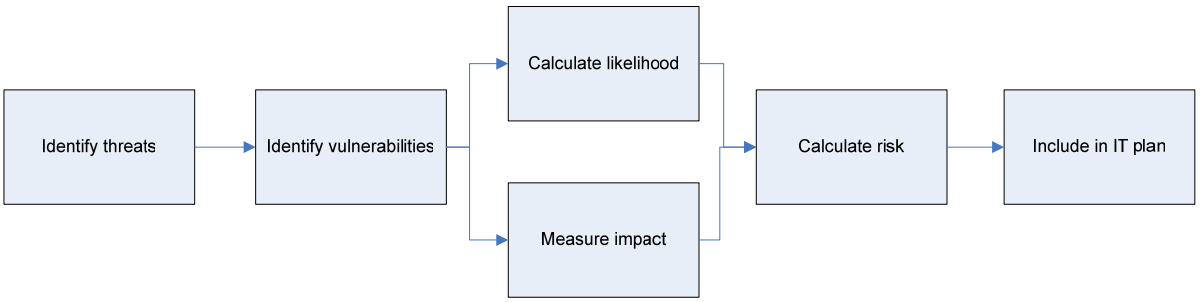


Figure 8.1: Order of completion of deliverables

8.3 Identify Threats

Threats to information assets may come in many forms and from various sources. Not all risks facing information assets may be blamed on the hacker, but neither can the hacker be excluded. The hacker is one of many threats facing any information-based environment.

Threats have been categorised in various ways, as it is easier to identify threats when the analyst is provided with some guidelines.

The following threat categories are used for this analysis method. They are based on the OCTAVE method but are used in a simplified format for use by an SMME [ALBE 2003]:

- Internal threats are those propagated by staff or systems within the organisation. Staff within the organisation may accidentally or intentionally harm an asset. Internal systems may accidentally affect another system or other asset. Internal threats are thus classified as human or system threats.
- External threats are those propagated by external people or systems attacking the organisation. These again may be accidental, or malicious. External threats are also classified as human or system threats.
- Other threats, as the name implies, include those threats that are not propagated by people or systems. Such threats include natural disasters.

8.3.1 Matching Threats to the Assets

The ISO 17799 information security standard provides a list of threats that may face any organisation [SABS 2000] [GMIT 2002]. The list is not conclusive and may be added to should other threats be identified. The risk management team should review this list and identify those risks that apply to the assets identified and valued in Chapter 7. Refer to Appendix 4 for the full ISO 17799 list of threats.

8.3.2 Create Risk Register

The second large proof documentation provided to the board is created in this step. The risk register is the collection of risk profiles, each of which is a combination of various pockets of data forming a descriptive map of the risk facing the information asset. This risk register is used to prioritise the risks once assessed, and also holds the mitigation information for the risks [BARR 1995].

The risk profile grows and develops throughout the risk management process, starting with information from the asset register, gaining information through the assessment, and being finally completed in monitoring.

The risk profile is referred to again in this chapter. In relation to threats, however, the following information is captured:

- Asset name and properties are the starting point of the risk profile. The risk profile identity is based upon the asset register. The board should be able to gauge a picture of the asset based on the name, access route, host system and business unit. The full asset register still remains holding all the asset information.
- Threat names and properties for each threat identified for the asset. The threat properties are as follows:
    - The threat description provides a non-professional's explanation of the threat, e.g. "failure of network components" may be a layman's description of a switch reducing routing speed to a non-performance amount.
    - The CIA affected by the threat is added. Not all threats may threaten each of the security requirements, but it is vital to understand which are threatened. For example, the switch used above will threaten network availability, thus the security requirement of availability.

8.3.3 Checklist

The checklist for this deliverable asks that the threats be selected, added to the risk profile and the description and effect on CIA also added (refer to Table 8.1). All checkboxes except for 2 must be checked to indicate the completed task, and completed step one. Number 2 is not mandatory. The checkbox may be left blank.

Table 8.1: Assessment checklist 1

Assessment Activities			
Step One		**Identify threats**	
	1	Select threats	☐
	2	Add more threats if applicable	☐
	3	Add threats to risk profile	☐
	4	Add descriptions and CIA affected to risk profile	☐

8.3.4 Risk Profile Example

The risk profile contains the name of the asset and the threats facing it. The information regarding the threat captured to the profile is the threat name, description and effect on CIA (refer to Figure 8.2). The risk profile continues to expand throughout this chapter. Each addition to the risk profile going forward is highlighted using bold font in the figure.

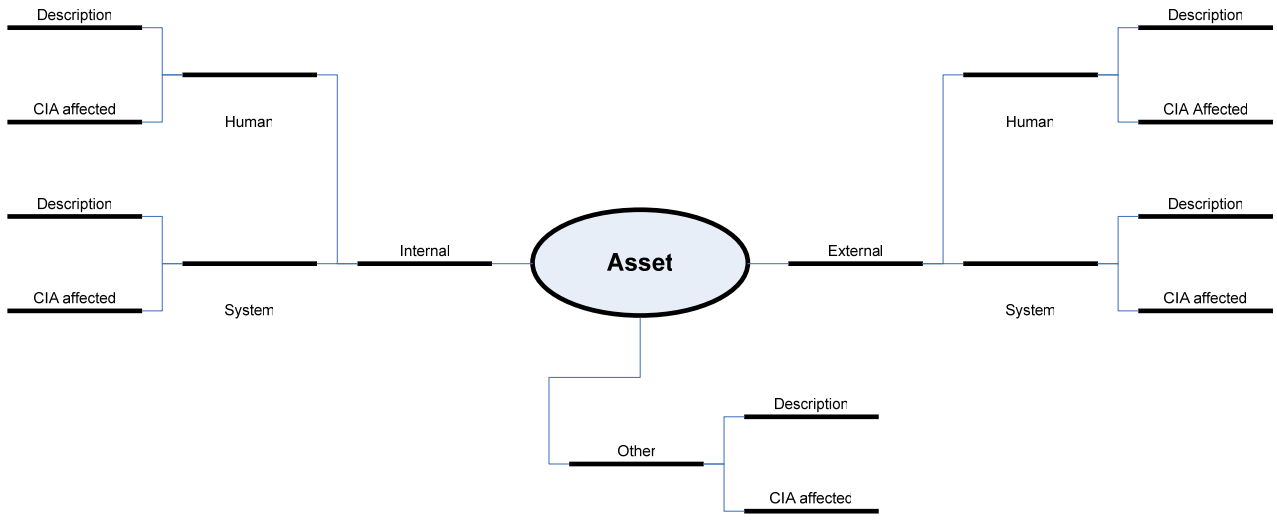


Figure 8.2: Risk profile 1

8.4 Identify Vulnerabilities

Vulnerabilities, unlike threats, are only concerned with the organisation itself, and not the outside world. Vulnerabilities of a government system, travel infrastructure or IT facilitating cabling cannot be altered by the organisation itself, and neither should the risk management team be utilised to attempt to solve their external environment's problems.

Vulnerabilities are, however, linked to both internal and external threats. An internal vulnerability, such as poor cabling structures within the building, may be threatened by an infiltration by an external hacker, abusing the weak cabling security for access to the information assets.

The same applies to internal threats, such as the inaccurate allocation of user access rights, exposing the organisation to the internal threat of unauthorised access to software.

Vulnerability itself causes no harm, but requires a threat to the associated asset to create the harm. There is not always a distinct link between threats and vulnerabilities, but awareness of both is vital. The ISO 17799 states that a threat without a corresponding vulnerability creates a non-risk, or the absence of risk [SABS 2000] [SPIN 1999].

The use of a software tool to identify network vulnerabilities may be used, but as stated earlier in the chapter, is not required. Appendix 4 provides the full list of vulnerabilities provided by ISO 17799. Again, the risk management team may add to the list if so required.

8.4.1 Checklist

The checklist for this deliverable asks that the vulnerabilities be identified, mapped to the threats and then added to the risk profile (refer to Table 8.2). All checkboxes, except 2, must be checked before continuing to step three. Number 2 is not mandatory. The checkbox may be left blank.

Table 8.2: Assessment checklist 2

Assessment Activities			
Step Two		**Identify vulnerabilities**	
	1	Identify the vulnerabilities applicable to the assets	☐
	2	Add more vulnerabilities if applicable	☐
	3	Map the vulnerabilities to the threats	☐
	4	Capture all information to the risk profile	☐

8.4.2 Risk Profile Example

The risk profile now includes the vulnerabilities that have been mapped to the identified threats (refer to Figure 8.3). The vulnerabilities have been added as an extension of the threats and are indicated in bold font.

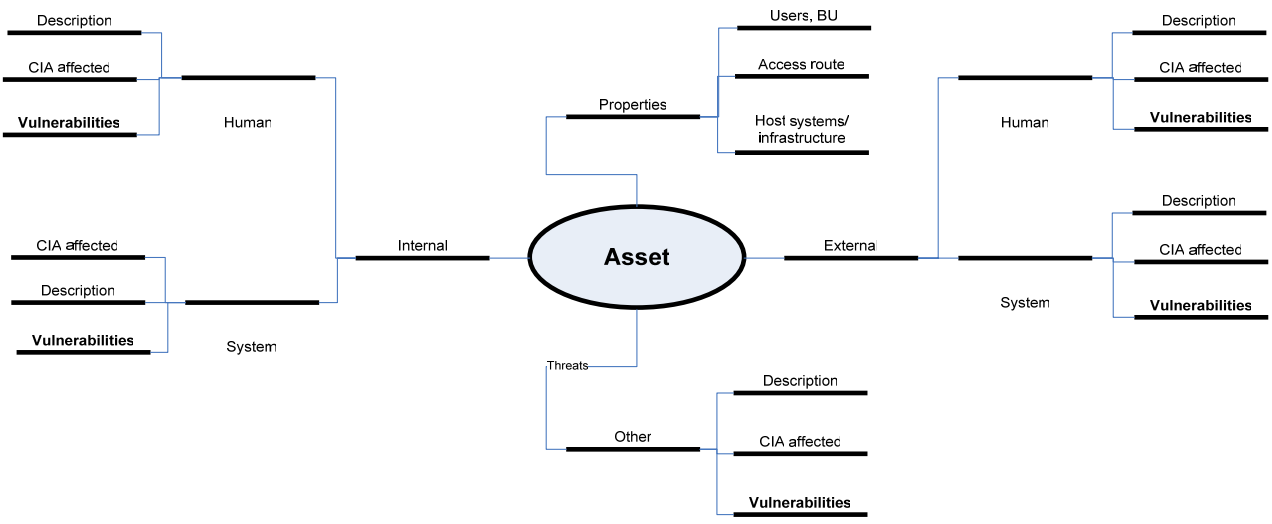


Figure 8.3: Risk profile 2

8.5 Calculate Likelihood of Occurrence

The likelihood of occurrence in risk management is the estimation or probability of the vulnerability being exposed to the threat [RISK 2002]. The likelihood is a subjective measure that could be based on historical data if available. If this is not available, the likelihood relies on the analysis of the threat and vulnerability information and probability estimation.

The likelihood levels are defined as [SABS 2000]:

- A high probability or likelihood of occurrence is the occurrence of a threat that is highly likely, or highly probable to occur.
- A medium probability or likelihood of occurrence is the occurrence of a threat that is somewhat likely, or possible to occur.
- A low probability or likelihood of occurrence is the occurrence of a threat that is not likely to occur.

For use later in the chapter, the values of 3, 6 and 9 are assigned to the levels for low, medium and high, respectively. This scale provides a wider scope for the calculation of impact and risk values later in this chapter, and also assists in the prioritisation of these values. The likelihood of occurrence or probability value is always denoted by the letter P for use in formulae.

This new information about the probability or likelihood of occurrence of the threat or exposure of the vulnerability must also be mapped to the risk profile.

The risk management team must update the risk profile as the information is obtained.

8.5.1 Checklist

The checklist for this deliverable asks that the likelihood levels be assigned and captured to the risk profile (refer to Table 8.3). All checkboxes must be checked before continuing to step four.

Table 8.3: Assessment checklist 3

Assessment Activities		
Step Three	**Calculate likelihood of occurrence (P)**	
	1 Assign likelihood values	☐
	2 Add likelihood values to risk profile	☐

8.5.2 Risk Profile Example

The risk profile is updated with the likelihood of occurrence values. The letter P represents the likelihood of occurrence or probability value assigned to the threat and is indicated in bold font.

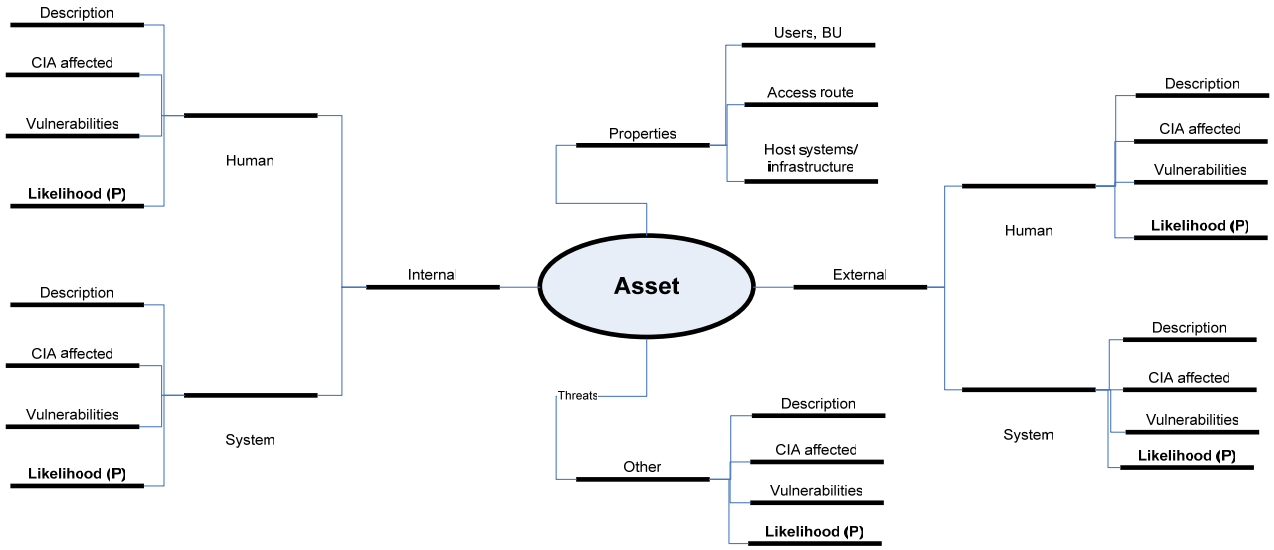


Figure 8.4: Risk profile 3

8.6 Perform Impact Measurement

Impact measurement, similar to likelihood of occurrence, makes use of the information gathered from identifying threats and vulnerabilities to estimate impact values.

The impact measurement of the threat is determined through the business impact that the exposure of the vulnerability will create. This business impact is measured considering the impact on generic areas of the business. These generic areas include reputation, health, productivity, legal penalties, monetary factors and facilities [ALBE 2003].

The method for measuring the impact of a realised threat has been represented in many different forms in literature [SPIN 1999] [SUH 2003] [ALBE 2003]. However, these methods are not very distinct or easily used by SMMEs.

The various methods require testing for suitability to the SMME environment.

8.6.1 Determining the Impact Areas

The impact of a threat can reach various areas of the business, depending on the industry. The generic areas already identified may increase the complexity and duration of the impact measurement. For this reason, the areas are compounded into the following:

1. Monetary loss. The exposure of a vulnerability to a threat may cause financial harm to the organisation in the context of a replacement cost of an asset, or revenue lost as a result of the exposure. For a small organisation, cash flow may be a great challenge, and monetary loss a great impact. The level of impact is compared to the appetite for risk identified in the preparatory activities. The ranges are unique to each organisation. For the purposes of demonstrating impact measurement, the appetite is R80 000 and the ranges R0 – R10 000 representing low impact, R11 000 – R40 000 representing a medium impact, and R41 000 - R80 000 representing a high impact.

2. Productivity loss. The loss of productivity in an organisation may be represented by the cost of payroll for the duration of the exposure. The impact is calculated using the following formula:

   $$\text{Impact (Productivity)} = \text{Days} \times \text{Payroll}$$

   The amount is compared to the appetite for risk ranges to determine the impact level of high, medium or low.

3. Reputation loss. SMMEs in South Africa account for a great number of enterprises. As such, outperforming the rest is vital for an SMME's survival. The loss in reputation may cause loss of accreditation of an industry standard, loss of customers and future growth.

These three areas represent the major concerns for an SMME and may be expanded to include more specific areas [ALBE 2003].

The areas are used to determine the impact of the threat. The method for using these areas is as yet undefined.

8.6.2 Determining the Ideal Impact Measurement Method

Three methods for measuring qualitative impact as mentioned above can be defined as worst case scenario, average impact and weighted impact.

- Worst case scenario impact assigns a value of high, medium or low to all the impacts identified, and assigns the highest value to the total impact.
- Average impact also assigns a value of high, medium or low, but in this case a numerical association is made and the average calculated. A value of 1 is assigned to low, 2 to medium and 3 to high. Total values of 1-3 are low, 4-6 are medium and 7-9 are high. The 9-point scale is used again as explained in 8.5.
- Weighted impact assigns weights to each impact identified, and calculates the total in a formula using the weights to favour certain impacts above others. The weights may differ in different industries. In the scope of the SMME, however, the monetary factor is almost always of highest concern. For the purposes of this test, the monetary area is granted the highest weight, with equal weight for productivity and reputation. Monetary weight is 40%, and productivity and reputation each 30%.

Impact, when used in a formula, is always denoted using the letter I. The abovementioned methods cannot be proven or disproved without testing the methods in the same scenarios. The scenario tests selected for this are as follows:

- A threat of malicious software exposes the open communication lines to the SMME.
- A threat of theft exposes poor physical protection of the building.

- A threat of wilful damage exposes the inadequate allocation of access rights.

8.6.3 Scenario Tests of the Impact Measurement Methods

Three scenarios are provided to test the impact measures.

Scenario 1

A virus attack causes a server to crash. The threat is malicious software; the vulnerability is unprotected public communication lines. The technical support staff will take two days to repair the damage.

The areas identified and methods discussed above are presented in Table 8.4.

Table 8.4: Impact measurement method test 1

Malicious Software			
Monetary loss	Revenue loss for 2 days is R20 000. Impact is medium.		
Productivity	Server downtime of 2 days. Payroll per day is R1 800. Technical staff required to recover the server and repair the damage are paid R500 per day. I(Pr) = Days × (Payroll + Technical staff) I(Pr) = 2 × (1 800 + 500) I(Pr) = R4 600 Impact is low.		
Reputation	Some customers are lost due to the 2 days of downtime. Impact is medium.		
Worst case		**Average**	**Weighted**
The highest impact is medium. Impact is medium.		I = Medium + Low = Medium I = 2 + 1 + 2 I = 5 Impact is medium.	I = Medium + Low + Medium I = 0.6 + 0.16 + 0.6 I = 1.36 Impact is medium.

The impact has been determined to be medium in all three methods. No distinct method is as yet selectable.

Scenario 2

The vulnerability of lack of physical protection has been exposed to the threat of theft. All servers and desktop computers have been stolen and will take at least one working week to replace. The scenario is presented in Table 8.5.

Table 8.5: Impact measurement method test 2

Lack of Physical Protection			
Monetary loss	All server and desktop hardware must be replaced at a cost of R70 000. Revenue loss for 5 days is R50 000. Impact is high.		
Productivity	The wait for hardware is at least 5 days. I(Pr) = Days × Payroll I(Pr) = 5 × 1 800 I(Pr) = R9 000 Impact is low.		
Reputation	Many customers are lost due to the 5 days of downtime. Impact is high.		
Worst case		**Average**	**Weighted**
The highest impact value is high. Impact is high.		I = High + Low + High I = 3 + 1 + 3 I = 7 Impact is high.	I = High + Low + High I = 1 + 0.3 + 0.9 I = 2.2 Impact is high.

Again, the test does not provide a clearly discernible best method as all results are high. A final test is attempted.

Scenario 3

The vulnerability of wrong allocation of access rights is exposed to wilful damage. Information is corrupted and irretrievably damaged. Recovery of the information is of vital importance. The scenario is presented in Table 8.6.

Table 8.6: Impact measurement method test 3

Wrong Allocation of Access Rights			
Monetary loss	The data is an information asset. It cannot be purchased for replacement. Revenue intake is reduced to half measures. Impact is high.		
Productivity	Productivity is reduced due to the unavailability of the data. The recreation of the data doubles the lack of productivity. It takes 4 days to recreate the data. This circumstance changes the formula: I(Pr) = Days * (Payroll + Recreation productivity) I(Pr) = 4 * (1 800 + 1 800) I(Pr) = R14 400 Impact is medium.		
Reputation	Many customers are lost due to the effort of recreating the data. Customers fear the repercussions to their own business due to the wilful damage. Impact is high.		
Worst case		**Average**	**Weighted**
The highest impact is high. Impact is high.		I = High + Medium + High I = 3 + 2 + 3 I = 8 Impact is high.	I = High + Medium + High I = 1.2 + 0.6 + 0.9 I = 2.7 Impact is high.

Again, all three methods provide the same answer. The conclusion may then be made that the calculation for determining the three impact values is sound and provides correct evidence for calculating the total impact value. As each method yields the same or a similar result, the easiest method should be used for the benefit of the risk management team. The simplest method is average and is entered as the method for this methodology.

8.6.4 Checklist

The checklist for this deliverable asks that the impact values be assigned to the threats and captured to the risk profile (refer to Table 8.7). All checkboxes must be checked to allow continuation to step five.

Table 8.7: Assessment checklist 4

Assessment Activities		
Step Four	**Perform impact measurement (I)**	
	1 Assign impact values	☐
	2 Add impact values to risk profile	☐

8.6.5 Risk Profile Example

The risk profile is updated with the impact measures assigned to each threat. A new leg in the risk profile tree is created to hold the assessment data. The impact values are represented by the letter I and are indicated on the profile using bold font.

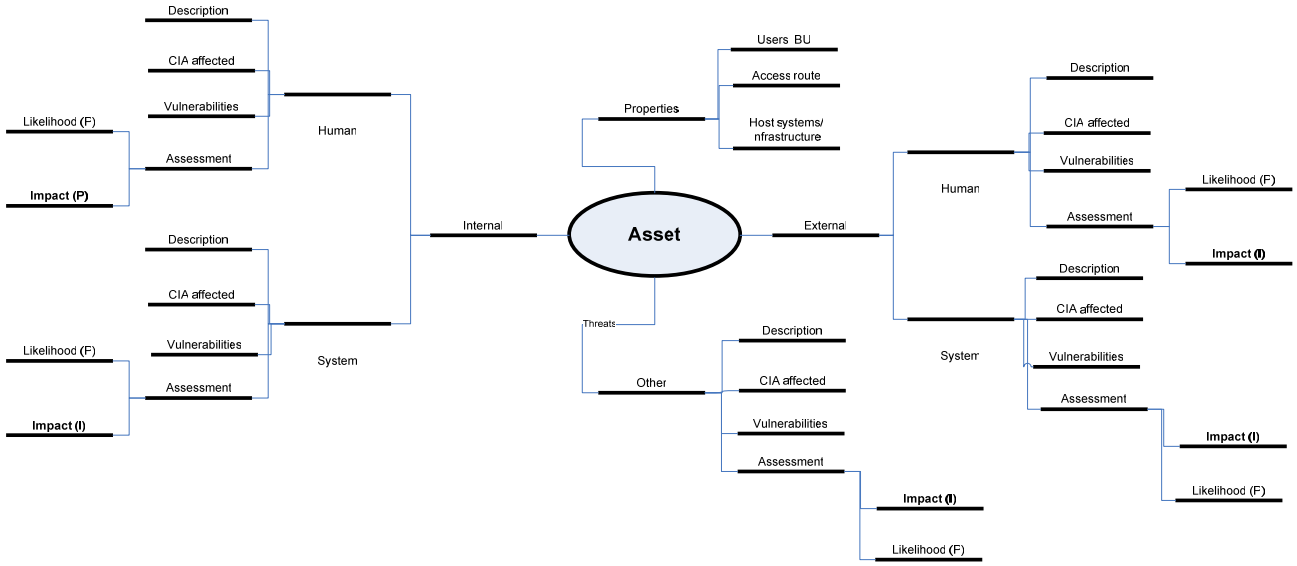


Figure 8.5: Risk profile 4

8.7 Calculate Risks

The culmination of the information that has been gathered to date, the purpose of the assessment, is the calculation of the risk values. These risk values provide the necessary prioritisation of risks to mitigate first, based on the urgency of the high value.

There are various methods of calculating risks and various arguments for and against these methods.

The risk management team, as applied in this methodology, is a group of individuals that most likely do not have a background in statistical and mathematical measurement of risk. For this reason, qualitative measures have been used for this calculation [KARA 2005].

8.7.1 The Standard Risk Calculation Method

The information gathered thus far in assessment, to summarise, is:

- The threats facing the asset
- The vulnerabilities of the asset
- The probability (likelihood of occurrence) of the threat (P)
- The impact of the occurrence of the threat (I)

Traditional calculation of the risk value has been based on the formula:

Risk (R) = Probability (P) * Impact (I)

This calculation is qualitatively performed using a PI matrix that allows the plotting of the risk value, based on the product of probability and impact (PI).

The column representing the impact value is highlighted, and intersects with the row representing the probability value. The intersection becomes the risk value (refer to Table 8.8).

Table 8.8: The standard PI matrix [STEP 2002]

		Impact		
Probability		**L**	**M**	**H**
	L	L	M	M
	M	M	***M***	H
	H	M	H	H

This system is flawed, however, as a risk with high impact and low probability (HILP) has the same value as a risk with high probability and low impact (HPLI),

now referred to as the HILP-HPLI problem [STEP 2002]. The same applies to any other risks valued as high, medium or low. The prioritisation mitigation of the list becomes impossible.

The answer to the HILP-HPLI problem has been addressed through various means. One approach is the assigning of numeric values to high, medium and low, still not resolving the prioritisation issue. Another method is increasing of the impact values of high, medium and low, causing the higher impact risk to be mitigated first (refer to Table 8.9) [STEP 2002].

Table 8.9: The adjusted PI matrix

		Impact		
Probability		**L 2**	**M 4**	**H 8**
	L 2	4	8	16
	M 3	6	***12***	24
	H 4	8	16	32

This raises the question of whether a higher probability risk is really lower in value than a higher impact risk. If this is true, the assigning of risk values is useless, as the impact values carry a greater weight than the probability. The time spent on probability and risk calculation is wasted and the requirements of Chapter 5 are not met.

8.7.2 The Standard Risk Calculation Method Revisited

The information gathered using the likelihood of occurrence and impact measurement methods has yielded values that may be classified as high, medium or low.

The formula for calculating risk is retained and likelihood of occurrence (P) is multiplied by impact (I). The resulting value provides a numerical figure for prioritising risks and thus determining the top risks to be mitigated. The nature of the 9-point scale used for high, medium and low, as well as the method and

areas for calculating impact have provided a broad range of possible risk figures, not as contained as in the method described above.

Scenario 1 used earlier is now completed to calculate the risk value. A probability of medium is assumed. This value is based on qualitatively collected data, and does not change to a quantitative statistical or monetary value. It remains qualitative. The risk value calculation is presented in Table 8.10.

Table 8.10: Calculation of the scenario 1 risk value

Asset	Threat	P	I	R
Server	Malicious software	6	5	30

These risk values calculated for each threat facing the highest weakness valued assets may now be prioritised into a benchmark top five highest risks, or should the organisation prefer, risk values higher than a numeric amount. The selection of five top risks is the minimum, thus eradicating the temptation to reduce the list and shorten the process.

8.7.3 Checklist

The checklist for this deliverable asks that the risk values be calculated and added to the risk profile, and finally prioritised for the top risks selection (refer to Table 8.11). All checkboxes must be checked for completion of step five.

Table 8.11: Assessment checklist 5

Assessment Activities			
Step Five		**Calculate risks**	
	1	Calculate risk values	☐
	2	Add risk values to risk profile	☐
	3	Sort risk register by risk value	☐
	4	Select top risks	☐

8.7.4 Complete Risk Profile

The completed risk profile provides all the information required for risk mitigation. The latest addition, the risk values, are presented in bold font (refer to Figure 8.6).

8.8 Include Risk Values in IT Plan

All of the information gathered thus far in the asset register and through risk assessment is represented in the risk profile of each asset.

The risk profiles collected create a risk register that can be inserted into the IT plan of the organisation. This is handed to the board as an informative explanation of the standing of the organisation's risks and assets.

If no IT plan exists for the organisation, the sponsor must hand the risk register to the board. The risk management team is not to be used to create an IT plan.

The risk register is again updated in the remaining steps in the risk management process. Each update must be communicated to the board and staff to ensure that the parties are aware of the risks and how the organisation is combating them.

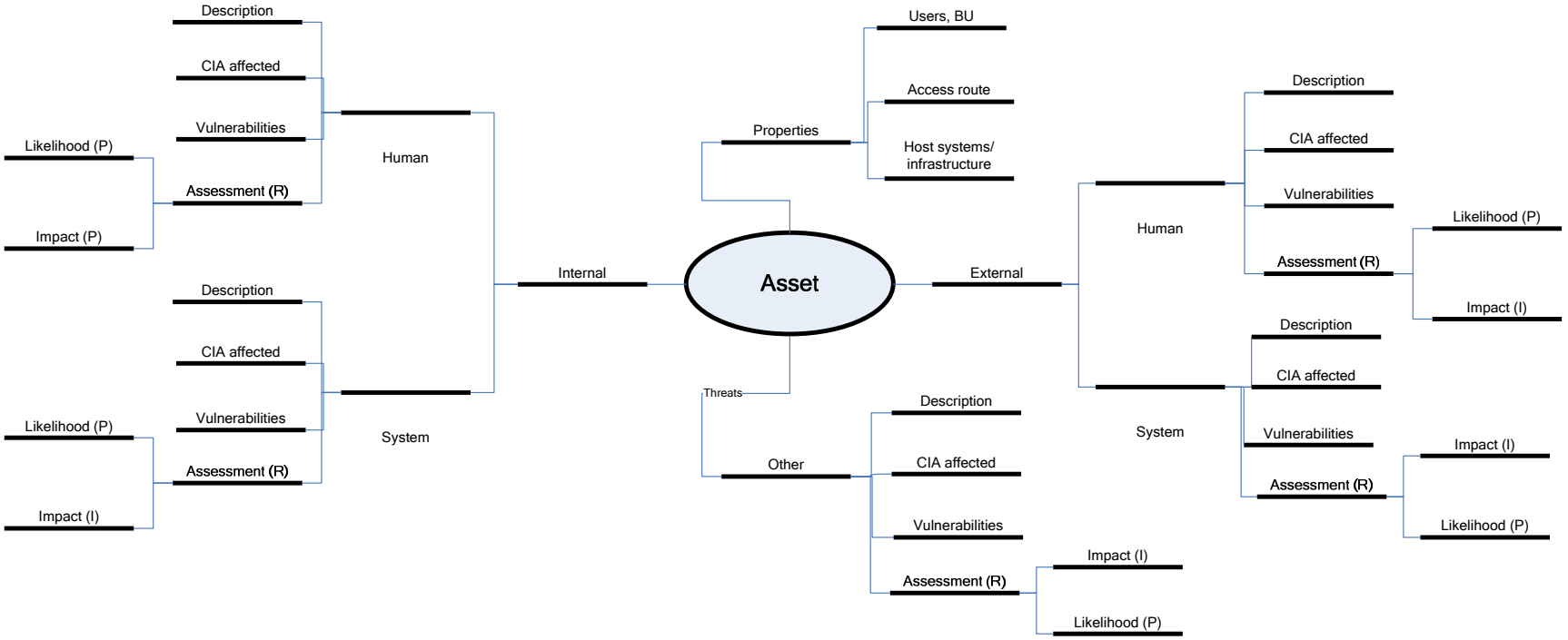


Figure 8.6: The complete risk profile

Checklist

The checklist for this deliverable asks that the risk register be included in the IT plan, or handed to the board (refer to Table 8.12).

Table 8.12: Assessment checklist 6

Assessment Activities			
Step Six		**Include risk profiles in IT plan**	
	1	Include risk profiles in IT plan or hand to the board	☐

8.9 Conclusion

The risk management process, as presented in the chapters of this dissertation, has been customised from established risk management methodologies. It offers the risk management team a simple but effective method of calculating the risks facing the organisation's information assets to create a prioritised list for mitigation and ultimately monitoring.

This chapter has achieved the goals specified and is summarised below.

The chapter used traditional methods in the use of the ISO 17799 lists of known threats and vulnerabilities to information assets. A connection needs to be made between a threat and vulnerability to create a risk. The failure to make a connection removes the threat from the risk profile.

The method for determining likelihood of occurrence has also been traditional, whereas the impact measurement method has been determined to be the average value of the three areas assessed; being monetary factors, productivity and reputation loss. This method was selected after testing three methods; worst case, average and weighted yielded no clear best option. Average was selected for its simplicity to benefit the risk management team.

The chapter has also presented the challenge of calculating risk values, as the traditional methods do not provide the answer to the HILP-HPLI problem. The benefit of the 9-point scale and impact measurement method used is the use of numerical associations with the risk values, thus removing the HILP-HPLI problem.

The chapter has also presented the checklists that ensure that all deliverables are completed before continuing to the next step of risk management, namely mitigation.

Chapter 9 presents the methodology for risk mitigation. The risk values calculated in this chapter are carried forward for mitigation strategies, and the risk register is used to host additional information known as the action plans.

9 Risk Mitigation

9.1 Introduction

The mitigation or reduction of risk is where all the information, knowledge and experience of the past steps in the risk management process come together to reduce the risk.

The mitigation step is where information gathering ends and interpretation of the information begins as financial decisions are made that may affect the way the organisation operates.

This is true to a large extent for the SMME. Smaller enterprises are more easily adaptable to change, as change is usually on a smaller scale. Any change is, however, difficult. The mitigation of a risk, for example the threat of unauthorised access, may lead to training all staff of the SMME to use more effective passwords and lock their workstations when they leave their desks.

This may seem a small change to implement, but changing the habit of a whole organisation is difficult.

The objective of this chapter is to provide the Peculium methodology for mitigation.

The goals of the chapter are:

1. The method for identifying the mitigation strategy for each risk
2. The method for selecting the controls for the risks identified for mitigation
3. The method for creating an action plan for each risk
4. The checklists for each deliverable

The goals are based on the requirements listed in Chapter 5. The collective achievement of the goals constitutes the achievement of the objective.

9.2 Overview of Risk Mitigation

Risk mitigation, different in a sense from risk assessment, does not offer such variety in methods and tools. Risk mitigation can be found to follow the steps of selecting the strategy, finding the control and planning its implementation in most methodologies [SPIN 1999] [SUH 2003] [ALBE 2003].

The difference in this methodology is the manner in which the information from previous steps is presented. The asset register and risk register are in a unique format in this methodology.

The decisions made in this step of the risk management process provide the organisation with the habitual changes, tool implementations and policies to reduce its risk to information assets.

These changes and implementations are performed in the next step, namely monitoring (refer to Figure 6.1).

The deliverables of the mitigation step are:

- The identified mitigation strategy for each risk
- The selected controls for each risk identified for mitigation
- The action plan for the mitigation of each risk

The deliverables are in sequential order and may not be completed out of order.

Figure 9.1: Order of completion of deliverables

9.3 Identify the Mitigation Strategy

The mitigation strategies that are required to be assigned to each risk determine how the risk is treated going forward. There are four specific options available as strategies for the risk, each with their own advantages and disadvantages [SCHW 2002].

- Risk avoidance is the most affordable but most dangerous of strategies to assign. In the case of avoidance, nothing is done about the risk. The organisation takes the decision to take no action against the risk until such time as it is deemed dangerous enough to mitigate. The risks that are prioritised for mitigation are already at a critical level. This strategy should not be considered for high impact or probability risks. In the event of an iteration of the process not yielding high impact or probability risks, such a strategy may be justified.
- Risk termination is the removal of the asset at risk from the organisation. The selection of this strategy would create many consequences, such as reduction in productivity and loss of information. An asset facing a threat to its availability should not be considered for termination, as the mitigation strategy becomes the threat.
- Risk mitigation in most cases involves the implementation of controls that reduce the threat to the asset. In some cases the control is system related (a code change), infrastructure related (improved perimeter security) or through the intervention of staff, such as security awareness training. Not all controls are at a purchase cost to the organisation, but may facilitate a productivity loss.
- Risk transfer concerns the movement of the risk onto a third party. In most cases the third party is an insurer that will reimburse the organisation for losses should the threat be realised. The transfer of risk, although with the assurance of reimbursement, does not protect the confidentiality or integrity of the information lost, and creates a period of no availability. Realisation of the threat could also lead to serious loss of reputation.

9.3.1 Assigning a Strategy to Each Top Risk

The process for assigning a strategy to each of the top risks identified must be followed to ensure that the strategy is justifiable to the board. The steps for assigning the strategy are as follows:

1. Gather the risk profile for each risk with the assessment information of the impact and probability of the risk.
2. Map the assessment information to the recommendations presented in the mitigation strategy matrix (refer to Table 9.1).

Table 9.1: The mitigation strategy matrix

Risk	Avoid	Terminate	Mitigate	Transfer
High impact, high probability		•	•	
High impact, medium probability			•	
High impact, low probability			•	•
Medium impact, high probability		•	•	
Medium impact, medium probability			•	
Medium impact, low probability				•
Low impact, high probability		•	•	
Low impact, medium probability			•	
Low impact, low probability	•			

The matrix provides a guideline for the selection of the strategy.

a. The strategy of mitigation occurs more often than any other strategy.
b. The strategy of avoidance should only be applied to low impact, low probability risks.
c. The strategy of termination may only be considered if availability is not a security requirement. However, should availability be a security requirement, mitigation may be

performed. This reinstates the HILP-HPLI problem but in a reduced scope in the security requirements.

d. The strategy of transfer is used for those risks that have a very low probability of occurring, but that may have an impact on the organisation. In some instances a secondary strategy of mitigation may be employed to reduce the impact should the vulnerability be exposed.

3. The strategy is added to the risk register against each risk (refer to Table 9.3).

9.3.2 Checklist

The checklist for this deliverable asks that the mitigation strategies be assigned and captured to the risk register (refer to Table 9.2). All checkboxes must be checked before continuing to the next step.

Table 9.2: Mitigation checklist 1

Mitigation Activities			
Step One		**Identify mitigation strategy**	
	1	Assign mitigation strategy to each risk	☐
	2	Capture mitigation strategy to risk register	☐

9.3.3 Risk Register

The risk register presented here does not contain the full risk profile as all relevant information is displayed in Chapter 8. The mitigation information in the risk register is used henceforth. A generic example is used to present information.

Table 9.3: Risk register 1

Risk Register	
Risk	**Mitigation Solution**
Risk 1	Transfer

9.4 Selecting the Mitigating Controls

The risks that were selected for mitigation in the previous deliverable are used again in this selection of controls. The remaining risks are revisited in “Create action plans”.

The selection of a control is a difficult process that requires careful consideration of the cost benefit of the control, as well as the ultimate fit to the risk at hand.

The process for selection of controls, also known as safeguards, can be described as demonstrated in Figure 9.2 [NIST 2002].

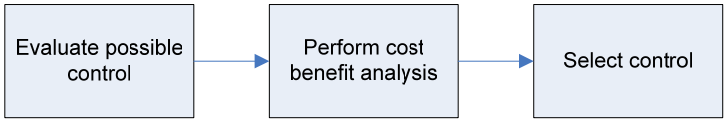


Figure 9.2: Process for selection of controls

1. A list of controls is reviewed for potential controls that fit the risk [GMIT 2002].
2. A cost benefit analysis is performed on each potential control to determine the best fit control for the organisation. The cost benefit analysis considers the following for each control:
    a. Impact as determined during risk assessment
    b. Impact after implementation
    c. Cost of the implementation, considering the purchase cost and productivity loss during implementation
3. The control is selected and entered into the risk register.

9.4.1 Performing the Cost Benefit Analysis

The cost benefit analysis is used to determine a best fit control when multiples are available to mitigate a risk and the return on investment of the control. The analysis is performed by considering the impact before the control is implemented, reduction in threat impact when the control is implemented and the cost of the implementation [NIST 2002].

The scenarios used to demonstrate the measurement of impact in Chapter 8 are used again here.

9.4.1.1 The Impact as Determined by Risk Assessment

The impact measurement performed for the three scenarios in Chapter 8 is as follows:

- Scenario 1: Medium
- Scenario 2: High
- Scenario 3: High

9.4.1.2 Determining the Impact after a Control is Implemented

Payroll used is at R180 per staff member per day in an organisation of ten staff. Technical staff are remunerated at R500 per day.

Scenario 1

In scenario 1 a virus attack causes a server to crash. The controls that have been selected are as follows:

- Ant-virus software that protects the server. It is a managed solution that automatically updates virus definitions on a daily basis.
- Software firewall protecting data entry to the server. The firewall may be configured to block viruses that use network protocols but not file attachment viruses. The probability of exposure is slightly reduced.

Table 9.4: Scenario 1 impact after implementation of the controls

Malicious Software		
Control	**Anti-virus**	**Firewall**
Monetary loss	No revenue is lost. Impact is low.	An email attachment contains a virus that causes the server to crash. Server is down for 2 days. Impact is medium.
Productivity	I(Pr) = Days × Payroll I(Pr) = 0 Impact is low.	Server downtime of 2 days. Payroll per day is R1 800. Technical staff are required to recover the server and repair the damage. I(Pr) = Days × (Payroll + Technical staff) I(Pr) = 2 × (1 800 + 500) I(Pr) = R4 600 Impact is low.
Reputation	No customers are lost. Impact is low.	Some customers are lost due to the 2 days of downtime. Impact is medium.

The impact after the implementation of the controls, based on the average calculation, is:

- Anti-virus: I = 1 + 1 + 1 = 3: Low
- Firewall: I = 3 + 1 + 3 = 7: High

Scenario 2

In scenario 2 the lack of physical protection has been exposed to the threat of theft. The controls that have been selected are as follows:

- Security gate at the entrances to the offices. Limited individuals have copies of the keys. The security gate is a preventative measure.
- Security alarm notifying a security company of unauthorised entry to the offices. The security alarm is a reactive measure.

Table 9.5: Scenario 2 impact after implementation of the controls

Lack of Physical Protection		
Control	**Security Gates**	**Security Alarm**
Monetary loss	The security gate is damaged and needs to be replaced. Impact is low.	Some computers are stolen before the response team arrives. The server is untouched. The value of the computers is R15 000. Impact is medium.
Productivity	Productivity is unaffected. Impact is low.	The wait for hardware is at least 2 days for 3 of 10 staff members. I(Pr) = Days × Payroll I(Pr) = 2 × 540 I(Pr) = R1 080 Impact is low.
Reputation	No customers are affected. Impact is low.	No customers are affected. Impact is low.

The impact after the implementation of the controls, based on the average calculation, is:

- Security gates: I = 1 + 1 + 1 = 3: Low
- Security alarm: I = 1 + 3 + 1 = 5: Medium

Scenario 3

Scenario 3 represents the vulnerability of wrong allocation of access rights which is exposed to wilful damage. Information is corrupted and irretrievably damaged. Recovery of the information is of vital importance. The controls that have been selected are as follows:

- A resource is allocated to obtain and enter the access rights required.
- A backup device is installed to create daily backups of the information.

Table 9.6: Scenario 3 impact after implementation of the controls

Wrong Allocation of Access Rights		
Control	**Access Rights Created**	**Backup Device**
Monetary loss	Unauthorised access is removed. Impact is low.	Restoration of the backup retards revenue intake for half a day. Impact is low.
Productivity	No productivity is lost. Impact is low.	Productivity is reduced due to the time required for the backup restore. It takes half a day to restore the data. I(Pr) = Days * (Payroll + Technical staff) I(Pr) = .5 * (1 800 + 500) I(Pr) = R1 650 Impact is low.
Reputation	No customers are affected. Impact is low.	No customers are affected. Impact is low.

The impact after the implementation of the controls, based on the average calculation, is:

- Access rights created: I = 1 + 1 + 1 = 3: Low
- Backup device: I = 1 + 1 + 1 = 3: Low

9.4.1.3 Cost of the Implementation

Cost of the implementation is calculated by considering the purchase cost of the control (including the first year of licensing, or monthly payments) and the productivity of staff that is lost during the implementation.

Table 9.7: Cost of implementation calculations

Scenario 1		
Control	**Anti-virus**	**Firewall**
Purchase cost	R3 000 for server licence	R10 000
Productivity loss	2 hours technical staff[14] R125	5 hours technical staff[14] R315
Total	R3 125	R10 315
Scenario 2		
Control	**Security Gates**	**Security Alarm**
Purchase cost	R2 000 for 2 gates	R7 000
Productivity loss	None	None
Total	R2 000	R7 000
Scenario 3		
Control	**Access Rights**	**Backup Device**
Purchase cost	None	R10 500
Productivity loss	4 hours single payroll[15] R90	None
Total	R90	R10 500

The preparatory information is now available for the cost benefit analysis.

9.4.1.4 The Cost Benefit Analysis of Selected Controls

Table 9.8: Cost benefit analysis of scenario 1

Scenario 1		
Impact before implementation	Medium	
Control	**Anti-virus**	**Firewall**
Impact after implementation	Low	Medium
Purchase cost	R3 000 for server licence	R10 000
Productivity loss	2 hours technical staff	5 hours technical staff

[14] Technical staff payroll is at R500 per day, 2 hours is at R125, 5 hours is at R315.
[15] Payroll at R180 per day, 4 hours is at R90.

	R125	R315
Total	R3 125	R10 315

The cost benefit analysis shows that the implementation of anti-virus is both lower in cost and provides a lower impact at risk realisation. Anti-virus is the control selected.

Table 9.9: Cost benefit analysis of scenario 2

Scenario 2		
Impact before	High	
Control	**Security Gates**	**Security Alarm**
Impact after	Low	Medium
Purchase cost	R2 000 for 2 gates	R7 000
Productivity loss	None	None
Total	R2 000	R7 000

The cost benefit analysis shows that the security gates are lower in cost and provide a lower impact at risk realisation. Security gates are the control selected.

Table 9.10: Cost benefit analysis of scenario 3

Scenario 3		
Impact before	High	
Control	**Access Rights**	**Backup Device**
Impact after	Low	Low
Purchase cost	None	R10 500
Productivity loss	4 hours single payroll R90	None
Total	R90	R10 500

The cost benefit analysis shows that access rights creation is lower in cost and although the impacts are both low, access rights creation is the control selected.

9.4.2 Pareto Analysis of Controls

The selection of controls, in whatever form, may inadvertently mitigate other risks not on the prioritisation list. For this purpose, a Pareto analysis can be done.

Pareto analysis gained its name from the pioneer of the principle of least effort thinking, Vilfredo Pareto, who discovered the imbalance of wealth and income in 19th century England. Pareto discovered that approximately 20% of the population were enjoying 80% of the wealth [KOCH 1997].

This 80/20 rule has been applied in financial circles, domestic applications and the military to determine the high impact low effort products, services or weapons. The result of this analysis is to focus more productivity on the high impact products, and less on the less effective products.

The same rule may be applied in the case of risk mitigation. One control may mitigate various risks, even inadvertently. The important point is to be aware of the mitigation of risks to keep the risk register up to date and provide the board with an accurate view of the state of the information assets.

9.4.2.1 Finding the Controls that apply the 80/20 Rule

The controls that mitigate more than one risk, preferably at least one risk in the top list, can be discovered by completing the following steps:

1. Ensure that the control selected is relevant to the list of top risks.
2. Use an electronic version of the risk register to search for the threats matching those related to the asset in the top risk list.
3. Select the risks that contain the matches.
4. Create a report of the risks that are mitigated by the implementation of the control.

The list of connected risks should help to convince the board of the value of the control, not only mitigating a critical risk, but also reducing more risks than were bargained for. The cost of the risk, when distributed across its implementations, is conceptually reduced.

9.4.2.2 Cost of Exposure Saving

Monetary measures have been included in the preparatory activities and the assessment steps of the risk management process. The mitigation step in the risk management process, as the scope for requesting budget for control implementation, must also make use of monetary measures to lend credibility to its requests (refer to Figure 9.3).

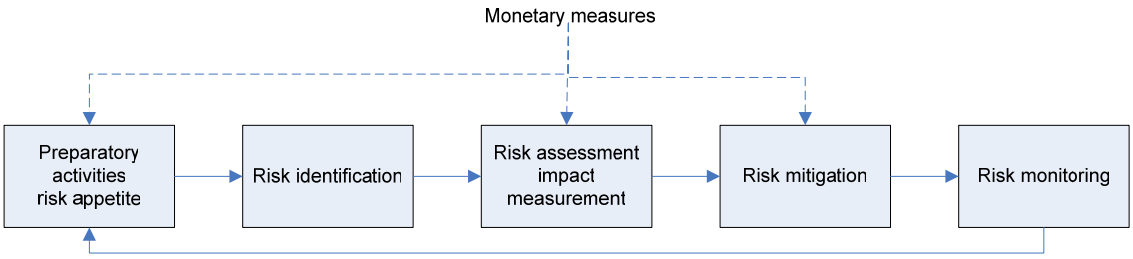


Figure 9.3: Use of monetary measures in the risk management process

The monetary value available to the risk management team thus far has been the appetite for risk. The appetite amount provides a threshold for risk management when considering monetary measurement and consideration of risks and controls.

Cost of exposure saving (CES) is calculated by subtracting the cost of the control from the appetite amount. However, this is not a utopian concept as the amount is most likely always higher than the cost of the control. The following is thus recommended:

- For a low impact risk, the upper barrier of the low impact range of the appetite as used in Chapter 8 is used.
- For a medium impact risk, the mean of the medium impact range of the appetite is used.

- For a high impact risk, the lower barrier of the high impact range of the appetite is used.

The ranges provide a conservative upper level for expenditure on a control, but prevent the lack of any benchmark by using the upper level of the low impact range of the appetite. This controls justifying the cost of a control for a low impact risk, as well as a medium or high impact risk.

The formula for calculating the CES is as follows:

$$CES = IA\ (H/M/L) - Cost\ of\ control$$

IA represents the impact range of the appetite, with H/M/L representing the amount as specified by the rules above.

The formula is adapted for the 80/20 rule controls by subtracting the cost of the control from the cumulative impact appetite of the 80/20 rule risks.

$$CES = \Sigma\ IA\ (H/M/L) - (Cost\ of\ control + Additional\ cost)$$

The adaptation of the control to apply to multiple risks may increase the cost of the control, such as the addition of anti-virus software licences. However, this may not always apply.

The result of the CES equation, when a positive amount, shows the savings the control will create should the risk be exposed. A higher result yields a more cost-effective control.

A negative amount, though, reminds the risk management team that the selected control is expensive and that the mitigation strategy selected may be in error.

A result of zero is a breakeven. In such a case the cost of the control is justified.

9.4.2.3 Scenario Test of CES

The testing of the formula is conducted using the three scenarios used previously.

Table 9.11: Scenario test of CES

Scenario 1		
Impact before	Medium	
Control	**Anti-virus**	**Firewall**
Total	R3 125	R10 315
CES	CES = IA(H/M/L) – Cost of control CES = IA(M) – Cost of control CES = 25 500 – 3 125 CES = 22 375 The control is justified.	CES = IA(H/M/L) – Cost of control CES = IA(M) – Cost of control CES = 25 500 – 10 315 CES = 15 185 The control is justified.
Scenario 2		
Impact before	High	
Control	**Security Gates**	**Security Alarm**
Total	R2 000	R7 000
CES	CES = IA(H/M/L) – Cost of control CES = IA(H) – Cost of control CES = 41 000 – 2 000 CES = 39 000 The control is justified.	CES = IA(H/M/L) – Cost of control CES = IA(H) – Cost of control CES = 41 000 – 7 000 CES = 34 000 The control is justified.
Scenario 3		
Impact before	High	
Control	**Access Rights**	**Backup Device**
Total	R90	R10 500
CES	CES = IA(H/M/L) – Cost of control CES = IA(H) – Cost of control CES = 10 000 – 90 CES = 9910 The control is justified.	CES = IA(H/M/L) – Cost of control CES = IA(H) – Cost of control CES = 10 000 – 10 500 CES = - 500 The control is not suitable.

The calculations in Table 9.11 reveal that the formula has shown some controls to have a greater saving than others, and one control that has been shown as an unjustifiable expense. The next task is to present these amounts to the board for approval of the selection of strategies and controls.

9.4.3 Board Approval of Mitigation Strategies

The list of controls and other mitigation strategies that have been entered into the risk register should be approved by the board before continuing planning the implementation of the strategies.

It may be the case that the board is not satisfied with, for example, a transfer strategy being selected for a risk, and may request a control to be nominated instead. The inverse applies as well.

The sponsor is expected to present the risk register to the board for approval, and make amendments as required.

9.4.4 Checklist

The checklist for this deliverable asks that controls be selected, the 80/20 rule applied to the register, an 80/20 rule report created and the controls captured to the risk register (refer to Table 9.12). Numbers 1, 2, 4 and 5 are mandatory. If number 2 yields no result, number 3 may be ignored and left unchecked.

Table 9.12: Mitigation checklist 2

Mitigation Activities			
Step Two		**Identify mitigation solution**	
	1	Select control for each mitigation risk	☐
	2	Apply 80/20 rule to risk register	☐
	3	Create 80/20 rule control report	☐
	4	Capture controls to risk register	☐
	5	Risk register acceptance by the board	☐

9.4.5 Risk Register

The risk register has to be completed with all the controls that have been selected. Those risks that are being mitigated need not be assigned a control. The top risks are listed first, with 80/20 rule risks listed thereafter. The register contains generic information to present its functionality.

Table 9.13: Risk register 2

Risk Register

Risk	Top Risk Y/N	Mitigation Solution	Control	CES
Risk 1	Yes	Transfer		
Risk 11	No	Mitigation	Anti-virus	R10 000

9.5 Create Action Plans

The creation of the action plan for each risk is the final submission of proof documentation to the board for approval of the preparation for reducing the information security risks of the environment. The action plan represents the culmination of the assessments and selections performed by the team, and should therefore not be a poor representation of the risk management process.

The action plan contains the following information, as required in Chapter 5:

- The risk mitigation strategy and control already identified
- The implementation cost of the control and CES
- The mitigation date
- The resources associated with the control/strategy
- The exposure response procedure
- The escalation procedure

Each section of the action plan must be completed before presentation to the board, with the exception of risks with no control assigned. Those risks still require the remaining sections to be completed.

9.5.1 The Mitigation Date

The mitigation date is used to indicate the date when the mitigation should be applied. The dates should be in order of most critical risk first, where controls apply, and urgent dates where transfer and termination of risks apply. In the case of termination, a strategy for change control should also be available to ease the organisation out of use of the asset.

The mitigation date is subject to approval from the board and should not be before the board or senior management forum date.

9.5.2 Resources Associated with the Control/Strategy

The staff members, or external resources associated with the strategies and controls of risks must be listed, e.g. in the case of transfer, the insurance firm. An example of a control resource would be a training resource for security awareness training.

9.5.3 The Exposure Response Procedure

The response to an exposed risk, or realisation of a threat, must also be described in the action plan. This applies especially in the case of risk avoidance. A contingency plan should be in place to recover lost assets, determine the extent of the damage and contact the appropriate resources for recovery.

This procedure applies especially in the case of opting for a strategy that does not effectively reduce the risk, or a control that does not prevent the exposure, but detects it. These procedures should be in place for the worst case exposure of the risk.

The following steps must be completed for including the exposure response procedure in the risk register:

1. Review the strategy of the risk:
    a. If the strategy is mitigation, is the control a preventative control, e.g. a security gate, or a reactive control, e.g. a security alarm? Continue to step 2.
    b. If the strategy is transfer or avoidance, continue to step 2.
    c. If the strategy is termination, no exposure response procedure is required.
2. Determine the first emergency reaction:
    a. For a preventative or reactive control:
        i. Assess the loss affected by the exposure.

ii. Inform the sponsor of the exposure and request authorisation of the risk appetite for recovery of the loss.

b. In the case of transfer:

i. Inform the sponsor of the exposure and request authorisation of the risk appetite for recovery of the loss.

ii. Contact the transferee for recovery of the appetite used.

c. In the case of avoidance, inform the sponsor of the exposure and request authorisation of the risk appetite for recovery of the loss.

3. Review the strategy for adaptation:

a. For a preventative control, strengthen the control.

b. For a reactive control, add a preventative control.

c. In the case of transfer, consider the application of a control.

d. In the case of avoidance, consider the application of a control, transfer or termination.

The strategy was recommended in Table 9.1. A risk that has been recommended for control should never be demoted to termination or avoidance if the applied control is not effective. The control must be strengthened.

9.5.4 The Escalation Procedure

The escalation procedure works hand in hand with the exposure response procedure. The staff resources that are responsible for the assets (as captured in the asset register) and the hierarchy leading up to the board or senior management forum must be included in the action plan.

The sponsor is always the first contact once an exposure has been discovered. Based on the exposure response procedure for each risk, the escalation path would include, for example, insurers for transfer and the board for authorising the use of the appetite amount.

9.5.5 Checklist

The checklist for this deliverable asks that an action plan be completed for each top and 80/20 rule risk (refer to Table 9.14). The action must be completed in all parts.

Table 9.14: Mitigation checklist 3

Mitigation Activities			
Step Three		**Create action plan**	
	1	For each risk, complete an action plan	☐

9.5.6 Risk Action Plan/Register

The updated risk register containing the action plan for the top risks and 80/20 rule risks should be presented to the board before continuing with the monitoring step in the risk management process (refer to Table 9.15).

Table 9.15: Risk action plan

Risk Action Plan							
Risk	**Mitigation Solution**	**Control**	**CES**	**Mitigation Date**	**Resources**	**Exposure Response Procedure**	**Escalation Procedure**

9.6 Conclusion

The risk management team is now prepared to mitigate risks and reduce the risk values on the risk profiles of the information assets. The action plans have been created that schedule the implementation of controls and other mitigation strategies.

This chapter has achieved the goals as stated. The goals are summarised below.

The chapter has provided the methods for identifying mitigation strategies by considering them against a table of impacts and probabilities of the risks. This table provides a logical approach to the selection of the strategy.

The method for selecting controls has been created to consider the cost benefit of the controls identified, as well as the cost of exposure saving. These two factors create a clear distinction for the selection of controls. These amounts are submitted to the board for approval. Pareto analysis has been used to determine whether there are lower valued risks that may be inadvertently mitigated by the implementation of a control. The CES is calculated to determine the saving of the control when implemented for multiple risks. The CES value presents the board with a conceptual win should they choose to fund the mitigation of the 80/20 rule risks.

Based on the approval of the board, action plans are created for the implementation of approved controls and strategies, including the implementation dates, exposure response procedures and escalation plans.

The exposure response procedure and escalation plans prepare the organisation for the advent of a risk exposure in the case of a transferred or avoided risk. The lack of a strong control is also managed and room is created for improving the strategy and control of the risk.

The chapter has also provided checklists ensuring that all tasks are completed before continuing with risk monitoring.

The information compounded in risk mitigation should provide the board with enough information to make an informed decision for approval of the budget for the launch of risk monitoring.

Chapter 10 continues with the methodology of risk monitoring.

C10 10 Risk Monitoring

10.1 Introduction

Risk monitoring, as the last step in the risk management process, is by no means the end of risk management. Risk management, as a governance responsibility, is a continuous function of the organisation and runs in a cyclical, step-based process.

Risk monitoring - as the name suggests - is a more passive step in the process when compared to identification, assessment and mitigation. It is also the most important step in the process. Risk monitoring is that business interest where the fluctuation of risks is monitored and controls put in place are watched for improvement of the risk register of the organisation.

Risk monitoring is also longer in duration when compared to the other steps, as there is no definite end to the step. Risk monitoring moves again to preparation after a predetermined period has passed. This period for the total cycle, as governance allows, is usually a calendar year [KING 2002]. This means that the full risk management process should be conducted on an annual basis.

The objective of this chapter is to present the Peculium methodology for risk monitoring.

The goals of the chapter are:

1. The method for including risk management and specifically monitoring in the day-to-day activities of staff
2. The method for maintaining the risk register with updated action plans and new assets
3. The method for measuring performance of the risk management process and the action plans using the key performance indicators identified in preparation

4. The method for monitoring measurement to determine the success of the monitoring phase
5. The method for maintenance of the business continuity plans inserted into the action plans
6. Checklists for the completion of the deliverables

The goals are based on the requirements listed in Chapter 5. The collective achievement of the goals constitutes the achievement of the objective.

The chapter begins with an overview of risk monitoring, with the remainder structured in the order of the deliverables listed above, except for the checklists that are presented throughout.

10.2 Overview of Risk Monitoring

Monitoring, as the ultimate state in risk management, is under-emphasised in IT governance and the security standard ISO 17799 (refer to the gap analysis performed in Chapter 5).

The current habits of the organisation are changed to improve security, and the systems architecture of the organisation is changed to accommodate the controls selected. Such changes are difficult to implement successfully without due emphasis of this step in the risk management process.

This change control and management is therefore the purpose of placing the incorporation of risk awareness into day-to-day activities as the first deliverable for risk monitoring. It is, for the operational levels of the organisation, almost the extent of risk monitoring, as the remaining deliverables are at a strategic level. The familiarisation of the BCPs also involves staff.

The growth of risk awareness, assurances to the board of implementation of controls and the awareness of BCPs all have impacts on the risk register of the organisation. For this reason, risks have to be reassessed, new risks identified and, as an organisation may have targeted only a portion of its operations, risk profiles created for the whole organisation, and their subsequent mitigation (refer to Figure 10.1).

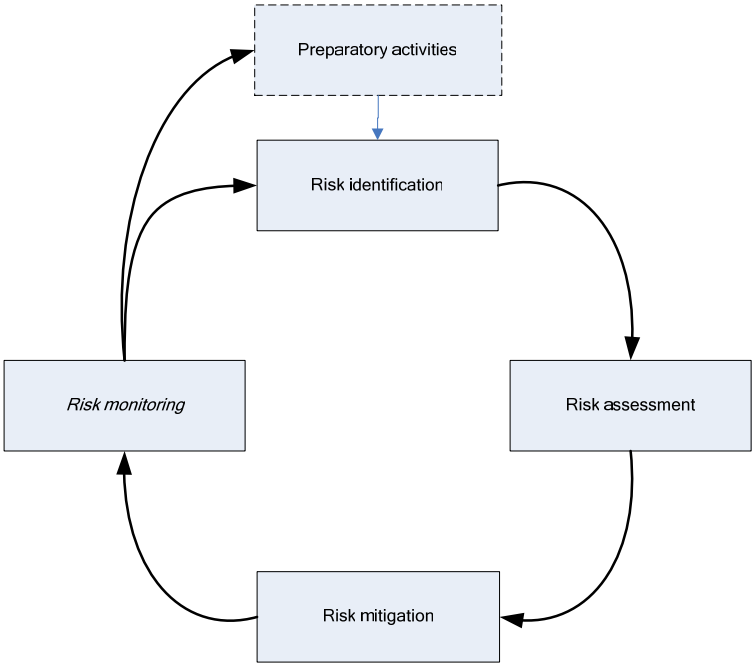


Figure 10.1: Risk monitoring in the risk management process

As reflected in Figure 10.1 above, the results of risk monitoring are used in both the preparatory activities and risk identification. The preparatory activities have to be revisited before continuing with identification.

The deliverables of monitoring are:

- Risk awareness included in day-to-day activities
- Risk register maintained
- Performance measured
- Monitoring measured
- BCPs maintained

The deliverables are not interdependent and may be conducted independently, except for the performance assessments accessing the risk register for updated action plans, and the measurement of monitoring including the performance assessment. Apart from these, the remaining deliverables are also in no particular order, or duration. The deliverables are repetitive, as demonstrated in Figure 10.2.

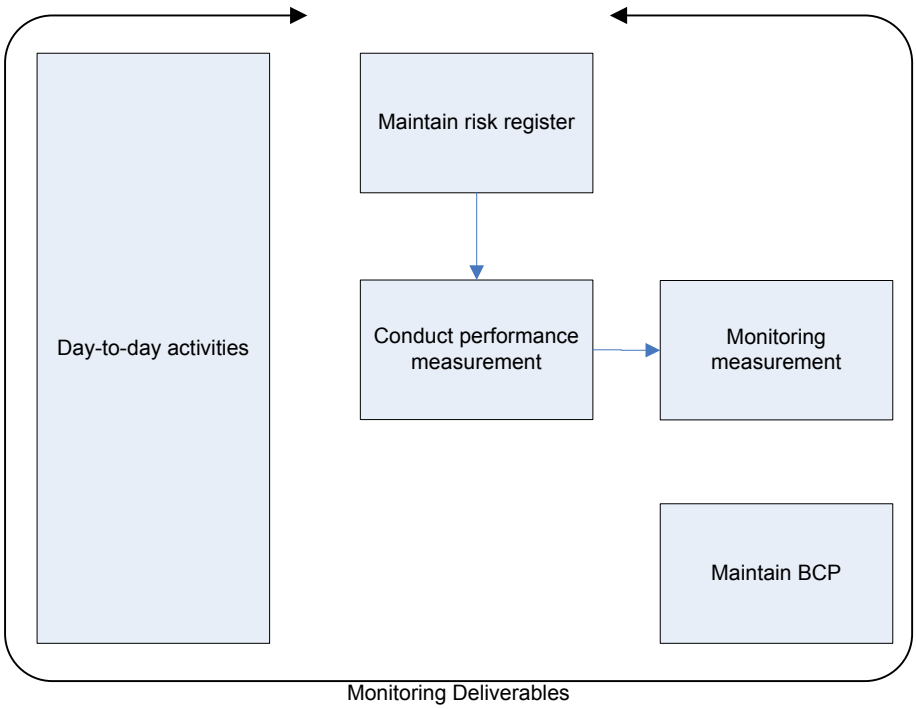


Figure 10.2: Order of completion of deliverables

As presented above, the day-to-day activities are not specifically linked to the other deliverables and are continuous throughout the monitoring step. The risk register has to be maintained for adequate performance measurement, and subsequently monitoring measurement.

The BCP has to be updated and maintained throughout the step as well.

10.3 Include Risk Awareness in Day-to-day Activities

The inclusion of risk awareness in the day-to-day activities of staff is a far greater challenge than what the title suggests. Any staff member is naturally opposed to change, unless the benefits outweigh the effort.

The benefits of risk management may not seem to staff as if they concern them, as an assigned team conducts the process and the board discusses the findings behind closed doors. It is therefore of vital importance that staff be involved in the process and feel ownership of the risks that affect the assets they may use, and the changes that will affect them.

10.3.1 Tasks of Risk Management Team

The risk management team should therefore work with the staff in the relevant risk management environment, and provide information on their progress as it is made.

The risk management team is therefore tasked with completing the following for all staff within the environment selected for risk management:

1. Conduct awareness training of the risks identified and their assessments.
2. The staff members have to understand the threats and vulnerabilities facing the assets, as well as the mitigation strategy identified for the asset.
3. The impact the mitigation strategy has on the operations of the environment must also be discussed and input requested from staff.
4. The staff members must be well trained in the process assigned to the asset for business continuity.

The risk management team and the staff members should also have regular sessions to ensure that the changes applied to the environment are welcomed and implemented and, if not successful, updated and communicated.

It is vital that the staff members buy in to risk management, as the greater majority of risks assessed usually stem from within the organisation [ALBE 2003].

The day-to-day activities do not cease with the end of the monitoring step; they continue unimpeded. The activities are implicit to every step of the process, although not indicated as a deliverable of each. This, of course, only applies after the first implementation of the risk management cycle.

10.3.2 Checklist

The checklist for this deliverable asks that staff be trained in the day-to-day activities of risk management and review sessions be held to monitor this change (refer to Table 10.1). All checkboxes must be checked before continuing to step two.

Table 10.1: Monitoring checklist 1

Monitoring Activities

Step One		**Include risk awareness in day-to-day activities**	
	1	Conduct awareness training	☐
	2	Ensure that risk profile is understood by staff	☐
	3	Ensure that impact of mitigation strategy is understood	☐
	4	Conduct business continuity process training	☐
	5	Hold sessions to review day-to-day activities	☐

10.4 Maintain Risk Register

The risk register created with information from identification, assessment and mitigation is a working document and is never complete. It is an active document that moves between the risk management team and the board.

The risk register, when last updated, contained the action plans for each of the top risks and the 80/20 risks. These action plans had due dates attached, as well as escalation plans, exposure responses and assigned resources.

These factors of the plans have been communicated to the board and are expected to be executed, the controls selected are expected to be implemented, and mitigation strategies that do not involve controls are expected to be carried out.

The plans also form a base for the performance assessments and monitoring assessments discussed later. It is vital that the risk register also be updated with new assets and their associated risks, as they are included in the environment. The new assets may not be set aside for assessment until the next iteration of the process, but must be assessed as soon as possible to ensure that the risks facing the highest valued assets are known across the environment.

10.4.1 Tasks of Risk Management Team

The risk management team is expected to maintain the risk register for the duration of the monitoring process. The tasks assigned to the team are as follows:

1. Maintain the asset register.
2. Maintain the risk profiles and create new profiles for new assets.

3. Maintain the risk register. Should new assets be at a higher value than those assets already being mitigated, continue the mitigation of assets by including the new assets. The top risks list can be expanded to include more risks. The mitigation of the initial top risks should not be abandoned for the new assets. The 80/20 rule should again be applied to any new controls that are selected for the new assets.

4. Maintain the action plans with updated information regarding the due dates for implementation of controls and the other mitigation strategies.

5. Communicate the updated register to the board, the environment's staff and the organisation as a whole. The training provided to the environment's staff, as shown in Figure 10.1, is not a once-off exercise, but continues throughout the monitoring step.

The risk management sponsor is ultimately responsible for these activities. The risk management team members should, however, act as watchdogs for new assets and inform the sponsor of the addition of the associated information to the risk register. The sponsor then presents the updated risk register to the board, as expected.

10.4.2 Checklist

The checklist for this deliverable asks that all profiles, registers and plans be maintained and communicated (refer to Table 10.2). All checkboxes must be checked before continuing to step three in the event of a new asset. The sponsor is responsible for ensuring that the checkboxes are left unchecked only if no new assets have arrived.

Table 10.2: Monitoring checklist 2

Monitoring Activities			
Step Two		**Maintain the risk register**	
	1	Update asset register	☐
	2	Update risk profiles	☐
	3	Update risk register	☐
	4	Update action plans	☐
	5	Communicate updates	☐

10.5 Conduct Performance Measurement

The performance of the risk management process to date should be measured in a manner which allows its continual updating based on the KPIs selected in the preparatory activities.

An easy way to measure the performance of the process is to create a dashboard or scorecard system that presents all the KPIs and their statuses. Such a system should be updated whenever a change is made, control implemented or new asset acquired to ensure that the information portrayed is a real-time representation of the process.

10.5.1 Risk Management Scorecard

The risk management scorecard, based on the KPIs identified earlier, must contain all of the KPIs. The scorecard is constructed to present a real-time informative status model of all the top and 80/20 risks being monitored.

The scorecard structure is recommended to be as follows:

Table 10.3: Risk management scorecard

Risk Management Scorecard			
Key Performance Indicator		**Due Date**	**Status**
1	Achieve milestone at each step of the risk management process		
1.1	Preparatory activities milestone achieved		
1.2	Identification milestone achieved		
1.3	Assessment milestone achieved		
1.4	Mitigation milestone achieved		
1.5	Monitoring milestone achieved		
2	Complete each deliverable at each step of the process		
2.1	Preparatory activities deliverables achieved		
2.2	Identification deliverables achieved		
2.3	Assessment deliverables achieved		
2.4	Mitigation deliverables achieved		
2.5	Monitoring deliverables achieved		
3	Present milestone summary to the board		
4	Complete asset register at the end of risk identification		
5	Complete risk register at the end of assessment		
6	Complete risk strategy at the end of risk mitigation		
6.1	Risk 1: Strategy A		
6.2	Risk 2: Strategy B		
6.3	Risk 3…5: Strategy C…E		

Key Performance Indicator	Due Date	Status
7 Complete action plan		
7.1 Risk 1: Control A		
7.2 Risk 2: Control B		
7.3 Risk 3…5: Control C…E		
8 Complete assessment report		
9 Update business continuity plan		

Table 10.3 presents the KPIs selected for the process and their due date assigned, and allows a status for each. The due dates are based on the expected duration of each step in the process and those assigned for implementation of control and other mitigation strategies.

The status of all the KPI defaults is not started at the beginning of the process, but should be updated as the steps are completed, and deliverables and milestones achieved.

The statuses suggested for use are:

- Not started: the KPI has not been attempted.
- Started: the KPI is in progress.
- Completed: the KPI has been successfully completed.

Each of these statuses is dependent on the due dates assigned and the process of risk management. Those KPIs that apply to later stages in the process cannot be attempted earlier, and should not be viewed as behind schedule until such time as the dependency is completed.

The statuses of the KPIs, although dependent on the due date, should not remain statically oblivious to the expiry of a due date. The statuses should therefore be colour-coded in the reports handed to the board:

- Status not started and past due: red
- Status started and past due: amber
- Status completed and past due: green

These colours create a traffic light representation of the statuses and are easy to recognise. The colours only come into effect when the dependency has been completed.

The scorecard should be available to the board in real time, i.e. accessible whenever required. The staff in the environment targeted must also be included in the communication of updates to the scorecard.

The risk management team is expected to maintain the scorecard on a regular basis, i.e. as soon as a KPI has been started, or completed. Ultimately, the responsibility for an up-to-date scorecard lies with the sponsor.

10.5.2 Determining Dependencies

The dependencies within the scorecard affect the traffic light representation of the completion of the indicators. As such, the dependencies need to be configured accurately to prevent an inaccurate and potentially damaging report from being given to the board. The obvious dependencies are presented in Figure 10.3. The dependencies between controls need to be determined by the risk management team.

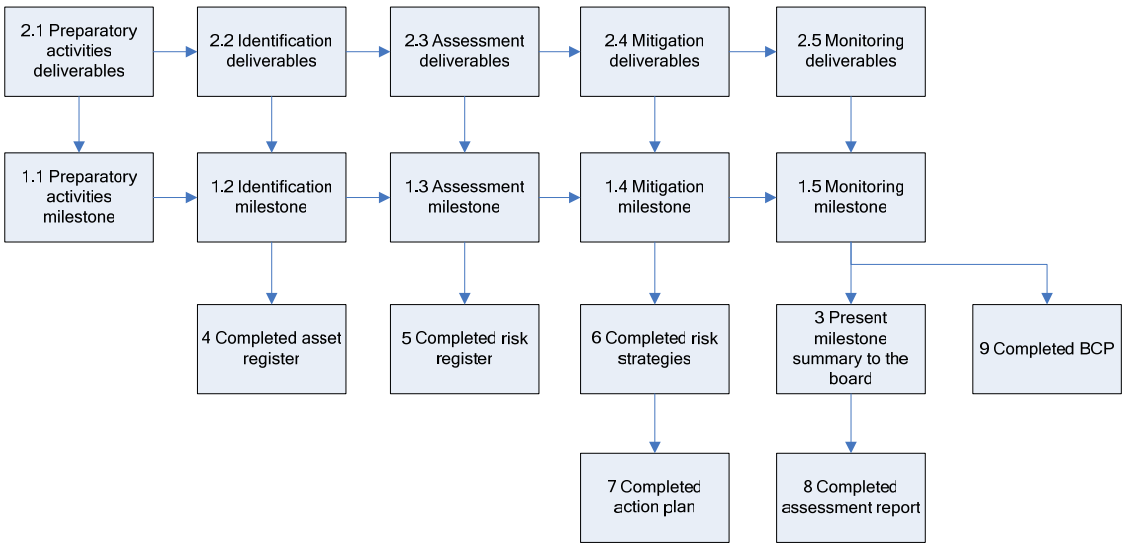


Figure 10.3: Dependencies in the risk management scorecard

10.5.3 Checklist

The checklist for this deliverable asks that the risk management scorecard be maintained and communicated (refer to Table 10.4). All checkboxes must be checked before continuing to the next iteration of the cycle.

Table 10.4: Monitoring checklist 3

Monitoring Activities			
Step Three		**Conduct performance measurement**	
	1	Maintain risk management scorecard	☐
	2	Communicate updated scorecard	☐

10.6 Measure Monitoring

Monitoring, as the most important step in the risk management process, is not adequately represented in the risk management scorecard. The activities in monitoring, as presented above, create a circular reference if included within the scorecard.

The performance of the activities within monitoring should be handed to the board separately to emphasise its importance, and ensure that it is given due consideration.

10.6.1 Report

The measurement of monitoring is therefore a compounded assessment report, including the following:

- Input received from staff during the awareness training and regular review sessions.
- The updated risk register, as and when updated with new assets, implemented controls and other tasks in the action plans.
- The risk management scorecard, as available at real time showing the progress of the process and the action plans. This is a one-page progress representation of the more detailed risk register.

This assessment report provides the board with the up-to-date information it requires to make a decision on the next iteration of the full process and the environment that will be selected for the process. The report is also a working document that must be updated regularly as the risk management scorecard is updated.

The board must, however, be aware that all controls and strategies implemented have to be reassessed in the next iteration of the process to determine to what extent the risks may have been reduced, and whether the return on investment was good.

10.6.2 Checklist

The checklist for this deliverable asks that the assessment report be created and communicated (refer to Table 10.5). Both checkboxes must be checked before continuing to the next cycle.

Table 10.5: Monitoring checklist 4

Monitoring Activities			
Step Four		**Measure monitoring**	
	1	Create assessment report	☐
	2	Communicate assessment report	☐

10.7 Maintain Business Continuity Plans

The exposure response procedures created in the action plans must always be easily accessible to the staff within the environment, and the plans well known to the staff, as included in their day-to-day activities.

These procedures or plans must be maintained and kept up-to-date at all costs, as the exposure of the vulnerability of an asset that is not properly protected due to whatever strategy was implemented may negatively impact the organisation. This is especially true for the SMME that has opted to transfer or avoid the risk, rather than invest in a control. The training of these plans must also be ongoing to ensure that the staff are trained for the latest business continuity procedures, and not a legacy version.

The risk management team is not responsible for creating the BCPs for the entire organisation. The exposure response procedures related to the specific risks identified for mitigation are added to an existing BCP. If no such plan exists, this task is changed to *Maintain exposure response procedures*.

Checklist

The checklist for this deliverable asks that the BCP be maintained, communicated and trained (refer to Table 10.6). The first checkbox only becomes compulsory when changes are required. The second checkbox must be checked before continuing to the next cycle.

Table 10.6: Monitoring checklist 5

Monitoring Activities			
Step Five		**Maintain BCP**	
	1	Update BCP	☐
	2	Communicate and provide training on BCP	☐

10.8 Conclusion

Risk monitoring, as the final step in the risk management process, provides a firm link between the board or senior management forum and the progress of risk management in the organisation.

The board or forum is provided with real-time information regarding the progress of action plans, performance reports of the mitigation of risks and the revelation of new risks, as well as an overall picture of the organisation's risk register.

In short, risk monitoring provides the board or forum with all the information required to make the preparatory activities in the next iteration easier. They have a clearer understanding of information security risk, a clear report on the mitigation of the highest rated risks and the data available to determine the return on the investment made in the mitigation strategies.

In the next iteration, the board will be able to adapt their objectives, key performance indicators, risk environment and team to generate improved information and risk management. The board will become more at ease with the process with every new iteration, and will have the power to assess and mitigate risks across the organisational business units.

The goals of this chapter have been achieved as follows:

- Risk awareness has been included in the day-to-day activities of staff by first training the staff, and then ensuring that they buy in to the changes required to increase the success of the changes.
- The risk register has been allowed to include new assets, threats, vulnerabilities and risk values. The risks, if at a high level, are added to the mitigation list, and no other high risks are moved off. This increases the cost of risk monitoring, but decreases the overall organisational risk.
- A performance measurement scorecard has been created that the risk management team must update as progress is made. This scorecard provides the board with real-time progress reports of the process. The scorecard is based on the KPIs selected by the board in the preparatory activities.
- A full assessment report is created that includes the scorecard, the updated risk register and all input received from staff related to the mitigation of risks. This information empowers the board even further with a real-time view of the detail of the process, as well as the staff acceptance of it.
- The BCPs, through the exposure response procedures, are also updated on a regular basis and staff are trained on the updates as they happen. This ensures that the staff members in the targeted environment are always prepared should risks be realised.
- Checklists have been created that ensure that all steps are completed before the process may reiterate. The assessment report and scorecard also graphically reflect when the steps have not been completed fully.

This chapter brings to an end the risk management process conceptually, although it has been made clear that the process should never end, but be reiterated annually. The process also becomes easier with each iteration as staff have increased awareness of risk and controls, and this reduces the vulnerabilities and threats from an internal human source and the duration of the initial steps of the process.

This concludes the Peculium Model in its presentation. A test of the model is presented in Appendix 5, which provides a step-by-step demonstration of the model in a real-world based SMME.

11 Conclusion

11.1 Revisiting the Problem Statement

The problem stated in Chapter 1 that led to the writing of this dissertation is the lack of enforced regulatory standards in the South African small, medium and micro enterprise environment.

This lack leads to ill-governed enterprises with a high failure rate and a low awareness of IT governance and information security risk management.

South Africa is also faced with the challenge of being a developing country, and thus may lack the high quality regulatory standards required to ensure success. As a further burden, those standards available to developed countries are not guaranteed to be applicable in South Africa, nor SMMEs in South Africa.

This poses a great challenge to SMMEs that have management with a goal of growing the business by applying good corporate and IT governance.

11.2 Steps to prove the Hypotheses and provide the Required Methodology

Through the dissertation hypotheses were articulated and challenges made to determine whether the problem statement was in fact valid and, if so, to provide a solution to the problem.

The first hypothesis stated was that South African SMMEs are distinctly different from those of other countries.

The second hypothesis challenged the applicability of existing corporate and IT governance standards to South African SMMEs.

If both of the hypotheses are true, and based on the ill fit of developed countries' methodologies, the last challenge was to create a model that would provide the necessary governance and yield viable results. This model had to

conform to the regulatory requirements of local governance standards and still provide a workable model for SMMEs.

The hypotheses results and achievement of the last challenge are described below.

11.2.1 Hypothesis One: South African SMMEs are Unique

The hypothesis regarding the definition of South African SMMEs was found to be proven. The method employed for proving the hypothesis included the following:

- Drawing a sample of developed and developing countries for comparison
- Obtaining the legal definitions of small enterprises in the samples
- Obtaining economic data for comparison in the samples
- Comparing South Africa's SMME definition and economic data to those of the sampled countries

The South African SMME definition was found to be very similar to the European Union's definition as used by the United Kingdom. There was, however, a distinct difference in the economic data. This information, together with the rest of the sample data from developed countries, reflected that small enterprises in the developed countries are economically more successful, and thus different from South African SMMEs, with their high failure rate and high figures of survivalist enterprises.

The developing countries, however, posed a different comparison of data. It was discovered that the developing countries do not have such stable economic development as was found in the developed countries. The countries also posed very different sets of inflation and GDP data from those of South African SMMEs. This again made it impossible to find common ground. South African SMMEs were thus found to be unique to the developing countries sample as well.

This led to the hypothesis that the applicability of these developed countries' regulatory standards to SMMEs as local standards is not appropriate.

11.2.2 Hypothesis Two: The Applicability of Corporate and IT Governance Standards to the SMME

This hypothesis was also proven that the corporate and IT governance standards applied to developed countries cannot be applied directly to South African SMMEs.

The proof followed a step-by-step process consisting of the following:

- Examining the local corporate governance standard, the King II Report of 2002, against the Australian corporate governance standard to determine its quality and international acceptance.
- Further examination of King II for usability in SMMEs.
- The examination of the internationally accepted IT governance standard, CobiT, for usability by SMMEs.
- The examination of international ISRM methodologies used for small enterprises for fit to South African SMMEs and advantages of them.

This proof forms a sizable part of the dissertation, known as Part 1, and provides a selection model and two frameworks for the examination as listed above.

11.2.2.1 Examining King II against Australia's Corporate Governance Standard

The King II Report, as described in Chapter 3, is the second version of the South African corporate governance standard. It has been found to be the most successful standard used in Africa and the Middle East, as South Africa yields the highest number of sustainability reports in the region. Although the number of reports is lower than the developed countries sample used, it is higher than in developing countries sample counterparts. King II was also found to be the accepted corporate governance standard for NEPAD.

King II was compared to the Australian Stock Exchange Corporate Governance Council's standard. A comparison was made of major factors in both standards, with the greatest difference found in the enforcement of reporting.

Another comparison was made of the sections of the standards, and the compared quality of each. King II performed well and is at a good standard of quality when compared to that of a developed country.

11.2.2.2 Examining King II for Usability in SMMEs

Each section of King II was evaluated for feasible applicability to SMMEs. A simplified guide was provided that allows the governance measures to remain, but at a lower cost to the enterprise and with less disruption in organisational productivity.

It is unfortunately a trait of corporate governance that effort has to be applied to reap the benefits.

The noticeable conclusion from the simplified standard was that risk management is vital, and that SMMEs, as organisations that can so easily be nullified, are managing the risks facing the systems on which they are so dependent.

11.2.2.3 Examining CobiT for Applicability to SMMEs

CobiT, as the international standard for IT governance, has been accepted to be the local standard as well. CobiT consists of six books and is made up of 34 control objectives.

It is understood that these 34 control objectives are not all compulsory, but that they do add value when applied. The challenge for the SMMEs, however, is how to decide which control objectives are suitable to the environment. This is no simple task for the business owner lacking in management skills. The full standard is not feasible for SMMEs.

For this purpose, a maturity model loosely based on the CobiT Capability Maturity Model was created which determines the maturity of the organisation's IT. Based on the result of this exercise, the organisation is guided in which controls should be applied.

The organisation with a very simple IT infrastructure would begin with an IT plan. This IT plan must correlate with the growth plans of the enterprise.

The levels of maturity, as they increase, eventually lead to an almost complete implementation of CobiT. This does, however, rest on the assumption that the enterprise already has certain controls in place, thus creating the maturity level. The controls selection framework also allows room for movement as the standard suggests.

11.2.2.4 Examining International ISRM Methodologies for Use by SMMEs

The examination of an internationally successful ISRM methodology is not a simple task. For this reason, a framework for evaluating these methodologies was created using information collected in previous chapters.

This framework was created in such a manner that SMMEs may use it for evaluating other undertakings as well. The framework was generically structured around three dimensions: the elements, their factors and their weights.

The elements of the framework were based on the definition of an SMME in South Africa, the regulatory requirements of corporate and IT governance, as well as the monetary cost of the undertaking, which is a major concern for any SMME.

Two methodologies were evaluated using the framework, and found to offer mediocre results. These methodologies were:

- The OCTAVE-S methodology specifically formulated for the small enterprise and based on the American OCTAVE methodology
- The CRAMM V Express software tool as a scaled-down, more affordable version of the CRAMM V Expert tool based on the British CRAMM methodology

The effectiveness or quality of the methodologies has not been questioned. The fit of the methodologies to South African SMMEs based on the framework dimensions was found to be lacking.

This proved the second hypothesis, and as a result required that a new methodology be created to conform to all the requirements created thus far, as well as offer a solution to the problem statement.

The evaluation did, however, offer a benefit as there are distinct advantages to both methodologies. These were used to create a requirements framework as the structure for the new methodology. The requirements framework was also supplemented with the regulatory requirements of corporate and IT governance. As a whole, the requirements framework provides a faster test for future evaluations of foreign methodologies.

11.2.3 The Peculium Model

The Peculium Model was based on the requirements framework as mentioned above and was structured to conform to the regulatory requirements included in the framework.

The Peculium Model has been divided into five steps of the risk management process, contrary to the existing norm of four. This was done to emphasise the importance of preparation for the active process, as the SMMEs are assumed not be highly skilled in the process or methodology of ISRM. These steps are:

- Preparation
- Risk identification
- Risk assessment
- Risk mitigation
- Risk monitoring

Each step is summarised below.

11.2.3.1 Preparation

The preparatory activities included in the first step of the process guide the organisation in obtaining all the required information, resources and training for the active steps of the ISRM process. Many of the activities are as a result of the influence of corporate governance on the requirements framework.

Major areas of interest in the step are the use of the balanced scorecard for standardising the representation of organisational objectives, the method for selecting a good representative team size for the undertaking and the training method of both full course and refresher training.

The first iteration of the process requires the preparatory activities to be completed fully. Next iterations will reduce the time requirement of the step as the board will already understand their role in preparing a team for the active steps of the process.

11.2.3.2 Risk Identification

The identification step in ISRM allows the risk management team to identify the environment for which the process is being performed, as well as the information assets present in the environment.

These assets may, however, be great in variety and number; as such, the assets undergo a weakness evaluation to determine those assets that are most suitable for a risk assessment and subsequent risk management. The evaluation also allows the SMME to reduce the cost of the process implementation by only continuing with those information assets that pose the greater threat to the environment.

The identification step provides the organisation with an asset register of the environment which includes the weakness values for future reference. This asset register forms the basis of the risk register that is used throughout the remainder of the process.

11.2.3.3 Risk Assessment

Risk assessment is performed to identify the threats to and vulnerabilities of the assets selected for the process in risk identification. These threats and vulnerabilities provide the necessary information for the risk management team to measure the impact of the threat, determine the probability of the exposure of the vulnerability and finally, based on this information, calculate the risk value of the threat to the information asset.

The methods employed for the various measures, calculations and determinations are a mixture of numerical qualitative and subjective qualitative methods. Subjective qualitative methods are used to determine the probability of the threat exposing the vulnerability of the asset. Numerical qualitative methods are employed to measure the impact of the exposure.

Impact is measured in such a manner that it considers not only financial loss due to the exposure, but also replacement cost, productivity loss and damage to the organisation's reputation. Reputation is very important to the SMME as it is a highly competitive market space.

The impact measurement employs calculations using financial and numerical figures. The results of these calculations determine the total qualitative representation of the impact considering the three areas as described above in equal measures.

The calculation of the risk values allows for numerical associations with the impact and probability measures. The standard formula for risk calculation, impact multiplied by probability, is used, resulting in numbers that are easily sorted for prioritisation of the risks that are planned for mitigation. The board of the organisation may decide whether they are satisfied to continue with a top five list of risks, or more.

All of the above information is added to the risk register, consisting of a risk profile for each of the information assets selected for the step.

11.2.3.4 Risk Mitigation

Risk mitigation consists of the identification of the mitigation strategy for the top risks nominated by risk assessment, selection of the controls for each and the planning of the actions that are taken to mitigate the risks.

The selection of the mitigation strategy is based on a recommendations framework that proposes the strategy most suited to the severity of the impact and probability of the risk.

Controls are selected using cost benefit analysis of the controls available to mitigate the risk. The cost benefit analysis considers the reduction in impact the control would facilitate, the cost of the control in cash, as well as the cost to productivity for the implementation of the control.

An additional function has been included, allowing the team to perform a Pareto analysis of the list of risks. This analysis allows the team to discover any other risks that may inadvertently be mitigated by those controls proposed for

mitigation of the top risks. The benefit of the implementation for the top risk and risks discovered through Pareto analysis is that it conceptually reduces the cost of the control.

This information allows the board to make a decision based on not only the monetary impact of the control, but also the return on investment in impact reduction. The risk management team may not continue with action plans for the risks until the board is satisfied with the strategies and controls selected.

The action plan for each risk includes the implementation of the strategy or control selected, and offers exposure response and escalation plans in the event that the risk is exposed before or after control implementation. Acceptance of these plans launches risk monitoring.

11.2.3.5 Risk Monitoring

Risk monitoring, as the longest step in the process, is more focused on maintaining the risk register and improving organisational awareness of risk than active tasks by the risk management team.

It is, however, the most important step in the process. It is in this step that the board can monitor whether the strategies and controls approved in risk mitigation are implemented as noted in the action plans, and that the risks are thus reduced.

The step also calls for the proactive maintenance of the risk register with any new assets that may have been acquired for the environment. These assets must also be assessed and mitigated, without the exclusion of any existing action plans. As such, the business continuity plan must also be updated.

The measurement of the success against key performance indicators identified in the preparatory activities is done using a scorecard system providing the board with real-time updates on the progress of the implementation of the action plans. The scorecard reflects whether the tasks are not started, started or completed, and uses colour-coding for schedule control.

This step in the process continues until the board calls for the second iteration of the process, albeit in the same environment or another. The information collected throughout the process is used as input into the new iteration.

11.3 Advantages and Limitations

The Peculium Model as described above is distinctly different from, but also similar to, other ISRM methodologies.

The Peculium Model, although following the basic structure of ISRM, allows the small organisation's board of directors or senior management to have control over the decisions made in the process, as well as receive periodic proof of progress.

This ensures that corporate governance is practised in the Model, but also that the board has buy-in and supports the process (refer to Figure 11.1). This support sets a good example to the staff of the small enterprise.

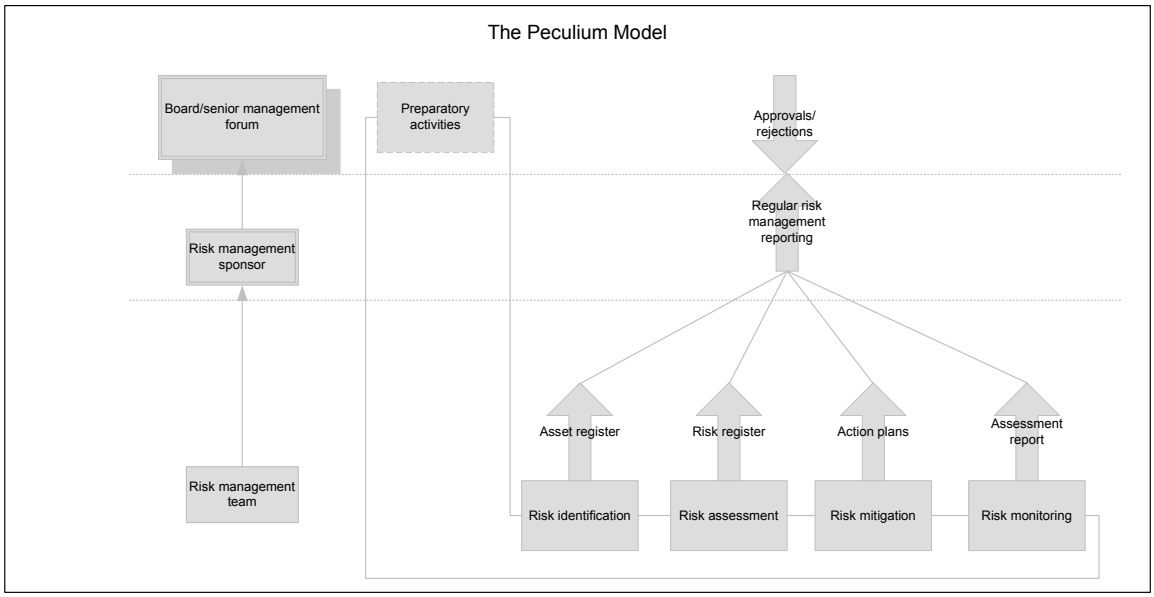


Figure 11.1: The Peculium Model

The Model also allows for simplified means of reaching values like the asset weakness value, the impact measurement and the risk values. The Model provides the scorecard for measurement against the key performance

indicators in an at-a-glance format, allowing the board easy access to a progress report.

Checklists ensuring the completion of all deliverables are also provided, controlling the completeness of the process. The Model has been created in a manner which eases each implementation by retaining the information gathered in the risk register for future use.

However, the Model has only been tested in a scenario environment and no certainty on the success of the Model in a real-world implementation is assured. The Model also rests on the completion of each deliverable before the next is attempted; the success of the Model lacking deliverables cannot be guaranteed.

The Model rests on the participation of the board or senior management forum. The lack of the participation of senior management in the support of the findings of the process and decision-making throughout the process is not tested for the purposes of the dissertation, and goes against the regulatory requirement. The lack of senior management participation will impede the process to a significant extent.

The Model has been created specifically to fit the South African regulatory and SMME environment, and as South African SMMEs are so unique, this Model cannot be guaranteed to be applicable to a small enterprise in another country.

11.4 Research Value

The literature study performed for the purposes of this dissertation has uncovered valuable findings regarding the economic stance of SMMEs in South Africa, as well as the quality of the corporate governance standard King II when compared to its Australian counterpart.

The angle of investigation, from the perspective of the small organisation, has opened new avenues for future research, specifically regarding the provision of regulatory standards for smaller enterprises, as well as the enhancement of methodologies that strengthen the organisations.

This dissertation has provided a model for investigating the fit of an undertaking to the small enterprise, providing the small enterprise owner with a tool to

determine whether the undertaking is a suitable one for the business. SMMEs have never before enjoyed such generic guidance tools in their business decision-making.

The Peculium Model has also provided SMMEs with a simple, yet focused solution to identifying the risks facing information assets in the SMME and methods for reducing them, without incurring huge costs.

As a whole, the dissertation notifies the academic community that SMMEs are a large untapped research environment where research projects can lend great assistance to the strengthening of SMMEs.

11.5 Future Research

As stated in the limitations, this dissertation did not include in its scope the testing of the Peculium Model in a real-world enterprise. Such a test could provide interesting research value that may improve the Model, or support the structure as is.

A further avenue for research would be to determine a version of the Peculium Model that is country-independent and that may be applied to any country's version of a small enterprise. Such a challenge would require an in-depth study of best practice on a global scale for both the regulatory side of the requirements framework and the methodology for ISRM.

A shortcut to the above would be the testing of the Model in various countries to determine whether it is successful in its current format, and to tabulate the challenges and shortcomings into a new requirements framework.

11.6 Closing Note

This is the end of a long journey that has allowed the growth and development of the author, as well as a great knowledge fount of learning regarding South African regulation and SMMEs.

The author thanks the academic community for their support and assistance.

12 Appendix 1: An evaluation of King II

The evaluation of the King II Report is provided in the section format of the report. The sections that are evaluated are:

- Introduction and Background
- Boards and Directors
- Risk Management
- Internal Audit
- Integrated Sustainability Reporting
- Accounting and Auditing
- Compliance and Enforcement

12.1 Introduction and Background

The introduction begins with the background of the King Report, which started with the King Committee in 1992. The first report was released in 1994 with the primary purpose of promoting the highest standards of Corporate Governance. The first report was groundbreaking in the sense that it emphasized the importance of the triple bottom-line, which encompasses economic, environmental and social aspects of the organisation [KING 2002].

The introduction continues with taking an important stance on the difference between accountability and responsibility. The report states that a director is accountable and must be able to justify an action. Responsibility is phrased as being liable to account to stakeholders. The term “responsible” has been added to the second report as the term “accountable” did not suffice in its previous role.

As an inclusive to the triple bottom-line, King II has enforced the consideration of customers, employees, suppliers and the community as stakeholders in the

organisation. As such, the purpose of the company must be defined, the values identified, and then communicated to these stakeholders. The concept of the community stakeholders also echoes in the sustainability reporting discussed later.

The concepts of Entrepreneurship and Enterprise are evaluated and recognised as factors driving business. It is presented that entrepreneurs are traditionally risk-takers and initiative thinkers. It is also warned though, that stakeholders should be considered and profitability balanced with enterprise. At the same instance, a balance should also be sought between enterprise and constraints. Due diligence to governance will allow the balance, thus promoting growth and profitability.

The next noticeable information transferred is more academic. It notes the organisational characteristics of the three corporate sins. These are listed as sloth, greed and fear.

- Sloth is the loss of flair, the enterprise gives way to administration
- Greed dictates decisions based on the short term for bonuses
- Fear is the sin of being subservient to investors, ignoring drive for sustainability and enterprise

The further academic content presents the characteristics of good Corporate Governance.

- **Discipline:** Correct and proper behaviour
- **Transparency:** Ease with which an outsider is able to make meaningful analysis of:
    - Company's actions
    - Economic fundamentals
    - Non-financial aspects pertinent to business
    - Measure of how good management is at making necessary information available in candid, accurate and timely manner (audit data, general reports, press releases). This is another valuable

statement. There are still many organisations that find it difficult to share information with operational level staff. The symptom of 'do it because I say so' is becoming less acceptable as staff are realising their right to have a stake in an issue that involved their daily working environment.

- **Independence:** The extent to which mechanisms are put in place to minimise potential conflicts of interest, such as dominance by a strong chief executive or large shareowner.
- **Accountability:** Individuals or groups in a company who make decisions and take actions need to be accountable for their decisions. Mechanism must exist and be effective to allow for accountability. They provide investors with means to query and assess actions of the board.
- **Responsibility:** Behaviour that allows for corrective action and for penalising mismanagement. The board is accountable to the company, must act responsively to and with responsibility towards stakeholders.
- **Fairness:** Rights of various groups have to be acknowledged and respected.
- **Social responsibility:** Placing high priority on ethical standards. A good corporate organisation is seen to be non-discriminatory, non-exploitative and responsible to environment and human rights. The organisation might experience improved productivity and good corporate reputation.

The characteristics, when applied should accompany the following outcomes of a well-governed organisation:

- Having clear majority outsiders on board, no management ties
- Holding formal evaluations of directors
- Directors with significant stakes, large portion of pay as stock options
- Being responsive to investor requests

The failure of Corporate Governance is presented to stem from:

- Weak legal and regulatory systems
- Poor banking regulation practices
- Inconsistent accounting and auditing standards
- Improperly regulated capital markets
- Ineffective oversight by corporate boards
- Scant recognition of rights of minority owners

The introduction conveys the concept of leadership for efficiency, probity and responsibility that is transparent and accountable.

12.2 Code of Corporate Practices and Conduct

The Code provides the guidelines of responsibility for the application of each of the sections in the report.

12.2.1 Boards and Directors

This section describes the composition of the board, highlighting the balance of executive and non-executive directors, which encompasses a majority if independent directors to protect the shareowners from bias. The creation of a nomination committee is promoted for the appointment to the board. This committee is also tasked with regularly evaluating board members for appropriate skills, experience and diversity.

The division of power between a chairperson and CEO is discussed, emphasizing that the CEO should not be chairperson, but that the chair be held by an independent party.

A very clear distinction is made between the concept of an executive director, non-executive director, and an independent non-executive director. The description of the independent director is on par with the Australian definition and is encouraged as majority of the board [ACCA 2004].

The report encourages fair remuneration of all executives on the board. A remuneration committee is suggested as the vehicle that evaluates the

framework of remuneration and the possibilities of share options and profit share.

12.2.2 Risk Management

It is immediately stated that the board is responsible for the total process of risk management as well as the evaluation of its effects. The board should implement risk management strategies in conjunction with management to ensure the day-to-day activities are integrated into the organisation.

Actual and potential risks should be identified, and each risk effectively managed. The Code makes no mention of avoiding risk. The board is responsible for disclosing its accountability for the process of risk management, that it is ongoing, that there is an internal control system in place to mitigate risks, and that any additional information required will be published in the annual report.

12.2.3 Internal Audit

The report emphasizes that the internal audit function is separated from external audit. An audit committee should be established with majority independent directors that evaluate the extent of the audit function.

12.2.4 Integrated sustainability reporting

The report once again takes into consideration the triple bottom-line in reporting. The annual reporting should include financial, social and environmental reports. The board determines that information which is disclosed. The reports are expected to include workplace conditions, the strategies in place to address and manage HIV/AIDS, environmental impact of the organisation, social investment and human capital development.

12.2.5 Accounting and Auditing

As stated previously, the audit committee should be in place to consider audit functions, and recommend the external auditor. The application of the committee should ensure an independent, impartial audit.

13 Appendix 2: A Summary of CobiT

13.1 Definitions

13.1.1 Control

“Control is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that desired events will be prevented or detected and corrected.”

This definition is complete in its description, although somewhat lengthy and heavily laden with terminology.

13.1.2 IT Control Objective

“IT Control Objective is defined as a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.”

This definition is not applicable to all the control objectives in the standard. The phrasing of the control objectives is more aligned with tasking, than stating a desired result or purpose, for example

- “Obtain Independent Assurance”, or
- “Develop and Maintain Procedures”

The definition might have been more apt if phrased to reflect that the control objective as a whole is a statement of purpose, and thus clears the confusion between control objective title, and the actual control objective.

13.1.3 Principles

The Framework principles rest on the requirements for information to support business requirements or objectives. Information is said to be a result of IT resources that are managed by IT processes.

13.2 Business Requirements of information

Quality requirements are listed as the quality, cost and delivery of the information. Fiduciary requirements apply to all information, and are listed as effectiveness and efficiency of operations; reliability of information; and compliance with laws and regulations. Security requirements are the standard elements of confidentiality, availability and integrity.

CobiT uses 7 principles, which are deduced from the abovementioned, some of which overlap [COBI01 2000]. These are:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability of information.

The entire above are defined adequately. They comprise the criteria with which all information should be evaluated for prioritisation. Any classification of data can also be based on which of the criteria it encompasses.

IT Resources

The following are defined as those resources that are used by IT processes in one form or another. Not all resources apply to all processes, and vice versa. The IT Resources are [COBI01 2000]:

- Data
- Application Systems
- Technology
- Facilities
- People

These are also defined adequately.

13.3 Domains

The four domains of CobiT are grouped together to conform to the standard life cycle of most processes, being the plan-do-check-act cycle. This was created to enable management to fit IT Governance into the regular flow of the other processes and governance methods.

13.3.1 Planning and Organisation

The Planning and Organisation domain covers any planning that goes into establishing IT Governance in the organisation. This includes drafting of policies, plans and such to enable the organisation to achieve their business objectives through their IT.

13.3.2 Acquisition and Implementation

This is the ‘do’ element of the cycle, where those policies and plans created in the ‘plan’ phase are put into practise. IT solutions are created to achieve the plans made.

13.3.3 Delivery and Support

In this domain, IT solutions are used to achieve the goals identified when drafting the IT strategies and plans. These solutions are supported for security, optimisation and others as required by the controls.

13.3.4 Monitoring

As with any monitoring phase, those steps taken have to be assessed for efficiency and effectiveness and decisions made as to whether the solutions in place work, or whether they need to be upgraded and/or altered.

These domains are comprehensive in the control objectives available, and no organisation is expected to make use of all the control objectives. There lies the challenge of determining which control objectives are functional for the organisation, keeping time and budget constraints in mind.

13.4 Control Objectives

There are 34 major control objectives that form part of CobiT. These control objectives are distributed over the domains mentioned previously. The organisation making use of CobiT may use its discretion in determining which control objectives are applicable to the organisation, but this decision can be time consuming, as all control objectives must be considered before making an informed decision.

13.4.1 Planning and Organisation

The Planning and Organisation domain consists of 11 control objectives, these are discussed below.

PO1. Define a Strategic IT Plan

1. Definition

Defining a strategic information technology plan to strike an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment.

It is enabled by a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long term plans should periodically be translated into operational plans setting clear and concrete short-term goals.

2. Critique

As with many facets of CobiT, the definition of a component is usually heavy in terminology, and lacking in visual accompaniment.

The understanding that can be obtained from the abovementioned is that several plans, and thus documents are created that ultimately form part of the business strategy. These plans are drilled down from high-level strategic plans, to operational plans with specific goals attached, to be achieved in a holistic deliverable for review at the next iterative strategic planning process.

As a result, much time is spent on the creation of these plans, and some energy must be put towards monitoring the execution of said plans. There is no specific reference made to these plans in the other domains concerning implementation or monitoring. The other domains are concerned with specifics and lose sight of

the holistic plan. The realisation that that CobiT is the holistic plan that is executed by the specific control objectives requires management cognisance.

PO2. Define the Information Architecture

1. Definition

Defining the information architecture of optimising the organisation of the information systems.

It is enabled by creating and maintaining a business information model and ensuring appropriate system are defined to optimise the use of this information.

2. Critique

This control objective concerns the technical composition of information as used by the organisation. The information architecture, as described here, is of a security concern, and must not be avoided at all.

PO3. Determine technological direction

1. Definition

Determining technological direction to take advantage of available and emerging technology to drive and make possible business strategy.

It is enables by creation and maintenance of a technological infrastructure plan that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms.

2. Critique

This control objective is in a peculiar position, as the very first control objective listed details the creation of a strategic IT plan. Determining the organisation's strategic IT direction should form part of the holistic strategic IT plan. If an organisation should blindly follow the CobiT model without previous study, repetition of management counsel would be required to follow this step. It becomes therefore imperative that any organisation considering CobiT should study the whole, before attempting the elements, and as a result implement it in its own manner (which is suggested at the very beginning).

This control objective is however extremely valuable when taking the role of IT Governance into consideration. The purpose of IT Governance is once again reflected here in stating that emerging technology drives the business strategy.

It is so important that organisation's carefully consider their technological options when discussing their business strategy.

PO4. Define IT Organisation and Relationships

1. Definition

Defining the IT organisation and relationships to deliver the right IT services.

It is enabled by an organisation suitable in numbers and skills with roles and responsibilities defined and communicated, aligned with the business and that facilitates the strategy and provides for effective direction and adequate control.

2. Critique

The control objective define here should not form part of a process, or a step following another, but should instead be a set policy in place when considering processes or steps.

Any organisation defines roles and responsibilities of its staff, whether formally or informally. The definition of IT roles and responsibilities should follow logically. This is also a task expected of every organisation to perform, both for its value in task ownership, and succession planning.

An organisation that has a stored record of all the roles and responsibilities of its staff, IT or otherwise, can more valuably map their disaster recovery processes due to the easy access to competency definitions. The document also provides the organisation with accountability Figures in any situation.

PO5. Manage the IT Investment

1. Definition

Managing the IT investment to ensure funding and control disbursement of financial resources.

It is enabled by a periodic investment and operational budget establishment and approved by the business.

2. Critique

This control objective is very clear in its entirety. Any businessman understands the importance of managing any investment. What is important here is that it is clear that IT is an investment, and not just a tool, or purchase. IT must be handled as a strategic part of business that undergoes justification studies for

cost and benefit. The definition of the control objective provides enough information for the business to proceed with it.

PO6. Communicate Management Aims and Direction

1. Definition

Communicating management aims and direction to ensure user awareness and understanding of those aims.

It is enabled by policies established and communicated to the user community; furthermore, standards need to be established to translate the strategic options into practical and usable use rules.

2. Critique

This is probably the most important control objective of all. There is no question whether any organisation should not communicate that which concerns the other stakeholders in the organisation.

Senior management buy-in is often emphasized, but equally important is operational staff buy-in. Revenue generating staff should be included in any business decisions that affect them, as they would be the most likely implementers or users of new business systems.

One method of formal communication that can be applied is the creation of policies and procedures surrounding the business change/ addition. It is however imperative that an organisation does not place full trust in such a passive mechanism. Measures should be in place to actively transfer knowledge to staff, considering options such as public address, awareness training and other methods.

PO7. Manage Human Resources

1. Definition

Managing human resources to acquire and maintain a motivated and competent workforce and maximise personnel contributions to the IT process.

It is enabled by sound, fair and transparent personnel management practices to recruit, line, vet, compensate, train, appraise, promote and dismiss.

2. Critique

This control objective seems strangely out of place in an IT Governance standard, as it should rather form part of Corporate Governance standard. It applies to the organisation as a whole, and not just to parts of the organisation involved in governing IT, or managing IT.

This control objective does however contain valuable guides as to managing the human resources of an organisation. No organisation owner/ senior manager should disregard its value.

PO8. Ensure Compliance with External Requirements

1. Definition

Ensuring compliance with external requirements to meet legal, regulatory and contractual obligations.

It is enabled by identifying and analysing external requirements for their IT impact, and taking appropriate measures to comply with them.

2. Critique

This control objective, strangely enough encompasses the role of this report. There are many standards of compliance in the industry, and requires an experienced auditor to determine the applicability of the standards to the organisation, and consequently audit the organisation for compliance. The mention of privacy, intellectual property and e-commerce sparks many flames of concerns for regulatory legislative compliance. An organisation should seek legal counsel when attempting e-commerce, and when claiming intellectual property.

PO9. Assess Risks

1. Definition

Assessing risks of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors.

It is enabled by the organisation engaging itself in IT-risk identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks.

2. Critique

This is an excellent control objective to form part of an IT Governance standard. It not only brings to light the facets of risk management, but also begins the detailed control objectives by aligning business risks associated with IT with the organisation's business objectives. By performing this step, the organisation realises how an exposure to risk may debilitate the business achieving an objective.

The terms assessment and identification are used loosely, with no clear differentiation between the two. This could prove to be confusing to the CobiT novice (refer to the clarification in Chapter 2).

The risk action plan suggested advises the reader to draft a plan which lists the risks and any means of mitigating exposure to the risks. It also makes it clear that the measures should be cost-effective. A risk analysis and consequent mitigation plan should never exceed the return on investment (ROI), as the organisation would lose faith in the practise, and not continue with reassessments.

It is also made clear that the controls implemented to mitigate the risks identified should be prioritised by maximum impact, and maximum ROI.

PO10. Manage Projects

1. Definition

Managing projects to set priorities and to deliver on time and within budget.

It is enabled by the organisation identifying and prioritising projects in line with the operational plan and the adoption and application of sound project management techniques for each project undertaken.

2. Critique

Project management is becoming an increasingly important function in any business as the benefits of detailed planning; deliverable identification and objective declarations have increased the success of new ventures, added organisational functions, implementation of new systems and general due diligence.

Many organisations are applying project management techniques to various facets of the business, and are becoming more aware of the organisation's business objectives through researching what the projects are aimed to achieve.

There are many facets to project management, as identified in the PMBoK [PMBO 2004]. How these are presented here is quite different. The order of the detailed control objectives is once again rather confusing, as risk management is discussed after phase approval. A project should not be launched if the risks are too great to be effectively mitigated.

It is however a good sign that post-implementation review is discussed, as this is a tool of governance that allows perpetual enhancement of methods applied.

The core areas of project management, being cost, schedule quality, and integration, are not emphasized enough, as these are the ultimate purpose of extensive planning. The extent to which planning is performed determines whether the constraints are abided by in the long run.

PO11. Manage Quality

1. Definition

Managing quality to meet IT customer requirements.

It is enabled by the planning, implementing and maintaining of quality management standards and systems providing for distinct development phases, clear deliverables and explicit responsibilities.

2. Critique

This is a very extensive control objective, as it covers various areas of quality assurance, including various tests and system development life cycle features. It is a very important part of IT Governance, as it creates control over IT in the organisation. IT creates control over the development of systems to ensure they are quality systems. Governance is control. Quality assurance therefore embodies the success of IT Governance.

Quality assurance is resource intensive, and requires a lot of input form various parties to ensure it works. Quality control standards (ISO series) might also be considered for assured implementation of the quality standards.

13.4.2 Acquisition and Implementation

The Acquisition and Implementation domain of six control objectives, these are discussed below.

AI1. Identify Automated Solutions

1. Definition

Identifying automated solutions to ensure an effective and efficient approach to satisfy the user requirements.

It is enabled by an objective and clear identification and analysis of the alternative opportunities measured against user requirements.

2. Critique

This objective expects the organisation to research, compare and propose solutions for automation. An organisation may not be empowered with reasonable knowledge of IT systems to conduct such research effectively. The organisation may need to approach a knowledgeable third party.

AI2. Acquire and Maintain Application Software

1. Definition

Acquiring and maintaining application software to provide automated functions which effectively support the business process.

It is enabled by the definition of specific statements of functional and operational requirements and a phased implementation with clear deliverables.

2. Critique

This objective provides some guidelines to the implementation of the solution identified in AI1 as most suitable. It again allows a project based introduction of the system to the users, and also emphasizes that the system should be acquired based on specific requirements of users. This could be a challenge, as users should be made aware that their requirements have to be all encompassing and specific to ensure they receive a system that provides all the services they require.

AI3. Acquire and Maintain Technology Infrastructure

1. Definition

Acquiring and maintaining technology infrastructure to provide the appropriate platforms for supporting business applications.

It is enabled by judicious hardware and software acquisition, standardising of software, assessment of hardware and software performance and consistent system administration.

2. Critique

The implementation of this control objective should be performed by an IT professional, as it clearly requires knowledge of hardware and software standardisation. The IT professional is held responsible for recommending standards for the systems, and upon management approval, implementing those standards.

AI4. Develop and Maintain Procedures

1. Definition

Developing and maintaining procedures to ensure the proper use of the application and the technological solutions put in place.

It is enabled by a structured approach to the development of user and operations procedure manuals, service requirements and training materials.

2. Critique

This control objective requires collaboration between management and the IT professional to ensure that the procedures are technologically correct, and their use supported by management. The procedures and manuals need to be transferred to users in an active manner to ensure application and justification of the time spent of creating the manuals.

AI5. Install and Accredit Systems

1. Definition

Installing and accrediting systems to verify and confirm that the solution is fit for the intended purpose.

It is enabled by the realisation of a well-formalised installation migration, conversion and acceptance plan.

2. Critique

The requirements obtained during AI1 circumvents this control objective if performed with due diligence. If, however, the realisation is reached that AI1 was not performed effectively, this control objective becomes helpful.

AI6. Manage Changes

1. Definition

Managing changes to minimise the likelihood of disruption, unauthorised alterations and errors.

It is enabled by a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the exiting IT infrastructure.

2. Critique

The management of change, or change control should be mapped early in the strategic IT process. Change management procedures need to be communicated to staff before a change is required. This control objective is placed in a ‘do’ domain, but should have been included in planning as well. It does bode well for CobiT that it has been included.

13.4.3 Delivery and Support

The Delivery and Support domain of 13 control objectives, these are discussed below.

DS1. Define and Manage Service Levels

1. Definition

Defining and managing service levels to establish a common understanding of the level of service required.

It is enabled by the establishment of service-level agreements which formalise the performance criteria against which the quantity and quality of service is measured.

2. Critique

This control objective as it stands fits very much into the corporate environment of the large organisation with a large IT department handling various requests from staff. Regarding IT Governance, it is rather operational, but still creates a

level of control with regards to user expectations and services offered to the users.

DS2. Manage Third-Party Services

1. Definition

Managing third-party services to ensure that roles and responsibilities of third-parties are clearly defined; adhered to and continue to satisfy requirements.

It is enabled by control measures aimed at the review and monitoring of existing agreements and procedures for their effectiveness and compliance with organisation policy.

2. Critique

Management of third-party services could easily have been included in the previous control objective, as service level agreements should be created in conjunction with third-party providers if they are present. The creation of service levels should not be done before the third-party providers have been qualified and selected. Once again the need of complete study of CobiT is required to ensure no duplication of effort is expended.

DS3. Manage Performance and Capacity

1. Definition

Managing performance and capacity to ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs.

It is enabled by data collection, analysis and reporting on resource performance, application sizing and workload demand.

2. Critique

This is a definite control mechanism where the service levels are tested for performance, and the systems in place are tested for performance versus demand. This exercise can also shed light on the standardisation of hardware and software performed in planning and organisation. The results of this analysis can be used to adapt the standards at the next cycle of IT Governance. This is a valuable control objective that provides tangible information for budgeting and strategic planning related to IT.

DS4. Ensure Continuous Service

1. Definition

Ensuring continuous service to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption.

It is enabled by having an operational and tested IT continuity plan which is in line with the overall business continuity plan and its elated business requirements.

2. Critique

This control objective is glaringly out of place in this domain. An IT continuity plan should most definitely not be drafted during the delivery of IT services. The continuity plan should be created and tested during planning.

The operational implementation of disaster recovery might have been a more apt description for placing a control objective of this nature in delivery and support.

DS5. Ensure Systems Security

1. Definition

Ensuring systems security to safeguard information against unauthorised use; disclosure or modification; damage or loss.

It is enabled by logical access controls which ensure that access to systems, data and programmes is restricted to authorised users.

2. Critique

This control objective is also out of place. A control objective in acquisition and implementation, develop and maintain procedures, can easily be used as vehicle for security procedures. The mechanisms identified in acquisition and implementation allows for the creation of the security procedures or policies, as well as their implementation and maintenance. The workload of the two control objectives can be combined and as such and the required communication reduced.

DS6. Identify and Allocate Costs

1. Definition

Identifying and allocating costs to ensure a correct awareness of the costs attributable to IT services.

It is enabled by a cost accounting system which ensures that costs are recorded, calculated and allocated to the required level of detail and to the appropriate service offering.

2. Critique

This control objective is very closely linked to the planning and organisation objective of strategic IT planning. Steps should be taken throughout the fiscal year to record cost of IT against the budget identified, and managing of any unforeseen expenditure. These recordings will assist management in creation of the next IT Strategy by basing the continuing costs on those recorded, and basing strategic additional costs on the unforeseen costs recorded.

DS7. Educate and Train Users

1. Definition

Educating and training users to ensure that users are making effective use of technology and are aware of the risks and responsibilities involved.

It is enabled by a comprehensive training and development plan.

2. Critique

This control objective has significant ties with procedural communication and business continuity/ disaster recovery planning. Any procedures or plans created have to be transferred to each user, either by awareness training or by involvement in creating the plans.

This objective is of utmost importance and should be applied by any organisation.

DS8. Assist and Advise Customers

1. Definition

Assisting and advising customers to ensure that any problem experienced by the user is appropriately resolved.

It is enabled by a helpdesk facility which provides first-line support and advice.

2. Critique

This objective is also out of place as the definition confuses a customer with a user. It is assumed that the user becomes the customer of the helpdesk described.

The functions of the helpdesk should have been included in the control objective determining the service levels. It does have its slot in this domain due to its support nature. This connection to the service levels should be identified to prevent redundancy.

DS9. Manage the Configuration

1. Definition

Managing the configuration to account for all IT components, prevent unauthorised alterations, verify physical existence and provide a basis for sound change management.

It is enabled by controls which identify and record all IT assets and their physical location and a regular verification programme which confirms their existence.

2. Critique

This control objective creates a firm tie with the auditing and accounting function described in Corporate Governance. Maintenance of an asset register is required by external auditing to justify IT spend with the assets identified and use of those assets. The responsibility of maintaining these registers should however be delegated to an individual knowledgeable of the IT systems in place, but reported in a language accessible by the external auditor.

DS10. Manage Problems and Incidents

1. Definition

Managing problems and incidents to ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence.

It is enabled by a problem management system which records and progresses all incidents.

2. Critique

This control objective also connects to the service levels and assistance of customer concepts. The operational resolution of problems will be allocated through the helpdesk. Adequate systems should also be provided to the helpdesk to record and progress incidents. A further suggestion is the use if a knowledge management system that allows searchable recording of problem solutions for future use.

DS11. Manage Data

1. Definition

Managing data to ensure that data remains complete, accurate and valid during its input, change and storage.

It is enabled by an effective combination of application and general controls over IT operations.

2. Critique

This control objective allows for the cognisance of the integrity of data, one of the information security services. It does not however recognise availability or confidentiality, which is rather alarming.

This control objective does however highlight the accuracy and validation of data during its creation and storage. Proof of successful measures that allow this protects the reporting portion of Corporate Governance, and lends credibility to the reporting mechanisms.

DS12. Manage Facilities

1. Definition

Managing facilities to provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards.

It is enabled by the installation of suitable environment and physical controls which are regularly reviewed for their proper functioning.

2. Critique

This control objective would be more suited to both planning and organisation and acquisition and implementation. Decision of which infrastructural controls are required should be considered with business continuity planning and the IT

strategy. An organisation cannot plan its physical controls for protection of its IT after the budgets have been assigned.

The testing of controls and subsequent installation should then form part of other acquisitions and implementations.

DS13. Manage Operations

1. Definition

Managing operations to ensure that important IT support functions are performed regularly and in an orderly fashion.

It is enabled by a schedule of support activities which is recorded and cleared for the accomplishment of all activities.

2. Critique

Operational implementation of service levels should not be defined this far into IT Governance. The creation of service levels should include the scheduled functions that are to be performed, and the frequency that is decided upon. The execution of those operations is in the correct domain, but not the creation of the operations and their schedules.

13.4.4 Monitoring

The Monitoring domain contains 6 control objectives, these are discussed below.

M1. Monitor the Processes

1. Definition

Monitoring the process to ensure the achievement of the performance objectives set for the IT processes.

It is enabled by the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting upon deviations.

2. Critique

This is an excellent inclusion and should be applied throughout the IT Governance cycle. It allows the creation of measures in the planning process, and creates the room for reporting and resolving shortcomings throughout the cycle.

M2. Assess Internal control Adequacy

1. Definition

Assessing internal control adequacy to ensure the achievement of the internal control set for the IT processes.

2. Critique

This control objective could have been included in the previous, more global objective, by identifying internal control as a process, which it is.

It has however been separated to emphasize and ensure that internal controls are included and do not disappear into a multitude of processes and is not afforded due diligence.

M3. Obtain Independent Insurance

1. Definition

Obtaining independent insurance to increase confidence and trust among the organisations, customers ad third-party providers.

It is enabled by independent assurance reviews carried out at regular intervals.

2. Critique

This measure allows the accreditation and certification of an organisation as being compliant with the regulations in place. Such regulations can be supplied by government or international bodies. Examples of such regulations are those of the ISO 17799, the ECT Act, and CobiT itself.

The only confusion in this objective is the use of the tem customer. In this instance it seems to relate to external parties making use of the organisations services or products.

M4. Provide for Independent Audit

1. Definition

Providing for independent audit to increase confidence levels and benefit from best practise advice.

It is enabled by independent audits carried out at regular intervals.

2. Critique

The functions described in this control objective link very closely with the previous. It is suggested the two are combined.

14 Appendix 3: CobiT Control Objectives Selection Guidelines

14.1 Control Objective Selection Guidelines

The following guidelines have been created to assist in identifying the scale of requirement for IT Governance, or alternatively put, the control objectives that should be implemented. A framework loosely based on the CobiT Capability Maturity Model is used to answer questions pointed at the IT Governance attitude of the organisation and the availability of its resources [COBI04 2000].

The guidelines follow a 4-step process to determine the organisation's IT Governance maturity level.

14.1.1 Identify the Organisation's IT Resource Management Maturity

By identifying the organisation's maturity an understanding can be reached of the scope of control objectives required. If an organisation is mature at level 5, a smaller contingent of objectives would be required and visa versa.

Has the organisation identified that there is a requirement for IT Governance?

0 No	The organisation is not concerned with managing its IT as a resource.
1 Initial	The organisation is aware of a lack of control of their IT resources.
2 Repeatable	The organisation has investigated the process of establishing control processes.
3 Defined	The organisation has defined control processes and has trained its staff.
4 Managed	The organisation measures the performance of the control processes and re-evaluates a process after the problem has been addressed.

5 Optimised	Control processes are formally defined and do not have any defects. IT resources are effectively managed and used.

14.1.2 Identify the level of authority by organisation owners or managers

The level of authority of business owners or managers would determine the amount of staff buy-in that may be obtained. An organisation unaccustomed to authority may not be easy to convince of an organisational shift in regard of IT resources.

Does the organisation have a formal management structure?

0 No	The organisation is not formally controlled and does not invite potential expansion.
1 Initial	The organisation practices basic management principles such as staff meetings and capital expense control and harbours potential for growth.
2 Repeatable	The organisation has a management team that monitor organisational performance and investigates opportunities for growth.
3 Defined	The organisation has a formal management forum that is accountable for the organisation's development. This forum is the authority on growth decisions. Staff has awareness of the role of the forum and are notified of significant happenstance.
4 Managed	The organisation measures the performance of the management forum. Management might be supplemented by independent advisors/ directors that monitor the performance of the organisation. The management forum produces formal documentation of the financial standing of the organisation which is presented to the directors/ shareholders.
5 Optimised	The organisation has a clearly defined hierarchy of management that encourages staff participation in organisational shifts, as well as the delegation of organisation management. The senior managers are highly skilled and competent. Staff opinions are valued and addressed. Formal documentation is produced presenting the

financial, social and environmental standing of the organisation.

14.1.3 Level of technological sophistication in the organisation

The level of technology used in the organisation will affect the control required of the systems in place. The greater the sophistication, the lower the resources required to control them.

What is the level of technological sophistication?

0 None	The organisation does not make use of technology as a resource.
1 Initial	The organisation makes use of technology is its simplest form and can continue manually if required.
2 Repeatable	The organisation has simple system in place managing its data. The systems do not have a continuity solution but does have paper-based alternative.
3 Defined	The organisation has systems specifically developed for the organisation and uses machines that can cope with the requirement.
4 Managed	The organisational systems have a structured maintenance cycle and are of a high standard. The machines are regularly maintained and have room for technological expansion if so required.
5 Optimised	The organisational systems are well maintained and have a strict level of standard. The organisational data is stored in a secure manner with a defined recovery procedure. The machines are of the highest standard and are rotated regularly to manage productivity requirements.

14.1.4 Technology/Information Risk Profile

The awareness of a risk profile may increase the consideration of decisions made and steps taken concerning the risk area. In the case of technology/ information risk, awareness may create carefulness with data storage as an example.

Is the organisation aware of a technology/ information risk profile?

0 No	The organisation has not considered risk to its technology/ information.
1 Initial	The organisation is aware that risks may exist but have identified a profile.
2 Repeatable	The organisation is aware of the risk profile but has not taken any mitigating steps.
3 Defined	The organisation is aware of the steps that need to be taken to mitigate some risks in the risk profile.
4 Managed	The organisation mitigates its risks and regularly updates the risk profile.
5 Optimised	The organisation invests resources into a formal risk evaluation, mitigation and management process and documents the process for publishing.

The model used above is now used to tabulate the control objective application ranges used to identify those control objectives most suited to the organisation range. The range is reached by adding the model values selected in each of the 4 questions above.

Table 14.1: The control objectives applicability ranges

Range	Range Definition
0	This range includes organisations that are not dependent on IT resources and are not expecting growth in the organisation. These organisations are excluded henceforth.
1 – 8	These organisations are aware that more focus on its IT resources are required, and that actions and not intentions bear

	results.
9 – 12	These organisations have made progress in their IT Governance and needs formalisation of the outcomes of their efforts.
13 - 20	These organisations have well-defined and structured control processes in place and are in an overall control phase.

The control objectives identified as applicable were selected considering the following assumption:

- Any control objective attempted should be done in a workshop environment allowing staff participation. As control objectives do require resources, buy-in becomes paramount.

The growth of the organisation from one maturity level to another should follow the "define process, implement sophistication, monitor process" route as demonstrated in Table 14.1.

The maturity levels[16] of define process, implement sophistication; monitor process can be expanded as follows:

- **Define process** selects the initial control objectives required for formalise the organisation's intended use of IT, assessing the risks the organisation faces, managing those resources required, developing service levels, formalising change and incident response structures and monitoring these initial steps during the process
- **Implement sophistication** creates room for the organisation to improve the policies and procedures already in place. This includes the acquisition of improved systems, higher levels of service delivery, more control over IT resources and improved monitoring of IT. This step involved the largest requirement of resources, as it lifts the organisation from acceptable control to sophisticated control.

[16] The terms maturity level and ranges are interchangeable as follows:
- Maturity level 1 is range 1 – 8
- Maturity level 2 is range 9 – 12
- Maturity level 3 is range 13 - 20

- **Monitor process** is the maintenance of the sophistication reached in the previous level. An organisation rated at this level already may require some backtracking if some of the sophistication markers are not in place. This level is least resource intensive, but may require increased resources if the required input for maintenance is not upheld.

The control objectives selected for the levels were chosen using judgment of the flow of sophistication. Some control objectives may seem controversial in their applicability to the maturity level. An example of such a controversy is the inclusion of *Manage Projects* in the first level. This control objective has been included as a defining control, as much of the implementation of control objectives requires management of resources, time, cost and integration into the existing organisation. These are the main themes of project management [PMBO 2004]. A controversial exclusion example is the exclusion of *Assist and Advise Customers* from the first level. This has been excluded as application of the grouped define controls should be done internal to the organisation. Inclusion of customers into changed control should only be considered once internal control has stabilised.

Table 14.2: Recommended use of CobiT by an SMME

Control Objective	1- 8	9 – 12	13 - 20
Planning and Organisation			
Define a strategic IT plan	●	●	●
Define the information architecture		●	
Determine technological direction	●	●	
Define the IT organisation and relationships	●	●	
Manage the IT investment		●	●
Communicate management aims and direction	●	●	●
Manage human resources	●	●	●
Ensure compliance with external requirements		●	●
Assess risks	●	●	●
Manage projects	●	●	●
Manage quality		●	●
Acquisition and Implementation			
Identify automated solutions		●	
Acquire and maintain application software		●	
Acquire and maintain technology infrastructure		●	
Develop and maintain procedures	●		
Install and accredit systems		●	●
Manage changes	●	●	●
Delivery and Support			
Define and manage service levels	●	●	
Manage third party services	●	●	
Manage performance capacity	●	●	
Ensure continuous service	●	●	●
Ensure system security	●	●	●
Identify and allocate costs	●	●	●
Educate and train users	●	●	
Assist and advise customers		●	
Manage the configuration			●
Manage problems and incidents	●	●	●
Manage data	●	●	●
Manage facilities		●	●
Manage operations	●	●	●
Monitoring			
Monitor the processes	●	●	●
Assess internal control adequacy	●	●	
Obtain independent assurance		●	●
Provide for independent audit		●	●

15 Appendix 4: ISO 17799 threats and vulnerabilities lists

15.1 ISO 17799 Threats List

The ISO 17799 threats list has been reordered to the categories as defined in Chapter 8.

External human

- Bomb attack
- Communications infiltrations
- Damage to cabling
- Eavesdropping
- Industrial action (strike)
- Masquerading of user identity
- Network access by unauthorised persons
- Theft
- Traffic analysis
- Wilful damage

External system

- Malicious software
- Misrouting or rerouting of messages

Internal human

- Communications infiltrations
- Damage to cabling
- Illegal software
- Illegal use of software
- Industrial action (strike)
- Maintenance error
- Misuse of resources
- Network access by unauthorised persons
- Operational support staff error
- Repudiation
- Staff shortage
- Theft
- Traffic analysis
- Unauthorised use of software
- Unauthorised use of storage media
- Use of network facilities in unauthorised manner
- Use of software by unauthorised users
- Use of software in unauthorised manner
- User error
- Wilful damage

Internal system

- Air conditioning failure
- Deterioration of storage media

- Failure of network components
- Hardware failure
- Software failure
- Traffic overloading
- Transmission errors

Other

- Airborne particles/ dust
- Earthquake
- Environmental contamination
- Extreme temperatures
- Failure of telecoms services
- Failure of water supply
- Failure of power supply
- Fire
- Flooding
- Lightning
- Power fluctuation

15.2 ISO 17799 Vulnerabilities List

The ISO 17799 list of vulnerabilities is as follows:

Personnel security

- Absence of personnel
- Unsupervised work by external staff, e.g. cleaning staff
- Insufficient security training
- Lack of security awareness
- Poorly documented software
- Lack of monitoring mechanisms
- Lack of policies for the correct use if information assets and telecommunications
- Inadequate recruitment procedures

Physical and environmental security

- Inadequate or careless use of physical access control to building, rooms and offices
- Lack of physical protection for the building, rooms and offices
- Location in an area susceptible to flood
- Unprotected storage
- Insufficient maintenance of storage media
- Lack of periodic equipment replacement schemes
- Susceptibility of equipment to dust
- Susceptibility of equipment to temperature variations
- Susceptibility of equipment to voltage variations
- Unstable power grid

Computer and network management

- Unprotected communication lines
- Poor joint cabling
- Lack of identification and authentication mechanisms
- Transfer of passwords in clear text
- Lack of proof when sending or receiving messages
- Dial-up lines
- Unprotected sensitive traffic
- Single point of failure
- Inadequate network management
- Lack of care at disposal
- Uncontrolled copying
- Unprotected public network connections

System access control, development and maintenance

- Complicated user interface
- Disposal or reuse of storage media without proper erasure
- Lack of audit-trail
- Lack of documentation
- Lack of effective change control
- Lack of identification and authentication mechanisms
- No logout when leaving a workstation
- No or insufficient software testing
- Poor password management
- Unclear or incomplete specification for developers
- Uncontrolled downloading and using software

- Unprotected password Tables
- Well-known flaws in software
- Wrong allocation of user access rights

16 Appendix 5: Scenario Implementation of the Peculium Model

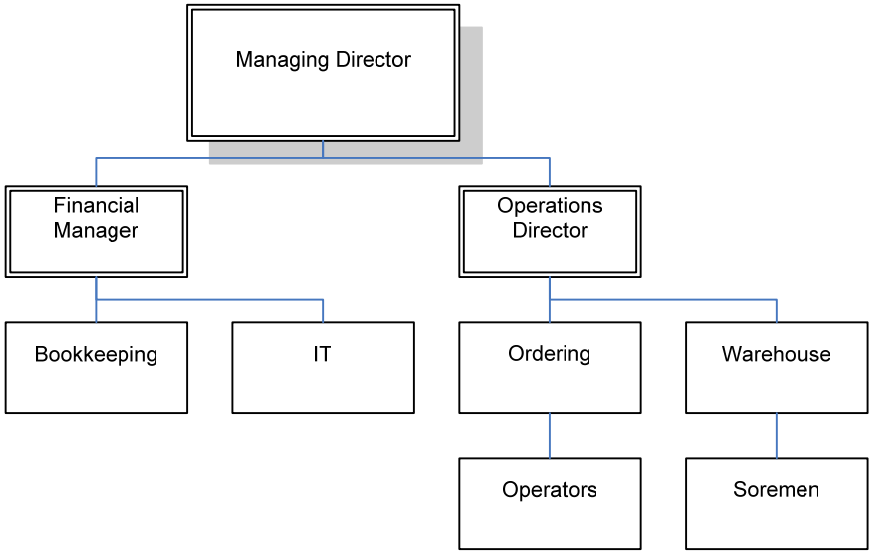
16.1 Introduction

A scenario implementation was performed on a real-world based non-for-profit organisation (NPO) called Muckleneuk Books. The scenario is based on the Peculium Model and follows all the steps provided.

Muckleneuk Books is an established NPO raising funds for charity through the sale of motivational books, CDs and DVDs. The media are specially manufactured at a reduced cost by a supplier to increase the funds raised. The funds are donated to a set list of approved charities. Muckleneuk Books has a stable client base ranging from individuals to franchise bookshops. Table 16.1 provides a summary of the organisation.

Table 16.1: A summary of Muckleneuk Books

Staff	15
Departments	
Bookstore	The bookstore holds examples of all the items in the stock list and is open to the public on specific dates and times.
Ordering	Operators in the ordering department conduct sales through telecommunications.
Warehouse	The warehouse houses the stock for sale and processes the orders for picking and shipment.
Finances	The financial department includes IT, debtors, creditors and general bookkeeping.
Senior management	The management team includes the managing directorship, operational directorship and financial management.

Organisational chart	
 *Figure 16.1: Simple organisational chart*	
Information assets	• Codes are provided for the assets using the abbreviations S for systems, IF for information assets and IS for infrastructure assets.
Systems	• Legacy ordering system (S1). The operators in the ordering department capture all the order details into this system. The system generates invoices that are passed to the warehouse and Finance for processing. • Workflow management system (S2). The workflow management system is used to manage the turnaround time of the orders and imports all order data automatically from the legacy system. • Pastel (S3). Muckleneuk Books makes use of Pastel for processing debtors, creditors and salaries.
Information	• Order information (IF1). The daily orders are housed in a batch flat file on the legacy system. The system is not backed up and is experiencing considerable reliability problems. • SQL database of workflow data (IF2). Dates on which orders are placed and stock is picked and shipped are

	captured into the SQL database through the workflow system. The data is backed up on a daily basis. • Stock database (IF3). The stock list is held in an Excel spreadsheet format. The file is backed up daily. • Exchange information store (IF3). Contact details of clients, although stored in Pastel, are not accessible in the ordering department. Exchange is used to store contact information and emailed orders. The information store is backed up on a daily basis. • Pastel data is backed up using the Backup Exec v8 software and LTO Backup tapes (IF4).
Infrastructure	• Legacy system hardware (IS1). The hardware of the system is showing increasing signs of collapse. Replacement hardware is not available. • Domain controller server (IS2). The server is relatively new and carries enough power for the management of the domain, exchange and workflow systems. The server runs on a Microsoft SBS 2003 operating system. • Pastel server (IS3). The Pastel server is a PC that is used to house the Pastel system and its data. • Desktop PCs (IS4). The organisation makes use of two separate groups of PCs: o Thin client workstations (IS4a). The operators and warehouse personnel make use of thin clients as they are dependent on server-based applications. o PCs (IS4b). The management staff makes use of PCs as more individualised use is required. These staff members also have access to the Internet. • Switch (IS5). A routing switch is also on the network directing traffic to the required destinations.

The organisation has never before conducted a risk assessment or management process.

16.2 The Peculium Model applied to Muckleneuk Books

The Peculium Model, as described in chapters 6 to 10, was applied to the organisation and the output from each step of the process is presented below.

16.2.1 Preparatory Activities

The preparatory activities have been performed. Table 16.2 offers the results.

Table 16.2: Preparatory activities

Confirm organisation is an SMME	Staff complement of 15
Obtain senior management involvement	Project Sponsor: Operations Director Roles and responsibilities signed

Organisational Objectives	

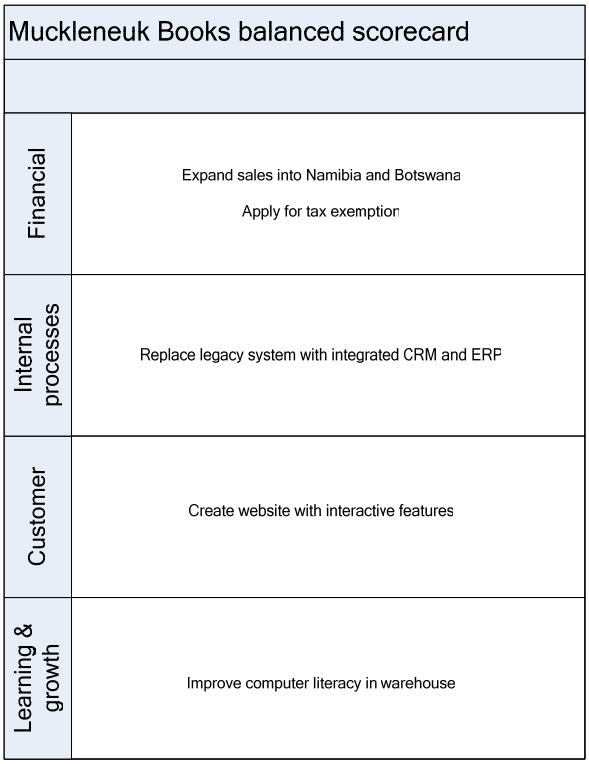



Figure 16.2: The Muckleneuk Books balanced scorecard	
Appetite for risk	R100 000

Identify key performance indicators	The minimum required list has been signed in as the full list.
Assemble risk management team	Team size: 3 Team members: a. One team member from Ordering b. One team member from the warehouse a. One team member from Finance Roles and responsibilities have been delegated. The warehouse team member is not keen on the process, and has asked to be replaced. A fellow warehouse staff member has been approached, and has agreed to

	participate.
Conduct training	None of the team members had any of the skills required. The team has been fully trained. The team has been assessed. The team member from Ordering has been found lacking in mitigation skills. This team member has been retrained and reassessed.

The preparatory activities have been completed. The following checklists prove the completion of these.

Completed Checklists

Table 16.3: Preparatory activities completed checklist

Preparatory Activities			
Step One		**Confirm organisation is an SMME**	
	1	Is the staff complement between the numbers of 1 and 200?	☒
Step Two		**Obtain senior management involvement**	
	1	Sponsor appointed by the board or management forum	☒
	2	Explain the sponsor roles and responsibilities to the sponsor	☒
	3	Sign off sponsor roles and responsibilities	☒
Step Three		**Identify objectives**	
	1	Explain use of balanced scorecard for standardising objectives	☒
	2	Complete balanced scorecard	☒
Step Four		**Identify appetite for risk**	
	1	Include risk appetite as an agenda item at the next meeting of the board	☒
	2	Decide on appetite amount	☒
Step Five		**Identify KPIs**	
	1	Include additional KPIs to minimum required KPI list provided	☒
	2	Enter final KPI list	☒
Step Six		**Assemble risk management team**	
	1	Include team assembly as an agenda item at the next meeting of the board	☒
	2	Explain role of the risk management team and size	☒
	3	Elect risk management team	☒
	4	Obtain elected members' buy-in	☒
Step Seven		**Conduct training**	
	1	Provide the required training to the risk management team	☒
	2	Assess the team to ensure that it is prepared for the process	☒

The preparatory activities are now complete and risk identification may commence.

16.2.2 Risk Identification

The risk identification activities have been performed. Table 16.4 offers the results.

Table 16.4: Risk identification activities

Identify environment	Ordering and warehouse departments
Team members verified	All members have been verified and remain in the team. The team member from Finance remains as she has strong analytical skills. All team members have been offered an additional three leave days for participating. This will be granted on completion of the process.
Responsibilities distributed	Ordering will conduct the identification of ordering assets, threats and vulnerabilities. Warehouse will conduct the identification of warehouse assets, threats and vulnerabilities. Finance will conduct the calculation of probability, impact and risk. The team will workshop mitigation together. The sponsor will own monitoring.
Identification of assets	

Asset Register

	Properties			
Asset	**Business Unit**	**Access Route**	**Users**	**CIA**
S1	Ordering	Switch	Operators	IA
S2	Warehouse	Server	Stock clerks	CIA
IF1	Ordering	Legacy system	Operators	IA
IF2	Warehouse	Server	Stock clerks	CIA
IF3	Ordering	Switch, Server	Operators	CIA
IF4	Ordering	Switch, Server	Operators	IA
IS1	Ordering	N/A	Operators	A
IS2	Both	N/A	Operators, stock clerks	IA
IS4a	Both	N/A	Operators, stock clerks	A
IS5	Both	N/A	Operators, stock clerks	A

Evaluate Assets against Weakness Value Scale

The asset properties are not repeated due to space restrictions. The assets have already been ranked according to highest weakness value.

All assets but one are above 30%.

Asset Register

Asset	Business Unit	Properties CIA	Weakness Value
S1	Ordering	CIA	100.00%
S2	Warehouse	A	100.00%
IF1	Ordering	IA	66.67%
IF2	Warehouse	A	66.67%
IF3	Ordering	A	66.67%
IF4	Ordering	CIA	55.56%
IS1	Ordering	CIA	55.56%
IS2	Both	IA	33.33%
IS4a	Both	CIA	33.33%
IS5	Both	IA	16.67%

The sponsor has selected the top five risks as the highest weakness value risks that will continue in the process.

Completed Checklists

Table 16.5: Risk identification completed checklists

Identification Activities

Step One	**Identify the environment/scope of risk management**	
	1 Identify business units	☒
	2 Identify environment	☒
	3 Approve identified environment	☒
	4 Document environment	☒
Step Two	**Distribute responsibilities**	
	1 Verify team members	☒
	2 Determine responsibilities	☒
	3 Assign responsibilities to the team members	☒
	4 Document assigned responsibilities	☒

Step Three	**Identify assets**	
	1 Create list of all systems, information, hardware and infrastructure	☒
	2 Complete asset register with properties	☒
Step Four	**Evaluate assets against weakness value scale**	
	1 Calculate weakness values	☒
	2 Capture weakness values to asset register	☒
	3 Reorder register according to weakness value	☒
	4 Identify highest weakness value assets	☒

All risk identification activities have been completed. Risk assessment may now commence.

16.2.3 Risk Assessment

The risk assessment activities have been performed. Table 16.6 offers the results.

Table 16.6: Risk assessment activities

Identify threats	
IF1	Malicious software Deterioration of storage media Network access by unauthorised persons Wilful damage
IS1	Airborne particles Fire Hardware failure Maintenance error Power fluctuation/failure Theft
S1	Malicious software Software failure Unauthorised use of software User error
IS4a	Failure of network components Failure of power supply Hardware failure

	Maintenance error Theft
IS5	Extremes of temperatures Failure of power supply Hardware failure Wilful damage

Identify vulnerabilities

The vulnerabilities have already been matched to threats. Any threats that have no corresponding vulnerability have been removed. The CIA exposed by the vulnerability is also reflected.

Asset	Threat	Vulnerability	CIA
IF1	Malicious software	Unprotected storage	A
	Deterioration of storage media	Lack of periodic replacement schemes	A
	Network access by unauthorised persons	Unprotected password tables	I
	Wilful damage	Lack of physical protection	IA
IS1	Airborne particles	Susceptibility of equipment to dust	A
	Fire	Lack of physical protection	A
	Hardware failure	Lack of replacement schemes	A
	Maintenance error	Insufficient maintenance	A
	Power fluctuation/failure	Unstable power grid	A
	Theft	Lack of physical protection	A
IS4a	Failure of network components	Insufficient maintenance	A
	Failure of power supply	Unstable power grid	A
	Maintenance error	Insufficient maintenance	A
	Theft	Lack of physical protection	A
IS5	Failure of power supply	Unstable power grid	A
	Hardware failure	Insufficient maintenance	A

	Wilful damage	Lack of physical protection	A

Calculate likelihood of occurrence

The likelihood of occurrence (P) is qualitatively estimated and assigned the values 3, 6 or 9 based on the low, medium or high value, respectively, as explained in Chapter 8, section 5.

Asset	Threat	P
IS1	Malicious software	M = 6
	Deterioration of storage media	H = 9
	Network access by unauthorised persons	M = 6
	Wilful damage	L = 3
IF1	Airborne particles	L = 3
	Fire	L = 3
	Hardware failure	M = 6
	Maintenance error	M = 6
	Power fluctuation/failure	M = 6
	Theft	M = 6
IF4a	Failure of network components	L = 3
	Failure of power supply	M = 6
	Maintenance error	M = 6
	Theft	M = 6
IF5	Failure of power supply	M = 6
	Hardware failure	L = 3
	Wilful damage	L = 3

Impact measurement

All impact values have already been calculated using the average method demonstrated in Chapter 8, section 6. The appetite for risk ranges are R0 – R15 000 as low, R16 000 – R45 000 as medium and R46 000 to R100 000 as high. An example

of the calculation follows this list.

Asset	Threat	I
IF1	Malicious software	H = 7
	Deterioration of storage media	M = 5
	Network access by unauthorised persons	M = 5
	Wilful damage	H = 8
IS1	Airborne particles	H = 7
	Fire	H = 7
	Hardware failure	H = 8
	Maintenance error	M = 6
	Power fluctuation/failure	M = 5
	Theft	H = 9
IS4a	Failure of network components	L = 3
	Failure of power supply	L 3
	Maintenance error	M 5
	Theft	H 9
IS5	Failure of power supply	L 3
	Hardware failure	L 3
	Wilful damage	M 4

The impact value of IF1 threatened by malicious software is used for this example. The batch file is corrupted and cannot be recovered.

- The batch file cannot be replaced. No revenue can be obtained in this period required to recreate the data. This carries a high impact.
- The productivity of the ordering and warehouse departments will come to a standstill as it will take five days to contact all clients and retrieve

possible orders. The formula provides a result of R9 000. The impact is low.

- The customers affected will have serious doubts about supporting Muckleneuk Books again. The impact is high.
- The average impact is high.

Calculate risks

The risks have already been calculated and are presented below. The method used is discussed in Chapter 8, section 7.

Asset	Threat	P	I	R
IF1	Malicious software	6	7	42
	Deterioration of storage media	9	5	45
	Network access by unauthorised persons	6	5	30
	Wilful damage	3	8	24
IS1	Airborne particles	3	7	21
	Fire	3	7	21
	Hardware failure	6	8	48
	Maintenance error	6	6	36
	Power fluctuation/failure	6	5	30
	Theft	6	9	54
IS4a	Failure of network components	3	3	9
	Failure of power supply	6	3	18
	Maintenance error	6	5	30
	Theft	6	8	48
IS5	Failure of power supply	6	3	18
	Hardware failure	3	3	9
	Wilful damage	3	4	12

Muckleneuk Books have elected the following top five risk values to continue to risk mitigation:				
IS1	Risk 1: Theft	6	9	54
	Risk 2: Hardware failure	6	8	48
IS4a	Risk 3: Theft	6	8	48
IF1	Risk 4: Deterioration of storage media	9	5	45
	Risk 5: Malicious software	6	7	42

Risk Assessment Completed Checklists

Table 16.7: Risk assessment completed checklists

Assessment Activities		
Step One	**Identify threats**	
	1 Select threats	☒
	2 Add threats to risk profile	☒
	3 Add descriptions and CIA affected to risk profile	☒
Step Two	**Identify vulnerabilities**	
	1 Identify the vulnerabilities applicable to the assets	☒
	2 Map the vulnerabilities to the threats	☒
	3 Capture all information to the risk profile	☒
Step Three	**Calculate likelihood of occurrence (P)**	
	1 Assign likelihood values	☒
	2 Add likelihood values to risk profile	☒
Step Four	**Perform impact measurement (I)**	
	1 Assign impact values	☒
	2 Add impact values to risk profile	☒
Step Five	**Calculate risks**	
	1 Calculate risk values	☒
	2 Add risk values to risk profile	☒
	3 Sort risk register by risk value	☒

	4 Select top risks	☒

16.2.4 Risk Mitigation

The mitigation activities have been completed. Table 16.8 offers the results.

Table 16.8: Risk mitigation results

Identify mitigation strategy		
The mitigation strategies have been identified for each top five risk.		
Risk	**Mitigation Strategy**	
Risk 1	Mitigation	
Risk 2	Transfer	
Risk 3	Mitigation	
Risk 4	Transfer	
Risk 5	Mitigation	
Two threats have been elected to be transferred as the legacy hardware cannot be replaced, but they have a high impact when exposed. The legacy system will not remain with Muckleneuk Books much longer (refer to balanced scorecard).		
Select the controls		
Risk	**Mitigation Strategy**	**Control**
Risk 1	Mitigation	Burglar bars, security alarm
Risk 2	Transfer	
Risk 3	Mitigation	Burglar bars, security alarm
Risk 4	Transfer	
Risk 5	Mitigation	Alternative storage and anti-virus software Backup device
The physical control of burglar bars or a security alarm should reduce the risk of theft of both the legacy hardware and the thin clients.		

The installation of anti-virus on the legacy hardware is not possible. As such, the batch file must be backed up to a different location and the location protected by anti-virus.

16.2.4.1 Cost Benefit Analysis

The cost benefit analysis of the three risks and associated controls as noted above has been performed. The following resulted from the analysis:

Theft of the Legacy System

Impact as measured in risk assessment: High

Impact after implementation is as follows:

Table 16.9: Impact after implementation for risk 1

Controls	Burglar Bars	Security Alarm
Monetary loss	The bars are damaged in the attempt and need to be repaired. Impact is low.	The hardware of the system is damaged and irreplaceable. The entire system would need to be replaced. A new ERP system requires a capital investment. Revenue loss is expected. Impact is high.
Productivity	Productivity is unaffected. Impact is low.	The wait for a new ERP system could be weeks. A manual process would be required to continue working. The ordering department would work at half productivity for at least 3 weeks. I(Pr) = Days × Payroll I(Pr) = 15 × 450[17] I(Pr) = R6 750 Impact is low.
Reputation	No customers are affected. Impact is low.	Customers' orders are delayed through the manual system. Muckleneuk Books' reputation will be

[17] Payroll for Ordering is at R900 per day. Half productivity lost per day is R450.

		damaged. Impact is medium.

Impact after implementation of burglar bars = 1 + 1 + 1 = 3: Low

Impact after implementation of security alarm = 3 + 1 + 2 = 6: Medium

The cost of the implementation is as follows:

Table 16.10: Cost of implementation for risk 1

Control	Burglar Bars	Security Alarm
Purchase cost	R4 000 including purchase and installation	R8 000 including purchase, installation and fees
Productivity loss	None	None
Total	R4 000	R8 000

The implementation of burglar bars both reduces the impact after implementation and presents a lower cost for implementation. Burglar bars are the recommended control.

Theft of the Thin Clients

Impact as measured in risk assessment: High

The impact after implementation is as follows:

Table 16.11: Impact after implementation for risk 3

Controls	Burglar Bars	Security Alarm
Monetary loss	The bars are damaged in the attempt and need to be repaired. Impact is low.	Two of the thin client devices have been stolen. Replacement can be made at a low cost and within 4 days. Revenue for the 4 days is reduced. Impact is low.
Productivity	Productivity is unaffected.	The wait for two thin clients has reduced the ordering department to

	Impact is low.	two-thirds productivity for 4 days. I(Pr) = Days × Payroll I(Pr) = 4 × 600[18] I(Pr) = R2 400 Impact is low.
Reputation	No customers are affected. Impact is low.	Customers' orders are delayed through the reduced productivity but not noticeably by the customer. Impact is low.

Impact after implementation of burglar bars = 1 + 1 + 1 = 3: Low

Impact after implementation of security alarm = 1 + 1 + 1 = 3: Low

The cost of the implementation is as follows:

Table 16.12: Cost of implementation for risk 3

Control	Burglar Bars	Security Alarm
Purchase cost	R4 000 including purchase and installation	R8 000 including purchase, installation and fees for the first year
Productivity loss	None	None
Total	R4 000	R8 000

Both controls offer the same reduction in impact after implementation. The burglar bars are at a lower cost and are therefore recommended. If both the legacy hardware and thin client theft are approved for mitigation, this cost is reduced.

Malicious Software Attack of the Batch File

Impact as measured in risk assessment: High

The impact after implementation is as follows:

Table 16.13: Impact after implementation for risk 5

[18] Payroll for Ordering is at R900 per day. Two-thirds productivity lost per day is R600.

Control	Alternative Storage and Anti-virus	Backup Device
Monetary loss	The legacy system cannot be used; a manual process must be used that slows the revenue intake. A specialist is required for the anti-virus removal. Impact is medium.	The legacy system cannot be used; a manual process must be used that slows the revenue intake. A specialist is required for the anti-virus removal. Impact is medium.
Productivity	Productivity is reduced for the manual process. The wait for specialist anti-virus removal is 3 days. I(Pr) = (Days × Payroll) + Specialist I(Pr) = (3 × 450) + 2 000 I(Pr) = R3 350 Impact is low.	Productivity is reduced for the manual process. The wait for specialist anti-virus removal is 3 days. I(Pr) = (Days × Payroll) + Specialist I(Pr) = (3 × 450) + 2 000 I(Pr) = R3 350 Impact is low.
Reputation	Customers' orders are delayed through the reduced productivity but not noticeably so by the customer. Impact is low.	Customers' orders are delayed through the reduced productivity but not noticeably so by the customer. Impact is low.

Impact after implementation of storage location and anti-virus = 3 + 1 + 1 = 5: Medium

Impact after implementation of backup device = 3 + 1 + 1 = 5: Medium

The cost of the implementation is as follows:

Table 16.14: Cost of implementation for risk 5

Control	Alternative Storage and Anti-virus	Backup Device
Purchase cost	R5 000 for developer to create the automatic	R12 000 including purchase and installation of the backup

	movement of the batch file to an alternative location; and purchase of the anti-virus.	device and automatic process allowing the storage of the batch file on the backup device.
Productivity loss	3 hours technical staff for installation of anti-virus and developed application. R187,50	1 hour technical staff for the installation of the developed application. R62,50
Total	R5 187,50	R12 062,50

Cost is the deciding factor once again as the impact after implementation for both are identical. The recommended control is the alternative storage and anti-virus.

Table 16.15: Pareto analysis

Identification of the 80/20 Rule Risks		
An electronic version of the risk register was searched for the threats that have already been targeted for control implementation. No additional risks were identified. The risk of theft to the assets IS1 and IS4a is, however, treated as an example to demonstrate CES.		
	Description	**CES**
Risk 1	Recommended control is burglar bars at R4 000	CES = IA (H) – Cost of control CES = 46 000 – 4 000 CES = 42 000
Risk 3	Recommended control is burglar bars at R4 000	CES = IA (H) – Cost of control CES = 46 000 – 4 000 CES = 42 000
The CES value for both is acceptable and the cost of the control justifiable. The amount resulting from the calculation is very high. The strengthening of the control of burglar bars with an additional security alarm has the following result:		
IS1	CES = IA (H) – Cost of controls	

IS4a	CES = 46 000 – (4 000 + 8 000) CES = 34 000
The CES value is still positive and high. An assumed 80/20 rule control is assumed for the calculation of the cumulative impact appetite and cost of control.	
IS(1&4a)	CES = Σ IA (H) – Cost of controls CES = 92 000 – 12 000 CES = 80 000

The implementation of both controls for both risks does not increase the cost, but improves the cost of exposure saving. The implementation of both controls for these risks is recommended.

The board is impressed with the results of the mitigation step of the risk management process, as the cost required by the implementation of the controls is at a total of R17 187,50. The board is satisfied with the calculations and approves the continuation of the process with the strategies elected and controls recommended.

16.2.4.2 Updated Risk Register

The information collected to date has been added to the risk register.

Table 16.16: Updated risk register

Risk Register

Risk	Top Risk	Mitigation Solution	Control	CES
IS1-Theft	Y	Mitigation	Gates & alarm	R42 000,00
IS1-Hardware failure	Y	Transfer		
IS4a-Theft	Y	Mitigation	Gates & alarm	R42 000,00
IF1-Deterioration	Y	Transfer		
IF1-Malicious software	Y	Mitigation	Anti-virus & application	R40 812,50

16.2.4.3 Created Action Plans

The risk management team has created the action plans for each top risk. As the same control applies to two risks this step was completed faster than expected. The action plans are presented below.

Table 16.17: The risk action plans

Risk Action Plan					
Risk	**Mitigation Solution/ Control**	**Mitigation Date**	**Resources**	**Exposure Response Procedure**	**Escalation Procedure**
Risk 1	Gates & alarm	03/01/2006	Boma Security	ERP1	EP1
Risk 2	Transfer	01/12/2005	HD Insurance	ERP2	EP2
Risk 3	Gates & alarm	03/01/2006	Boma Security	ERP2	EP1
Risk 4	Transfer	01/12/2005	HD Insurance	ERP3	EP3
Risk 5	Anti-virus & development	01/02/2006	MQS	ERP4	EP4

Vendors for the mitigation controls have been established. The vendor for the transfer of risk to an insurance firm is HD Insurance.

As an example, Exposure Response Procedure ERP1 and EP1 are expanded.

Exposure Response Procedure ERP1

The exposure response procedure for the risk of theft of the legacy system is as follows:

1. Assess the loss of the asset, i.e. is the complete asset lost, or portions of the asset?
2. Contact the Financial Manager and inform her of the extent of the loss.
3. Review the security gates and alarm. Have the controls been damaged? Did the controls offer any resistance to the theft? Can additional strength be added to the controls to prevent a similar attack?

Escalation Procedure EP1

The escalation procedure for the risk of theft of the legacy system is as follows:

1. First point of contact: Financial Manager (informing of the exposure)
2. Second contact: Operations Director (informing of the exposure)
3. Third contact: The board chairperson (authorisation for improvement of control)

16.2.4.4 Risk Assessment Completed Checklists

Table 16.18: Risk mitigation completed checklists

Mitigation Activities		
Step One	**Identify mitigation strategy**	
	1 Assign mitigation strategy to each risk	☐
	2 Capture mitigation strategy to risk register	☐
Step Two	**Identify mitigation solution**	
	1 Select control for each mitigation risk	☐
	2 Apply 80/20 rule to risk register	☐
	3 Create 80/20 rule control report	☐
	4 Capture controls to risk register	☐
	5 Risk register acceptance by the board	☐
Step Three	**Create action plan**	
	1 For each risk, complete an action plan	☐

All risk mitigation activities have been completed. Risk monitoring may now commence.

16.2.5 Risk Monitoring

The risk monitoring activities have been performed. Table 16.19 offers the results.

Table 16.19: Risk monitoring activities

Include risk management in day-to-day activities
The risk management team has hosted workshops and informed all members of staff of the risks they identified and how these risks will be mitigated. They have explained that the risks associated with the legacy system will be mitigated using short-term insurance, as the system replacement is already planned and in progress. The workshops also included awareness training of the exposure response procedures and escalation plans created for the risks. The team held interactive role-play sessions to ensure that the staff all understood the concepts of risks and mitigation and are prepared for exposure response. The risk management team has, with the cooperation of the staff, selected one Friday a

month for risk management training which will include progress reports and notification of any new risks discovered. Attendance of these training sessions is mandatory.

Maintain risk register

The risk management team, as representatives of their respective departments in the environment, hold the responsibility of calling a team meeting whenever a new asset arrives. The team is fully prepared for the arrival of the replacement ERP system and will include a full assessment into the risk register one week after installation is completed.

Risk management scorecard

The risk management scorecard has been updated at most one day after progress thus far. The scorecard to date is as follows:

Risk Management Scorecard

Key Performance Indicator			Due Date	Status
1	Achieve milestone at each step of the process			
	1.1	Preparatory activities milestone achieved		Completed
	1.2	Identification milestone achieved		Completed
	1.3	Assessment milestone achieved		Completed
	1.4	Mitigation milestone achieved		Completed
	1.5	Monitoring milestone achieved	28/02/2006	Started
2	Complete each deliverable at each step of the process			
	2.1	Preparatory activities deliverables achieved		Completed
	2.2	Identification deliverables achieved		Completed
	2.3	Assessment deliverables achieved		Completed
	2.4	Mitigation deliverables achieved		Completed
	2.5	Monitoring deliverables achieved	28/02/2006	Started
3	Present milestone summary to the board		28/02/2006	Started
4	Complete asset register at the end of risk identification			Completed
5	Complete risk register at the end of assessment			Completed
6	Complete risk strategy at the end of risk mitigation			
	6.1	Risk 1: Mitigation		Completed
	6.2	Risk 2: Transfer		Completed
	6.3	Risk 3: Mitigation		Completed
	6.4	Risk 4: Transfer		Completed
	6.5	Risk 5: Mitigation		Completed
7	Complete action plan			
	7.1	Risk 1: Burglar bars and security alarm	03/01/2006	Started
	7.2	Risk 2: HD Insurance		Completed
	7.3	Risk 3: Burglar bars and security alarm	03/01/2006	Started
	7.4	Risk 4: HD Insurance		Completed
	7.5	Risk 5: Anti-virus and application	01/02/2006	Started
8	Complete assessment report		01/03/2006	Started
9	Update business continuity plan			N/A

Measure monitoring
The risk management team is making regular additions to the assessment report as progress is made. A draft is submitted to the board at each meeting and presented by the sponsor. The report includes the minutes of the workshops held to train staff and staff feedback sheets completed at the end of the workshops. The report includes the risk register, which has not been changed significantly since the completion of the mitigation step. The risk management scorecard as at the day of the meeting is also included.

Maintain business continuity plan
The exposure response procedures have not been changed for the assets. A procedure will be created when the replacement ERP system is in place.

Risk Monitoring Completed Checklists

Table 16.20: Risk monitoring completed checklists

Monitoring Activities			
Step One		**Include risk awareness in day-to-day activities**	
	1	Conduct awareness training	☒
	2	Ensure that risk profile is understood by staff	☒
	3	Ensure that impact of mitigation strategy is understood	☒
	4	Conduct business continuity process training	☒
	5	Hold sessions to review day-to-day activities	☒
Step Two		**Maintain the risk register**	
	1	Update asset register	☐
	2	Update risk profiles	☐
	3	Update risk register	☐
	4	Update action plans	☐
	5	Communicate updates	☐

Step Three		**Conduct performance measurement**	
	1	Maintain risk management scorecard	☒
	2	Communicate updated scorecard	☒
Step Four		**Measure Monitoring**	
	1	Create assessment report	☒
	2	Communicate assessment report	☒
Step Five		**Maintain BCP**	
	1	Update BCP	☒
	2	Communicate and provide training on BCP	☒

The monitoring step as reflected here works on the assumption that it is not yet complete, but will end at the end of the financial year, with the new iteration starting with the Muckleneuk Books' financial year. This has been proposed by the board and will be so for at least three years.

This completes the scenario test of the Peculium Model.

17 Appendix 6: A paper published for the ISSA 2005 Conference

The paper listed below was published in the proceedings of the ISSA (Information Security South Africa) 2005 conference held at the Balalaika Hotel in Sandton, South Africa, from 29 June to 1 July 2005.

A FRAMEWORK FOR EVALUATING INFORMATION SECURITY RISK MANAGEMENT METHODOLOGIES FOR SMMEs

[1]L van Niekerk **[2]L Labuschagne**

Academy for Information Technology, University of Johannesburg, South Africa

[1]lieslv@netsurit.com [2]ll@na.rau.ac.za

+27 11 489-2847

PO Box 524, Auckland Park, Johannesburg, South Africa, 2006

ABSTRACT

The South African economy has grown considerably in the last 10 years, with black empowerment being supported by the state and investors to develop previously disadvantaged communities. Government has also targeted small, medium and micro enterprises (SMMEs) for development.

SMMEs are not directly affected by corporate or IT Governance, and as a result 80% of SMME failures are attributed to lack of management knowledge. This lack of knowledge extends to the management of information security risk.

This article evaluates information security risk management methodologies available to international small businesses for fit to the South African SMME to discover whether they may be used to reduce the failure rate. The evaluation framework provides a tool that may forewarn the lack of fit of a methodology.

KEYWORDS

Information security risk management; SMME; small business; OCTAVE-S; CRAMM V Express

A FRAMEWORK FOR EVALUATING INFORMATION SECURITY RISK MANAGEMENT METHODOLOGIES FOR SMMEs

1 Introduction

Small, medium and micro enterprises (SMMEs) form a sizable portion of the gross domestic product (GDP) in South Africa. The SMME market portion contributes 42% to the GDP [South Africa, Business Guidebook], but comprises an estimated 99% of the total number of enterprises in the economy [National Treasury].

The information security risk management (ISRM) methodologies commercially available to SMMEs were created in developed countries, and for different types of small businesses to that of the South African SMME. These methodologies require evaluation for a South African SMME before they can be recommended as an organisational improvement tool.

This article presents the creation of a framework for this evaluation, and the subsequent evaluation of two internationally available methodologies for small businesses.

The framework was created considering the requirements of Corporate Governance and IT Governance, as well as the constraints experienced by SMMEs, time and resources.

The article first presents the framework, followed by a summary of the methodologies of OCTAVE-S and CRAMM V Express. Each are evaluated using the framework before a conclusion is drawn.

2 Framework for the evaluation of ISRM methodologies

The framework has been created out of the characteristics of an SMME, as well the benchmark of procedural order required by corporate and IT Governance. The characteristics were devised from the most pertinent constraints faced by the SMME, being cost, resources and business knowledge.

Corporate and IT Governance both require a process including planning, execution and control or monitoring of risk management as a cyclical process [King Commission on Corporate Governance; IT Governance Institute]. This creates continual awareness of risk, and the management thereof.

A further requirement is the fit of the methodology to the definition of the South African SMME, as it is unique compared to that of other countries. These requirements, coupled with the constraints mentioned above, create the major elements of the framework.

17.1 The Framework Explained

The framework in Figure 1 that has been created for evaluation of SMME methodologies is three-dimensional, comprising the following:

Dimension 1. Elements. There are 4 elements in the framework: availability, cost, regulatory fit and SMME fit.

Dimension 2. Factors. The elements consist of factors, and in some cases, sub-factors. The constraints and requirements mentioned above are multi-faceted and cannot be represented fairly in one dimension.

Dimension 3. Weights. All of the elements and factors have associated quantifiable weights assigned. The weights create a quantitative measure for the framework, allowing comparisons of methodologies after evaluation.

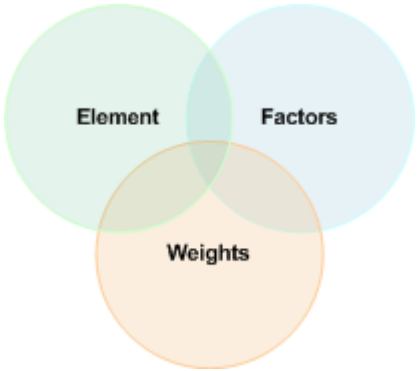


Figure 1: The three-dimensional framework

The elements based on the constraints faced by an SMME and the requirements of corporate and IT Governance are:

17.1.1 Visibility

Visibility pertains to the ease with which the ISRM approach may be obtained, specifically by an SMME. This includes whether the full methodology is obtainable with ease, or whether only promotional material is available. The objective of visibility is to measure whether the interested party within the SMME can reasonably obtain an understanding of the methodology and thus make an informed decision of whether to proceed with the ISRM methodology.

17.1.2 Cost

The cost of implementing the methodology is an estimated measure, as the true cost of any exercise can only be determined after the fact. Cost is, however, a relative term, as there are many facets to a methodology that may be added as a cost, even though no direct spending was involved. Cost is therefore split into these factors:

- Purchase cost is the requirement of cash spend on the methodology, whether it is an upfront cost, or expenditure throughout the methodology for obtaining the methodology.
- Organisational involvement is attributable to the human resources involved in the methodology, through various channels. These channels, known as sub-factors, are:

- Knowledge requirement. All training required by the organisation, or elected individuals.
- Senior management buy-in. The involvement of senior management in a methodology is an expensive factor, as senior management time is at a higher premium than an operational employee's.
- Self-directed or consulted. The nature of the methodology also impacts the cost of the implementation. A self-directed approach may be higher in organisational involvement cost, but lower in purchase cost. The inverse applies to a consulted approach. The purchase cost may be higher, but organisational involvement is less. The duration of the methodology, as prescribed by the nature of the methodology, must also be considered.

  The duration of a consulted approach may be shorter, as the schedule is managed by a third party. The duration of a self-directed approach is self-led, and thus may be prone to operational delays.

17.1.3 Regulatory Fit

The regulatory fit refers to the process being of a cyclical nature and including both planning and monitoring phases. This would create fit to the corporate and IT Governance standards of King II and CobiT, respectively [King Commission on Corporate Governance; IT Governance Institute].

17.1.4 Fit to the South African SMME

The South African SMME has been determined to be unique when compared to 5 other nations' definitions, and this should be considered before implementing a methodology created for the SMME of a different nation.

The fit to the South African SMME is evaluated contrariwise against the following factors:

- Horizontal or vertical industry. The methodology should not promote or be aligned with a horizontal or vertical industry. There should be no restriction on the industry of the SMME.
- The size of organisation. The South African SMME is defined as ranging from 1 staff member to 200 [South Africa]. The methodology should not be focused on a number excluding parameters of this range.
- The type of organisation. Any structure of small businesses should be allowed, especially when considering the existing lack of business skills. There should be no restriction on structure.

To summarise, the only restriction that is endorsed is the maximum allowance of 200 employees.

The framework is summarised in Figure 2.

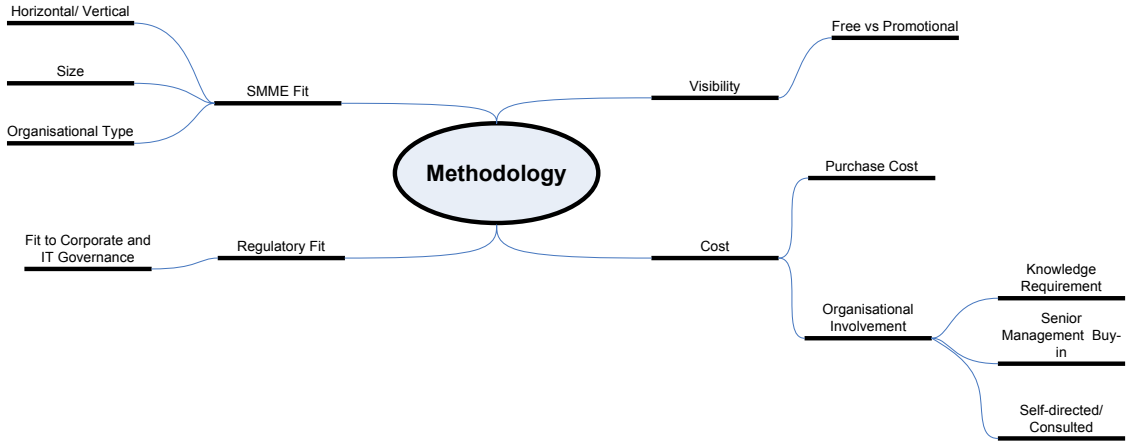


Figure 2: The framework, its elements and factors

The framework has thus far been explained in two dimensions. The third dimension, the weighting, is assigned as follows.

17.2 The Weighted Dimension

Weights have been assigned to each element, factor and sub-factor. The weights have been assigned, based on estimated importance of the element.

Cost has been assigned the highest weight due to the cost-focus of SMME's. A high purchase cost alone, could dissuade the SMME owner or decision maker from implementing a methodology. However, cost is not the only consideration. Lack of SMME or regulatory fit will result in a very low return on investment, even though the cost is low.

Visibility also carries a great importance. The remaining weights become of no consequence if the decision maker cannot obtain an initial understanding of the methodology. Avoidance of visibility would create a 'blind' implementation of the methodology.

The remaining weights are also go/ no-go weights. If the methodology scores low on SMME and regulatory fit, the organisation can be assured that, for their enterprise, it will not be the optimum solution. A score of zero in both are immediate dismissals.

As the result of these arguments, the highest weight is assigned to cost, as the primary concern for the SMME owner, with equal distribution of weight over the remaining elements.

The total of the weights when added will provide a score out of 100. This is then easily compared to other evaluations for decision making. Should two options score equally, the elements themselves should be compared, using go/ no-go decision blocks.

Tables 1-4 present the elements, factors and sub-factors with their assigned weights. A description of the assigning of weights for each factor is provided, creating guidance for quantification. Each elemental Table has a decision point. All decision points are also highlighted, providing the evaluator with the option to dismiss a methodology. The score for the element is calculated by selecting the rule (rules are in *Italic* font) in the Table with best fit to the methodology, and adding the rule weights for

an element score. The final decision is based on a framework score higher than a reasonably conservative 30.

Table 1: The weights of visibility

Element, factors and sub-factors		**Assigned weight**
Visibility		**20**
The methodology is freely available and user-friendly	*20*	
Promotional information is freely available with details for further information	*10*	
No information is freely available	*0*	
SCORE		____
GO/NO GO DECISION – HIGH RISK OF FUTILE IMPLEMENTATION		

Table 2: The weights of cost

Element, factors and sub-factors		**Assigned weight**
Cost		**40**
Purchase cost		20
The methodology is free	*15*	
The methodology is free but has a tool that reduces organisational involvement available at a cost	*5*	
The methodology has a cost attributed	*0*	
The methodology has a cost attributed that includes a tool that reduces organisational involvement	*5*	
Organisational involvement		20
Knowledge requirement		5
The organisation is expected to already have all knowledge required for the methodology	*0*	
There is training available for the organisation at a cost	*5*	
No previous knowledge is required	*5*	
Senior management buy-in		5
The methodology promotes senior management buy-in or sponsorship	*5*	
The methodology requires senior management execution	*0*	
The methodology does not promote or require senior management buy-in	*0*	
Self-directed or consulted		10
The methodology is self-directed	*5*	
The methodology is self-directed with consulting available	*10*	
The methodology is consulting based with no operational involvement from the organisation	*5*	
SCORE		____
GO/NO GO DECISION: IS THE COST TOO HIGH?		

Table 3: The weights of regulatory fit

Element, factors and sub-factors		Assigned weight
Regulatory fit		**20**
The methodology conforms to the steps in Table 2	*10*	
The methodology does not conform to the steps in Table 2, but does include at least planning and arranging	*5*	
The methodology does not conform to the steps in Table 2 at all	*0*	
The methodology is cyclical and promotes reviewing	*10*	
The methodology is not cyclical and does not promote reviewing	*0*	
SCORE		
GO/NO GO DECISION: HIGH RISK OF ANTI-REGULATORY SOLUTION		

Table 4: The weights of SMME fit, the final score

SMME fit		20
Horizontal/vertical		5
The methodology is restricted to a horizontal or vertical industry	*0*	
The methodology is not restricted to any industry	*5*	
Size		10
The methodology restricts the size of the organisation to a range within the parameters of the South African SMME	*0*	
The methodology is restricted to the parameters of the South African SMME	*10*	
Organisational type		5
The methodology is restricted to a specific type of organisation, e.g. hierarchical structure	*0*	
The methodology is not restricted to a specific type of organisation	*5*	
SCORE		
GO/NO GO DECISION: HIGH RISK OF INAPPROPRIATE SOLUTION		
TOTAL SCORE		**100**
GO/NO GO DECISION: IS THE SCORE HIGHER THAN 30?		

The framework has been established in all three dimensions. The following section uses the framework to evaluate the OCTAVE-S Information Security Risk Management methodology.

3 OCTAVE-S Evaluated

OCTAVE-S is discussed in summary to create the foundation from which information is extracted for the framework evaluation that follows later. OCTAVE-S is based on the OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) Approach [Alberts & Dorofee] designed specifically for the unique constraints experienced by small organisations [Software Engineering Institute]. OCTAVE-S was developed by the Technology Insertion, Demonstration and Evaluation program of the Software Engineering Institute (SEI).

The framework of OCTAVE was retained, with simplified implementation of the detail. OCTAVE-S v0.9 is summarised below and subsequently evaluated.

17.3 OCTAVE-S Summarised

OCTAVE-S is a self-directed information security risk evaluation. It requires a 3- to 5-member interdisciplinary team to lead the methodology, and also requires that these staff members have a broad insight into the organisation's business and security

processes. The ultimate outcome of the methodology is an organisation-wide protection strategy and risk mitigation plans.

The OCTAVE-S approach is divided into three phases. These phases are:

1. Build asset-based threat profiles
2. Identify infrastructure vulnerabilities
3. Develop security strategy and plans

17.3.1 Build Asset-based Threat Profiles

The team uses this phase to create a set of criteria against which risks will later be evaluated. All organisational assets are identified and the existing security practice is defined. No external consulting is offered in this phase, as all operational tasks are completed by the team itself.

A selection process is used to select 3 to 5 critical assets, on which the remainder of the evaluation will be conducted.

Finally, security requirements are defined, and threat profiles created for each critical asset. The threat profile is based on 3 levels: the asset, followed by all connected aspects that may expose a threat and the outcomes if the threat is realised.

17.3.2 Identify Infrastructure Vulnerabilities

The team analyses the computing infrastructure in this phase, focusing on the access means to the critical assets, for example systems and data. The team also analyses which parties are responsible for the maintenance of these assets, in many cases with small businesses, an outsourced party.

17.3.3 Develop Security Strategy and Plans

This phase requires the team to identify risks to the critical assets and what may be done to mitigate these risks. Risks are measured on a qualitative scale of high, medium or low. All this information is collated into a protection strategy for the organisation's critical assets, and mitigation plans to reduce the risks. The worksheets provided are a structured benchmark for creating these plans. No expectation of when these plans are executed is provided.

17.3.4 Scope of Application

OCTAVE-S is aimed at organisations ranging from 20 to 80 staff members. This excludes the majority of South African SMMEs (91%). The organisational structure is flat, with people from different departments being accustomed to interdepartmental projects.

An organisation such as this is expected to be able to assign 3 to 5 people that have broad knowledge of the organisation and its security practices.

OCTAVE-S is not recommended for an organisation that cannot create a team of knowledgeable staff members, for example an organisation that consists of independent business units, or dispersed groups of staff that do not interact much.

The team members are expected to have problem-solving abilities, analytical skills, teamwork ethic and time, described as a few days. It is not indicated whether the few days are full days, or the total of various short sessions.

17.3.5 Preparation Guidelines

OCTAVE-S provides a module containing all preparation activities that are suggested before kicking off the methodology.

- The first notable preparation is senior management sponsorship. OCTAVE-S makes it very clear that senior management sponsorship is vital, but cannot clearly define how to obtain it.
- The next preparation activity is selection and training of the team. The team should be made up of individuals with the skills listed above, containing at least one leader in the group, and a staff member with close links to IT, either through working closely with IT, or the third-party provider.
- The use of managers on the team is encouraged, but managers should not be the majority of the team as this may restrict open communication.
- Training of the team is addressed by promoting the training of at least one team member on OCTAVE-S.
- Setting the scope of the evaluation allows the team to identify which areas of the organisation will be evaluated. A subset of the organisation's business units may be selected. OCTAVE-S recommends at least 4 business units, one of which must be the IT department or IT management department.
- The schedule for the methodology is created next. Worksheets are provided to offer guidelines of workshop durations, depending on the experience of the team. The duration of the methodology in phases ranges as follows:

Table 5: Duration of OCTAVE-S

Phase	From	To
Preparation	4 days	8 days, 4 hours
Build asset-based threat profiles	1 day	2 days, 6 hours
Identify infrastructure vulnerabilities	3 hours	1 day
Develop security strategy and plan	1 day	5 days, 1 hour
Total	**6 days, 3 hours**	**17 days, 3 hours**

The worksheets also provide a checklist at each process to ensure that all steps have been completed. Guidance is also provided on managing logistics for all workshops.

17.3.6 Implementation Guidelines

OCTAVE-S provides a set of guidelines for each process in each phase with step-by-step instructions of what information is to be gathered and which worksheet is to be completed as well as definitions of any terminology used.

17.4 OCTAVE-S Evaluation Outcomes

The evaluation of OCTAVE-S based on the implementation guide is presented in the Table below.

Table 6: OCTAVE-S framework evaluation

Elements, factors and sub-factors	Score achieved
Visibility	**20**
OCTAVE-S is freely available online and is easy to understand	20
SCORE	**20**
Cost	**40**
Purchase cost	
OCTAVE-S is available at no cost	15
Vulnerability tools may be obtained at a cost but are not required	5
Organisational involvement	
There is training available for the organisation at a cost	5
OCTAVE-S requires senior management buy-in or sponsorship	5
OCTAVE-S is self-directed	5
SCORE	**35**
Regulatory fit	**20**
OCTAVE-S does include at least planning and arranging	5
SCORE	**5**
GO/NO GO DECISION: HIGH RISK OF ANTI-REGULATORY SOLUTION	
SMME fit	**20**
Horizontal/vertical	
OCTAVE-S is not restricted to any industry	5
Size	
OCTAVE-S restricts the size of the organisation to 20 to 80 staff members	*0*
Organisational type	
OCTAVE-S restricts the organisation to a flat hierarchy with more than 4 business units	*0*
SCORE	**5**
GO/NO GO DECISION: HIGH RISK OF INAPPROPRIATE SOLUTION	
TOTAL	**65**

OCTAVE-S achieves an average score on total, but ranks very low in the regulatory and SMME fit elements. It is a high risk methodology for ISRM.

4 CRAMM V EXPRESS Evaluated

CRAMM V Express is discussed in summary to create the foundation from which information is extracted for the framework evaluation that follows later. CRAMM V Express [Insight Consulting], similar to OCTAVE-S, is based on the large organisation version CRAMM V Expert. The software has been developed by Insight Consulting based on the CRAMM methodology.

CRAMM V Express is a tool for rapid yet effective risk assessments that require limited time and human resources.

17.5 The CRAMM V Express Tool

The tool follows a very simple process for assessing the risks facing an organisation's systems, and proposing mitigating controls, or as CRAMM describes them, countermeasures to reduce the risk.

The tool presents user-friendly screens that allow input from a single user, with reporting available for review. The process followed by the tool is presented in Figure 3.

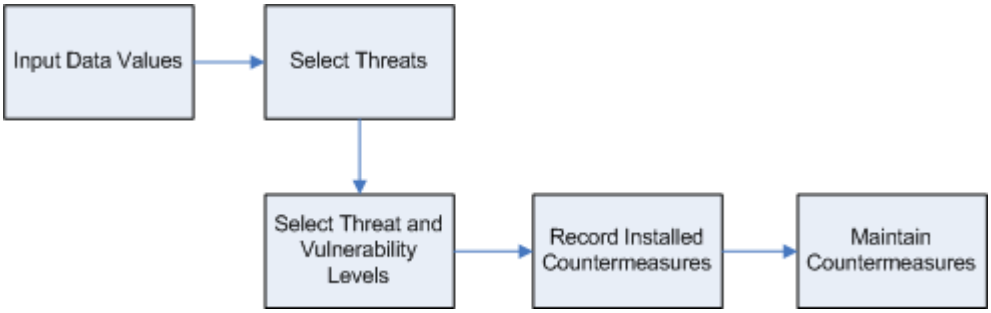


Figure 3: The CRAMM V Express process

17.5.1 Scope of Application

The tool may be used for any system; there is, however, no distinction of which systems should be assessed. There is also no promotion of an organisation-wide assessment or assessment on departments or business units only.

There is no guidance offered regarding who is responsible for managing the assessment, for example who is required to enter the information, and who is responsible for ensuring that the mitigating controls are applied.

The tool does not offer any training on identifying threats, vulnerabilities, or assessing the level of vulnerability once the risk has been identified. The tool assumes that the user is knowledgeable of this specialist information, but still requires a tool to present the countermeasures.

17.5.2 Preparation

The tool itself does not require any preparation, but does assume that the user is aware of all systems that should be entered into the tool. The onus lies on the user to nominate which systems are to be assessed, and gain the assessment skill beforehand as well.

17.5.3 Implementation

Implementation of CRAMM V Express does not take place *per se*, as the use of the tool takes very little time, but no guidance is offered on when or how the proposed mitigating controls are to be implemented. The onus again lies on the user to make those decisions.

17.5.4 Cost

The CRAMM V Express tool is available at a cost of £1 500,00 excluding tax, with an additional annual licensing fee of £250,00. In Rand, this translates to a purchase cost of R17 205,00 excluding taxes, and R2 867,50 per year (calculated at the current exchange rate of R11,47 per British pound).

This is not an extremely large sum of money, but may be contested if the tool is not used to its full potential. It is, however, fast to use and has low cost in organisational involvement.

17.6 CRAMM V Express Evaluation Outcomes

The evaluation of CRAMM V Express based on the implementation guide is presented in the Table below.

Table 7: CRAMM V Express framework evaluation

Elements, factors and sub-factors	Score achieved
Visibility	**20**
Promotional information is freely available with details for further information	10
SCORE	**10**
Cost	**40**
Purchase cost	
CRAMM V Express has a cost attributed that includes a tool that reduces organisational involvement	5
Organisational involvement	
The organisation is expected to already have all knowledge required for the methodology	*0*
The methodology does not promote or require senior management buy-in	0
The methodology is self-directed	5
SCORE	**10**
GO/NO GO DECISION: IS THE COST TOO HIGH?	
Regulatory fit	**20**
CRAMM V Express promotes reviewing by offering a record of countermeasures used and still to be implemented	10
SCORE	**10**
SMME fit	**20**
Horizontal/vertical	
The CRAMM V Express is not restricted to any industry	5
Size	
CRAMM V Express has no restrictions on organisational size at all	10
Organisational type	
CRAMM V Express is not restricted to a specific type of organisation	5
SCORE	**20**
TOTAL	**50**

CRAMM V Express scores below average and fails in the cost element. This is surprising as very little organisational involvement is required, although a purchase cost is attributed. The double edge of the sword is the lack of a requirement of senior management involvement. This has been stipulated by King II as vital, as well as CobiT, which also supports the low regulatory score. The high score in SMME fit is inconclusive, as CRAMM V Express does not specifically cater for small businesses, nor does it exclude them.

The inference has to be made that although the above approaches may offer some benefits to a South African SMME, there are risks that they become difficult to apply and are abandoned before completion. There is no support available for either of these approaches should the organisation grow weary of self-direction.

5 Conclusion

This article has presented a framework that may be used to evaluate any methodology by an SMME concerned with information security risk management. The framework focuses its greatest weight on the cost concern of the SMME, but also considers the visibility of the methodology, fit to the South African structure of an SMME, and fit to the regulations of the South African environment.

The framework was applied to OCTAVE-S and CRAMM V Express. The framework has found that neither of these approaches is ideal for the South African SMME, with mediocre scores of 65% and 50%, respectively.

The framework has provided a weapon in the SMME's armoury for forewarning inappropriate implementation of a methodology that may cost the organisation resources it cannot afford, or provide a solution it cannot use.

An outcome of these evaluations was the realisation that a new, South African SMME-based information security risk management methodology needs to be developed that scores high on the evaluation framework, and thus meets all the requirements of an SMME.

It is however acknowledged that the framework is experimental and has not been tested on all information security risk management methodologies for small businesses and that further research into methodologies is planned for the future. Further research is also planned into the abovementioned creation of the methodology for the South African SMME.

6 References

1. South Africa. 2003. *South Africa Business Guidebook 2002/2003*. Writestuff Publishing.
2. National Treasury. 2002. *The Relative Importance of SME's in the South African Economy: An Analysis of Issues and Quantification of Magnitudes*.
3. Dispatch Online. 2003. *SMME's failure blamed on poor management*. http://www.dispatchonline.co.za.
4. King Commission on Corporate Governance. *King Report of Corporate Governance for South Africa – 2002*.
5. IT Governance Institute. 2000. *CobiT Framework 3rd edition 2000*.
6. South Africa. 2003. *National Small Business Amendment Act 2003*. Government Printer.
7. Alberts, CJ & Dorofee, AJ. June 2002. *Managing Information Security Risks. The OCTAVE Approach*. Pearson Education Limited.
8. Software Engineering Institute. 2003. *OCTAVE-S Implementation Guide Version 9.0; Volume 1: Introduction to OCTAVE-S.*
9. Software Engineering Institute. 2003. *OCTAVE-S Implementation Guide Version 9.0; Volume 2: Preparation Guidance.*
10. Software Engineering Institute. 2003. *OCTAVE-S Implementation Guide Version 9.0; Volume 3: Method Guidelines.*
11. Insight Consulting. 2004. *CRAMM V Express Walkthrough Flash Presentation.* http://www.insight.co.uk.

References

[ACCA 2004] Towards Transparency: Progress on Global Sustainability Reporting 2004; ACCA 2004; Accessed through CorporateRegister.com; http://www.corporateregister.com; Accessed November 2004.

[AFRI 2005] African History on the Internet; www-sul.standaford.edu; Accessed November 2005.

[ALBE 2003] Alberts C., Dorofee A.; 2003; Managing Information Security Risks – The OCTAVE Approach; Pearson Education; ISBN: 0-321-11886-3; Terms: “Risk”.

[ALEX 2005] “Live with the Poor”; Alexanda Renewal Project; 13 June 2004; http://www.alexandra.co.za; Accessed November 2005.

[AMER 2004] Bartleby.com; The American Heritage Dictionary of the English Language; Terms: “Risk”; http://www.bartleby.com; Accessed October 2004.

[ASX 2003] ASX Corporate Governance Council Principles of Good Corporate Governance and Best Practice Recommendations March 2003; Australian Stock Exchange; http://www.asx.com.au/corporategovernance; Accessed November 2003.

[ATIS 2004] Alliance for Telecommunications Industry Solutions; http://www.atis.org; Terms: "Asset", "Vulnerability", "Threat", "Risk Assessment", "Risk Analysis", "Exposure", "Risk Mitigation", "Return on Investment", "Security"; Accessed October 2004.

[AU 2005] African Union Website; http://www.africa-union.org; Accessed November 2005.

[AYYA 2003] Ayyagari, M.; SME's Across the Globe, A New Database; Meghana Ayyagari et al.; 2003; Worldbank.org; http://www.worldbank.org; Accessed October 2004.

[BALA 2002] Balanced Scorecard Report; Volume 4; Number 2; March-April 2002; Harvard Business School Publishing.

[BAND 1999] A Framework for Integrated Risk Management in Information Technology; Bandyopadhyay et al.; Management Decision 1999; Terms: "Information Security Risk Management".

[BARR 1995] Barry, LJ.; Assessing Risk Systematically; Risk Management; Volume 42; Issue 1; January 1995.

[BSI 2002] BSI Business Information; BS 7799 Guide to Risk Assessment; PD 3002.2002.

[BURE 2004] Bureauveritas.com; Terms: "Assets", "Risk Assessment"; http//:www.bureauveritas.com; Accessed October 2004.

[CIA 2004] CIA World Factbook; Accessed through TheFreeDictionary.com;

http://www.encyclopedia.thefreedictionary.com/List+of+developed+nations; Accessed October 2004.

[CLIF 2004] Review of the Corporate Governance in South Africa; Accessed through CliffeDekker.co.za; http://www.cliffedekker.co.za; Accessed October 2004.

[COBI01 2000] IT Governance Institute; 2000; CobiT 3rd Edition – Framework; Information Systems Audit and Control Foundation; ISBN: 1-893209-14-8.

[COBI02 2000] IT Governance Institute; 2000; CobiT 3rd Edition – Control Objectives; Information Systems Audit and Control Foundation; ISBN: 1-893209-17-2.

[COBI03 2000] IT Governance Institute; 2000; CobiT 3rd Edition – Implementation Tool Set; Information Systems Audit and Control Foundation; ISBN: 0-893209-16-14.

[COBI04 2000] IT Governance Institute; 2000; CobiT 3rd Edition – Management Guidelines; Information Systems Audit and Control Foundation; ISBN: 1-893209-12-1.

[COBI05 2000] IT Governance Institute; 2000; CobiT 3rd Edition – Audit Guidelines; Information Systems Audit and Control Foundation; ISBN: 1-893209-18-0.

[COMM 2003] Commission Recommendation of 6 May 2003 concerning Definition of Micro, Small and Medium-sized Companies; Official Journal of the European Union; May 2003.

[CRAM 2005] CRAMM.com; CRAMM Methodology; http://www.cramm.com; Accessed May 2005.

[CW 2005] The Commonwealth Website; http://www.thecommonwealth.org; Accessed November 2005.

[DAIL 2004] Daily News Homepage; Daily News Online; http://www.dailynews.co.za, April 2004.

[DICT 2004] Dictionary.com; 2004; Terms: “Security”; http://www.dictionary.com; Accessed October 2004.

[DISP 2003] Dispatch Online; “SMMEs failure blamed on poor management”; Accessed through DispatchOnline.co.za; http://www.dispatchonline.co.za; Accessed September 2004.

[EDUC 2005] “Address by the Minister of Education, Ms Naledi Pandor, MP, at the Steve Biko International Peace Awards”; 23 September 2005; www.education.pwv.gov.za; Accessed November 2005.

[EURO 2004] EEA.com; European Environment Agency Glossary; Terms: "Vulnerability"; http://www.eea.org; Accessed October 2004.

[FIND 2004] FindingPost.com; Terms: "Return on Investment"; http://www.findingpost.com; Accessed October 2004.

[FIRE 2004] Donald-Firesmith.com; Firesmith Open Process Framework; Terms: "Risk Monitoring"; http://www.donald-firesmith.com; Accessed October 2004.

[FUND 2004] Fundes.org; SME's Indicators in the FUNDES Region; http://www.fundes.org; Accessed October 2004.

[GLOS 2004] Glossary; Terms: "Information Security"; http://www.glossary.its.bldrdoc.gov; Accessed October 2004.

[GMIT 2002] Guidelines for the Management of IT Security Part 3 under Revision in ISO/IEC JTC1/SC27.

[GOV 2004] The South African Government; http://www.gov.org.za. Accessed October 2004.

[IMF 2004] IMF List of Advanced Economies; Accessed through Reading.org; http://www.read/ing.org/membership/devel.countries.html; Accessed October 2004.

[INET 2004] I-Net Bridge; Insurance Cover Now Available for SMME Bosses; Http://www.inet.co.za; Accessed September 2004.

[INSI 2005] Insight Consulting; 2005; CRAMM V Express Walkthrough Flash Presentation – CRAMM V (Computer Program).

[INVE 2004] InvestorWords.com; Terms: "Risk", "Risk Assessment"; http://www.investorwords.com; Accessed October 2004.

[ITGI 2005] ITGI Homepage; http://www.itgi.org; Accessed January 2005.

[JOBU 2005] “Diepsloot gets a facelift”; 27 July 2004; Ndaba Dlamini; http://www.joburg.co.za; Accessed November 2005.

[KARA 2005] Karabarak, B., Sogukpinar, I.; ISRAM: Information Security Risk Analysis Method; Bilge Karabacak, Ibrahim Sogukpinar; Computers & Security; 2005, 24.

[KING 2002] King Committee on Corporate Governance; 2002; King Report on Corporate Governance for South Africa; Institute of Directors; ISBN: 0-620-28851-5.

[KIRI 1999] Kiriri, P.; Small and Medium Enterprises (SMEs); Validating Life Cycle Stage Determinants; Strathmore University; Kenya; 1999.

[KOCH 1997] Koch, R.; The 80/20 Principle. The Secret of Achieving More with Less; 1997; Nicholas Brealey Publishing.

[LECH 2004] Lecholo, DS.; Botswana’s Experience of Informal Traders, Sustainable Livelihoods and Economic Development through Trade; Presented at the SADC Workshop on Informal Traders; February 2004.

[MCNA 1999] McNamee, D.; Risk Assessment Glossary; 1999; Terms: “Risk Identification”.

[NATI 2003] The Relative Importance of SME’s in the South African Economy: An Analysis of Issues and Quantification of Magnitudes (requested by National Treasury).

[NIST 2002] Risk Management Guide for Information Security Systems; Recommendations of the National Institute of Standards and Technology; Stoneburner, G., Goguen, A. Feringa, A.; Special Publication 800-30; July 2002; US Government Printing Office; Terms: “Information Security”.

[OCTA01 2003] OCTAVE-S Implementation Guide, Version 0.9; Volume 1: Introduction to OCTAVE-S; Alberts, C., Dorofee, A., James, C., Woody, C.; August 2003.

[OCTA02 2003] OCTAVE-S Implementation Guide, Version 0.9; Volume 2: Preparation Guidance; Alberts, C., Dorofee, A., James, C., Woody, C.; August 2003.

[OCTA03 2003] OCTAVE-S Implementation Guide, Version 0.9; Volume 3: Method Guidelines; Alberts, C., Dorofee, A., James, C., Woody, C.; August 2003.

[OLIV 1999] Olivier, MS.; Information Technology Research. A Practical Guide; 1999.

[PMBO 2004] A Guide to the Project Management Body of Knowledge; Third Edition; ANSI/PMI 99-001-2004; Terms: “Risk Mitigation”.

[PSAR 2002] Psaros, J., Seamer, M.; Horwath; 2002; Corporate Governance Report by Prof Jim Psaros and Michael Seamer; University of Newcastle Australia; ISBN: 0-9581-0-0; Accessed through Horwath.com.au; http://www.horwath.com.au; Accessed November 2004.

[SABS 2000] SABS ISO 17799; Information Technology Code of Practice for Information Security Management; The South African Bureau of Standards; 2000; ISBN 0-626-12835-8.

[SBA 2005] SBA.gov; United States Small Business Administration; http://www.sba.gov; Accessed November 2005.

[SCHW 2002] Schwalbe, K.; Information Technology Project Management; Course Technology 2002; ISBN: 0-619-03528-5.

[SOCI 2004] SRA.com; Society for Risk Analysis; Terms: “Risk Identification”; http://www.sra.org; Accessed October 2004.

[SOUT 2002] South Africa Business Guidebook 2002/2003.

[SPIN 1999] Spinellis, Kokolakis, Gritzalis; Security Requirements, Risks, and Recommendations for Small Enterprise and Home-office Environments; Information Management and Computer Security; Volume 7; Issue 3; 1999.

[STEP 2002] A Step by Step Approach to Risk Assessment; The Griffin Tate Group; 2002.

[SUH 2003] Suh, B., Han, I.; The IS Risk Analysis Based on a Business Model; Information & Management; Elsevier Science; 2003.

[TOUR 2005] South African Government Department of Environmental Affairs and Tourism Website; http://www.environment.gov.za; Accessed November 2005.

[UN 2005] United Nations Website; http://www.un.org; Accessed November 2005.

[WEBS 2004] Webster's Revised Unabridged Dictionary; http://www.websters-online-dictionary.org; Terms: "Security"; Accessed October 2004.

[WORD 2004] WordIQ.com; Terms: "Threat", Exposure", "Monitoring", "Corporate Governance"; http://www.wordIQ.com; Accessed October 2004.

[WORL 2004] World Markets Research Centre South Africa: Country Risk Summary; Accessed through WorldMarketsAnalysis.com; http://www.worldmarketsanalysis.com; Accessed October 2004.